Alcatel-Lucent 5620

SERVICE AWARE MANAGER | RELEASE 8.0 R8

USER GUIDE

3HE 05719 AAAH TQZZA Edition 01

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent tries to ensure that this information accurately reflects information provided by the supplier, please refer to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

Alcatel-Lucent License Agreement

SAMPLE END USER LICENSE AGREEMENT

1. LICENSE

1.1 Subject to the terms and conditions of this Agreement, Alcatel-Lucent grants to Customer and Customer accepts a nonexclusive, nontransferable license to use any software and related documentation provided by Alcatel-Lucent pursuant to this Agreement ("Licensed Program") for Customer's own internal use, solely in conjunction with hardware supplied or approved by Alcatel-Lucent. In case of equipment failure, Customer may use the Licensed Program on a backup system, but only for such limited time as is required to rectify the failure.

1.2 Customer acknowledges that Alcatel-Lucent may have encoded within the Licensed Program optional functionality and capacity (including, but not limited to, the number of equivalent nodes, delegate workstations, paths and partitions), which may be increased upon the purchase of the applicable license extensions.

1.3 Use of the Licensed Program may be subject to the issuance of an application key, which shall be conveyed to the Customer in the form of a Supplement to this End User License Agreement. The purchase of a license extension may require the issuance of a new application key.

2. PROTECTION AND SECURITY OF LICENSED PROGRAMS

2.1 Customer acknowledges and agrees that the Licensed Program contains proprietary and confidential information of Alcatel-Lucent and its third party suppliers, and agrees to keep such information confidential. Customer shall not disclose the Licensed Program except to its employees having a need to know, and only after they have been advised of its confidential and proprietary nature and have agreed to protect same.

2.2 All rights, title and interest in and to the Licensed Program, other than those expressly granted to Customer herein, shall remain vested in Alcatel-Lucent or its third party suppliers. Customer shall not, and shall prevent others from copying, translating, modifying, creating derivative works, reverse engineering, decompiling, encumbering or otherwise using the Licensed Program except as specifically authorized under this Agreement. Notwithstanding the foregoing, Customer is authorized to make one copy for its archival purposes only. All appropriate copyright and other proprietary notices and legends shall be placed on all Licensed Programs supplied by Alcatel-Lucent, and Customer shall maintain and reproduce such notices on any full or partial copies made by it.

3. TERM

3.1 This Agreement shall become effective for each Licensed Program upon delivery of the Licensed Program to Customer.

3.2 Alcatel-Lucent may terminate this Agreement: (a) upon notice to Customer if any amount payable to Alcatel-Lucent is not paid within thirty (30) days of the date on which payment is due; (b) if Customer becomes bankrupt, makes an assignment for the benefit of its creditors, or if its assets vest or become subject to the rights of any trustee, receiver or other administrator; (c) if bankruptcy, reorganization or insolvency proceedings are instituted against Customer and not dismissed within 15 days; or (d) if Customer breaches a material provision of this Agreement and such breach is not rectified within 15 days of receipt of notice of the breach from Alcatel-Lucent.

3.3 Upon termination of this Agreement, Customer shall return or destroy all copies of the Licensed Program. All obligations of Customer arising prior to termination, and those obligations relating to confidentiality and nonuse, shall survive termination.

4. CHARGES

4.1 Upon shipment of the Licensed Program, Alcatel-Lucent will invoice Customer for all fees, and any taxes, duties and other charges. Customer will be invoiced for any license extensions upon delivery of the new software application key or, if a new application key is not required, upon delivery of the extension. All amounts shall be due and payable within thirty (30) days of receipt of invoice, and interest will be charged on any overdue amounts at the rate of 1 1/2% per month (19.6% per annum).

5. SUPPORT AND UPGRADES

5.1 Customer shall receive software support and upgrades for the Licensed Program only to the extent provided for in the applicable Alcatel-Lucent software support policy in effect from time to time, and upon payment of any applicable fees. Unless expressly excluded, this Agreement shall be deemed to apply to all updates, upgrades, revisions, enhancements and other software which may be supplied by Alcatel-Lucent to Customer from time to time.

6. WARRANTIES AND INDEMNIFICATION

6.1 Alcatel-Lucent warrants that the Licensed Program as originally delivered to Customer will function substantially in accordance with the functional description set out in the associated user documentation for a period of 90 days from the date of shipment, when used in accordance with the user documentation. Alcatel-Lucent's sole liability and Customer's sole remedy for a breach of this warranty shall be Alcatel-Lucent's good faith efforts to rectify the nonconformity or, if after repeated efforts Alcatel-Lucent is unable to rectify the nonconformity, Alcatel-Lucent shall accept return of the Licensed Program and shall refund to Customer all amounts paid in respect thereof. This warranty is available only once in respect of each Licensed Program, and is not renewed by the payment of an extension charge or upgrade fee.

6.2 ALCATEL-LUCENT EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, REPRESENTATIONS, COVENANTS OR CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OR REPRESENTATIONS OF WORKMANSHIP, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, DURABILITY, OR THAT THE OPERATION OF THE LICENSED PROGRAM WILL BE ERROR FREE OR THAT THE LICENSED PROGRAMS WILL NOT INFRINGE UPON ANY THIRD PARTY RIGHTS.

6.3 Alcatel-Lucent shall defend and indemnify Customer in any action to the extent that it is based on a claim that the Licensed Program furnished by Alcatel-Lucent infringes any patent, copyright, trade secret or other intellectual property right, provided that Customer notifies Alcatel-Lucent within ten (10) days of the existence of the claim, gives Alcatel-Lucent sole control of the litigation or settlement of the claim, and provides all such assistance as Alcatel-Lucent may reasonably require. Notwithstanding the foregoing, Alcatel-Lucent shall have no liability if the claim results from any modification or unauthorized use of the Licensed Program by Customer, and Customer shall defend and indemnify Alcatel-Lucent against any such claim.

6.4 Alcatel-Lucent Products are intended for standard commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The Customer hereby agrees that the use, sale, license or other distribution of the Products for any such application without the prior written consent of Alcatel-Lucent, shall be at the Customer's sole risk. The Customer also agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the Products in such applications.

7. LIMITATION OF LIABILITY

7.1 IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF ALCATEL-LUCENT, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ANY CLAIM, REGARDLESS OF VALUE OR NATURE, EXCEED THE AMOUNT PAID UNDER THIS AGREEMENT FOR THE LICENSED PROGRAM THAT IS THE SUBJECT MATTER OF THE CLAIM. IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF ALCATEL-LUCENT, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ALL CLAIMS EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER TO ALCATEL-LUCENT HEREUNDER. NO PARTY SHALL BE LIABLE FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER OR NOT SUCH DAMAGES ARE FORESEEABLE, AND/OR THE PARTY HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7.2 The foregoing provision limiting the liability of Alcatel-Lucent's employees, agents, officers and directors shall be deemed to be a trust provision, and shall be enforceable by such employees, agents, officers and directors as trust beneficiaries.

8. GENERAL

8.1 Under no circumstances shall either party be liable to the other for any failure to perform its obligations (other than the payment of any monies owing) where such failure results from causes beyond that party's reasonable control.

8.2 This Agreement constitutes the entire agreement between Alcatel-Lucent and Customer and supersedes all prior oral and written communications. All amendments shall be in writing and signed by authorized representatives of both parties.

8.3 If any provision of this Agreement is held to be invalid, illegal or unenforceable, it shall be severed and the remaining provisions shall continue in full force and effect.

8.4 The Licensed Program may contain freeware or shareware obtained by Alcatel-Lucent from a third party source. No license fee has been paid by Alcatel-Lucent for the inclusion of any such freeware or shareware, and no license fee is charged to Customer for its use. The Customer agrees to be bound by any license agreement for such freeware or shareware. CUSTOMER ACKNOWLEDGES AND AGREES THAT THE THIRD PARTY SOURCE PROVIDES NO WARRANTIES AND SHALL HAVE NO LIABILITY WHATSOEVER IN RESPECT OF CUSTOMER'S POSSESSION AND/OR USE OF THE FREEWARE OR SHAREWARE.

8.5 Alcatel-Lucent shall have the right, at its own expense and upon reasonable written notice to Customer, to periodically inspect Customer's premises and such documents as it may reasonably require, for the exclusive purpose of verifying Customer's compliance with its obligations under this Agreement.

8.6 All notices shall be sent to the parties at the addresses listed above, or to any such address as may be specified from time to time. Notices shall be deemed to have been received five days after deposit with a post office when sent by registered or certified mail, postage prepaid and receipt requested.

8.7 If the Licensed Program is being acquired by or on behalf of any unit or agency of the United States Government, the following provision shall apply: If the Licensed Program is supplied to the Department of Defense, it shall be classified as "Commercial Computer Software" and the United States Government is acquiring only "restricted rights" in the Licensed Program as defined in DFARS 227-7202-1(a) and 227.7202-3(a), or equivalent. If the Licensed Program is supplied to any other unit or agency of the United States Government, rights will be defined in Clause 52.227-19 or 52.227-14 of the FAR, or if acquired by NASA, Clause 18-52.227-86(d) of the NASA Supplement to the FAR, or equivalent. If the software was acquired under a contract subject to the October 1988 Rights in Technical Data and Computer Software regulations, use, duplication and disclosure by the Government is subject to the restrictions set forth in DFARS 252-227.7013(c)(1)(ii) 1988, or equivalent.

8.8 Customer shall comply with all export regulations pertaining to the Licensed Program in effect from time to time. Without limiting the generality of the foregoing, Customer expressly warrants that it will not directly or indirectly export, reexport, or transship the Licensed Program in violation of any export laws, rules or regulations of Canada, the United States or the United Kingdom.

8.9 No term or provision of this Agreement shall be deemed waived and no breach excused unless such waiver or consent is in writing and signed by the party claimed to have waived or consented. The waiver by either party of any right hereunder, or of the failure to perform or of a breach by the other party, shall not be deemed to be a waiver of any other right hereunder or of any other breach or failure by such other party, whether of a similar nature or otherwise.

8.10 This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario. The application of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly excluded.

Preface

The Preface provides general information about the 5620 Service Aware Manager documentation suite.

Note — You can use the Search function of Acrobat Reader (File→Search) to find a term in a PDF of this document. To refine your search, use appropriate search options (for example, search for whole words only or enable case-sensitive searching). You can also search for a term in multiple PDFs at once. For more information, see the Help for Acrobat Reader.

5620 SAM documentation suite

The 5620 SAM documentation suite describes the 5620 SAM and the associated network management of its supported devices. Contact your Alcatel-Lucent support representative for information about specific network or facility considerations.

Table 1 lists the documents in the 5620 SAM documentation suite.

Table 1 5620 SAM customer documentation suite

Guide	Description
5620 SAM core documentation	
5620 SAM Planning Guide	The *5620 SAM Planning Guide* provides information about 5620 SAM scalability and recommended hardware configurations.

(1 of 4)

Guide	Description
*5620 SAM	5650 CPAM Installation and Upgrade Guide*	The *5620 SAM	5650 CPAM Installation and Upgrade Guide* provides OS considerations, configuration information, and procedures for the following: • installing, upgrading, and uninstalling 5620 SAM and 5650 CPAM software in standalone and redundant deployments • 5620 SAM system migration to a different system • conversion from a standalone to a redundant 5620 SAM system
5620 SAM User Guide	The *5620 SAM User Guide* provides information about using the 5620 SAM to manage the service-aware IP/MPLS network, including GUI basics, commissioning, service configuration, and policy management. The *5620 SAM User Guide* uses a task-based format. Each chapter contains: • a workflow that describes the steps for configuring and using the functionality • detailed procedures that list the configurable parameters on the associated forms 5620 SAM management information specific to LTE network elements is covered in the *5620 SAM LTE ePC User Guide* and *5620 SAM LTE RAN User Guide*. 5620 SAM management information specific to 1830 PSS network elements is covered in the *5620 SAM 1830 PSS User Guide*.
5620 SAM Parameter Guide	The *5620 SAM Parameter Guide* provides: • parameter descriptions that include value ranges and default values • parameter options and option descriptions • parameter and option dependencies • parameter mappings to the 5620 SAM-O XML equivalent property names There are dynamic links between the procedures in the *5620 SAM User Guide* and the parameter descriptions in the *5620 SAM Parameter Guide*. See Procedure 2 for more information. Parameters specific to LTE network elements are covered in the *5620 SAM LTE Parameter Reference*. Parameters specific to 1830 PSS network elements are covered in the *5620 SAM 1830 PSS Parameter Reference*.
5620 SAM Statistics Management Guide	The *5620 SAM Statistics Management Guide* provides information about how to configure performance and accounting statistics collection and how to view counters using the 5620 SAM. Network examples are included.
5620 SAM Scripts and Templates Developer Guide	The *5620 SAM Scripts and Templates Developer Guide* provides information that allows you to develop, manage, and execute CLI-based or XML-based scripts or templates. The guide is intended for developers, skilled administrators, and operators who are expected to be familiar with the following: • CLI scripting, XML, and the Velocity engine • basic scripting or programming • 5620 SAM functions

5620 SAM Troubleshooting Guide	The *5620 SAM Troubleshooting Guide* provides task-based procedures and user documentation to:
	• help resolve issues in the managed and management networks
	• identify the root cause and plan corrective action for:
	  • alarm conditions on a network object or customer service
	  • problems on customer services with no associated alarms
	• list problem scenarios, possible solutions, and tools to help check:
	  • network management LANs
	  • PC and Sun platforms, and operating systems
	  • 5620 SAM client GUIs and client OSS applications
	  • 5620 SAM servers
	  • 5620 SAM databases

(2 of 4)

Guide	Description
5620 SAM Maintenance Guide	The *5620 SAM Maintenance Guide* provides procedures for: • generating baseline information for 5620 SAM applications • performing daily, weekly, monthly, and as-required maintenance activities for 5620 SAM-managed networks
5620 SAM Integration Guide	The *5620 SAM Integration Guide* provides procedures to allow the 5620 SAM to integrate with additional components.
5620 SAM System Architecture Guide	The *5620 SAM System Architecture Guide* is intended for technology officers and network planners to increase their knowledge of the 5620 SAM software structure and components. It describes the system structure, software components, and interfaces of the 5620 SAM. In addition, 5620 SAM fault tolerance, security, and network management capabilities are discussed from an architectural perspective.
5620 SAM NE Compatibility Guide	The *5620 SAM NE Compatibility Guide* provides release-specific information about the compatibility of managed device features in 5620 SAM releases.
5620 SAM Release Description	The *5620 SAM Release Description* provides information about the new features associated with a 5620 SAM software release.
5620 SAM Glossary	The *5620 SAM Glossary* defines terms and acronyms used in all of the 5620 SAM documentation, including 5620 SAM LTE documentation.
5620 SAM-O OSS Interface Developer Guide	The *5620 SAM-O OSS Interface Developer Guide* provides information that allows you to: • use the 5620 SAM-O OSS interface to access network management information • learn about the information model associated with the managed network • develop OSS applications using the packaged methods, classes, data types, and objects necessary to manage 5620 SAM functions
5620 SAM LTE documentation	
5620 SAM LTE ePC User Guide	The *5620 SAM LTE ePC User Guide* describes how to discover, configure, and manage LTE ePC devices using the 5620 SAM. The guide is intended for LTE ePC network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire *5620 SAM LTE ePC User Guide* before you attempt to use the 5620 SAM in your LTE network.
5620 SAM LTE RAN User Guide	The *5620 SAM LTE RAN User Guide* describes how to discover, configure, and manage the eNodeB using the 5620 SAM. The guide is intended for LTE RAN network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire *5620 SAM LTE RAN User Guide* before you attempt to use the 5620 SAM in your LTE network.
5620 SAM LTE Parameter Reference	The *5620 SAM LTE Parameter Reference* provides a list of all LTE ePC and LTE RAN parameters supported in the 5620 SAM.
5620 SAM LTE Alarm Reference	The *5620 SAM LTE Alarm Reference* provides a list of LTE ePC and LTE RAN alarms that can be reported in the 5620 SAM GUI.
5620 SAM-O 3GPP OSS Interface Developer Guide	The *5620 SAM-O 3GPP OSS Interface Developer Guide* describes the components and architecture of the 3GPP OSS interface to the 5620 SAM. It includes procedures and samples to assist OSS application developers to use the 3GPP interface to manage LTE devices.
5620 SAM-O 3GPP OSS Interface Compliance Statements	The *5620 SAM-O 3GPP OSS Interface Compliance Statements* document describes the compliance of the 5620 SAM northbound interface with the 3GPP standard.
5620 SAM Optical documentation	
5620 SAM Optical User Guide	The *5620 SAM Optical User Guide* describes how to discover, configure, and manage optical devices using the 5620 SAM. The guide is intended for optical network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire *5620 SAM Optical User Guide* before you attempt to use the 5620 SAM in your network.

(3 of 4)

Guide	Description
5620 SAM Optical Parameter Reference	The *5620 SAM Optical Parameter Reference* provides a list of all optical device parameters supported in the 5620 SAM.
5620 SAM Optical Alarm Reference	The *5620 SAM Optical Alarm Reference* provides a list of optical device alarms that can be reported in the 5620 SAM GUI.

(4 of 4)

Procedure 1 To find the 5620 SAM user documentation

The user documentation is available from the following sources:

- the User_Documentation directory on the product DVD-ROM
- Help→5620 SAM User Documentation in the 5620 SAM client GUI main menu

Note — Users of Mozilla browsers may receive an error message when using the User Documentation Index page (index.html) to open the PDF files in the 5620 SAM documentation suite. The offline storage and default cache values used by the browsers are the cause of the error message.

Alcatel-Lucent recommends changing the offline storage (Mozilla Firefox) or cache (Mozilla 1.7) values to 100 Mbytes to eliminate the error message.

Procedure 2 To view parameter descriptions from the *5620 SAM User Guide*

You can click on a parameter name in a *5620 SAM User Guide* procedure to open the matching parameter description in the *5620 SAM Parameter Guide*. Ensure the following conditions are true beforehand:

- the *5620 SAM Parameter Guide* and *5620 SAM User Guide* are located in the same directory
- Adobe Reader Release 5.0 or later is installed

1 To view a parameter description when both the *5620 SAM User Guide* and the *5620 SAM Parameter Guide* are open in Adobe Acrobat, click on the parameter name in the *5620 SAM User Guide*.

The parameter description is displayed in the *5620 SAM Parameter Guide*.

2 To view a parameter description when only the *5620 SAM User Guide* is open in Adobe Acrobat:

i Click on a parameter name in a procedure in the *5620 SAM User Guide*. The *5620 SAM User Guide* closes and the *5620 SAM Parameter Guide* opens to display the parameter description.

ii Double-click on the Previous View button in Adobe Acrobat (or press Alt + ←) to re-open the *5620 SAM User Guide*. The *5620 SAM User Guide* opens and displays the parameter from step i.

Prerequisites

Readers of the 5620 SAM documentation suite are assumed to be familiar with the following:

- 5620 SAM software structure and components
- 5620 SAM GUI operations and tools
- typical 5620 SAM management tasks and procedures
- device and network management concepts

Conventions

Table 2 lists the conventions that are used throughout the documentation.

Table 2 Documentation conventions

Convention	Description	Example
Key name	Press a keyboard key	Delete
Italics	Identifies a variable	*hostname*

(1 of 2)

Convention	Description	Example
Key+Key	Type the appropriate consecutive keystroke sequence	CTRL+G
Key-Key	Type the appropriate simultaneous keystroke sequence	CTRL-G
*	An asterick is a wildcard character, which means “any character” in a search argument.	log_file*.txt
↵	Press the Return key	↵
—	An em dash indicates there is no information.	—
→	Indicates that a cascading submenu results from selecting a menu item	Policies→Alarm Policies

(2 of 2)

Procedures with options or substeps

When there are options in a procedure, they are identified by letters. When there are substeps in a procedure, they are identified by Roman numerals.

Example of options in a procedure

At step 1, you can choose option a or b. At step 2, you must do what the step indicates.

1 This step offers two options. You must choose one of the following.

   a This is one option.

   b This is another option.

2 You must perform this step.

Example of substeps in a procedure

At step 1, you must perform a series of substeps within a step. At step 2, you must do what the step indicates.

1 This step has a series of substeps that you must perform to complete the step. You must perform the following substeps.

   i This is the first substep.

   ii This is the second substep.

   iii This is the third substep.

2 You must perform this step.

Measurement conventions

Measurements in this document are expressed in metric units and follow the Système international d’unités (SI) standard for abbreviation of metric units. If imperial measurements are included, they appear in brackets following the metric unit.

Table 3 lists the measurement symbols used in this document.

Table 3 Bits and bytes conventions

Measurement	Symbol
bit	b
byte	byte
kilobits per second	kb/s

Important information

The following conventions are used to indicate important information:

Warning — Warning indicates that the described activity or situation may, or will, cause equipment damage or serious performance problems.

Caution — Caution indicates that the described activity or situation may, or will, cause service interruption.

Note — Notes provide information that is, or may be, of special interest.

Contents

5620 SAM system management

Device management

Introduction

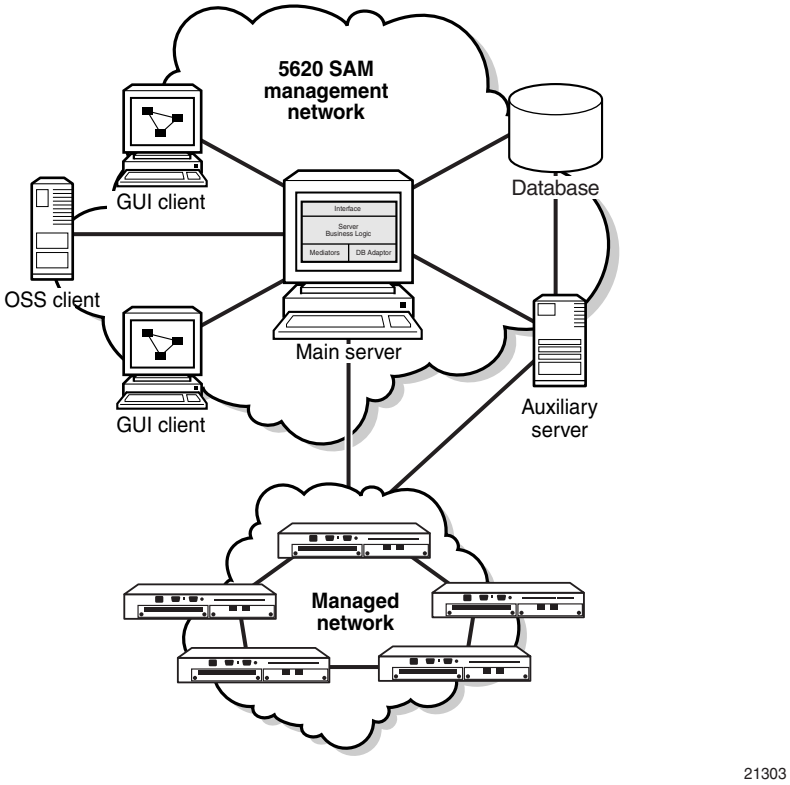
1 — 5620 SAM system overview

1.1 5620 SAM system overview

The 5620 SAM is a system that is designed to manage Alcatel-Lucent network elements, or NEs, such as routers and switches. The 5620 SAM also supports the management of some Telco devices, and provides limited management of other third-party devices, which are called generic NEs.

A 5620 SAM system has client, server, and database components that are deployed in a standalone or redundant configuration. Figure 1-1 shows a block diagram of a standalone 5620 SAM system and the network that it manages. The management network, which contains the 5620 SAM components, connects to the managed network of NEs from one or more points, depending on the deployment complexity.

Figure 1-1 Standalone 5620 SAM system



A 5620 SAM operator performs network management or system administration tasks using a GUI or OSS client that connects to a main server. The main server sends and receives NE management traffic, and directs optional auxiliary servers to perform intensive tasks such as NE statistics collection. Main and auxiliary servers store information in the same 5620 SAM database.

The 5620 SAM uses a Java-based technology that provides distributed, secure, and scalable processing. See the *5620 SAM System Architecture Guide* for system design information. See chapter 6 for information about 5620 SAM system redundancy.

1.2 About this guide

The *5620 SAM User Guide* describes the various 5620 SAM functions, explains the GUI operations associated with each function, and indicates whether the function is available through the OSSI. See the *5620 SAM-O OSS Interface Developer Guide* for information about using the OSSI to perform a 5620 SAM function.

5620 SAM User Guide procedures that contain configurable parameters have links to parameter descriptions in the *5620 SAM Parameter Guide*, where appropriate.

Note — The *5620 SAM User Guide* parameter links can function only when the *5620 SAM Parameter Guide* is in the same directory as the *5620 SAM User Guide*.

This guide contains the following volumes, which are ordered by functional area, from lowest to highest:

- Introduction—contains general 5620 SAM information such as the following:
  - a system overview
  - feature lists by release
  - basic GUI operation instructions
  - GUI map management
- 5620 SAM system management—contains information about 5620 SAM administration such as the following:
  - system configuration
  - system redundancy
  - system and user security
  - interworking with other systems
- Device management—contains information about device functions that are not directly related to networking, such as the following:
  - device support
  - preparing devices for 5620 SAM management
  - 5620 SAM device and equipment management functions
- Network management—contains information about network functions such as the following:
  - general routing and forwarding
  - protocol-specific routing and forwarding
  - traffic management using MPLS and service tunnels
  - fault management
  - OAM diagnostic tests
  - NE redundancy
- Policy management—contains information about configuring and applying 5620 SAM policies that define rules for NE, network, or 5620 SAM operation
- Service management—contains information about managing customer services, such as the following:
  - service creation and configuration
  - customer and subscriber management
  - service verification, troubleshooting, and root-cause analysis
  - scheduling of routine, service-related operations

1.3 Workflow for network management using the 5620 SAM

The following workflow describes the sequence of high-level tasks required to deploy the 5620 SAM and use it to perform network management.

You can use an OSS client to perform many of the functions described in this workflow. See the *5620 SAM-O OSS Interface Developer Guide* for more information.

You can use scripts and templates to perform complex CLI configuration of managed devices from the 5620 SAM. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

1 Plan your 5620 SAM deployment by considering things such as the following:

- the number of NEs the 5620 SAM is to manage
- the hardware required for the 5620 SAM system
- the redundancy requirements
- management network latency
- management network bandwidth requirements
- naming conventions for 5620 SAM objects that you create
- NE compatibility with the 5620 SAM software

See the *5620 SAM Planning Guide* and the *5620 SAM NE Compatibility Guide* for more information.

2 Install the 5620 SAM software, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

3 Become familiar with GUI basics such as the following:

- navigating the GUI, using the GUI elements, and performing searches; see chapter 2
- using topology maps; see chapter 4

4 Customize or configure the 5620 SAM operating environment, as required.

a See chapter 5 for information about the following:

- viewing or changing 5620 SAM license information
- using the auto-client update utility to define the configuration of each GUI client
- securing 5620 SAM server/database communication
- changing global network-management operating parameters

b Manage 5620 SAM system redundancy; see chapter 6.

c Configure database logging, and manage other database administration functions such as backups and restores; see chapter 7.

d Create 5620 SAM user groups and accounts with privileges for specific operational scopes; see chapter 8.

e Configure SSL security for the 5620 SAM system; see chapter 9.

f Configure integration for the 5620 SAM and external systems such as the 5620 NM, the 5650 CPAM, and the 5780 DSC; see chapter 10.

5 Prepare the network devices for 5620 SAM management.

a Become familiar with the support that the 5620 SAM provides for various devices; see chapter 11.

b Commission devices for 5620 SAM management, and configure how and when the 5620 SAM polls the devices for MIB changes; see chapter 12.

c Perform 5620 SAM discovery of the commissioned network devices, and optionally configure SSH2 security for CLI sessions, if required; see chapter 13.

d Use a Telnet or SSH CLI from the 5620 SAM to view and modify device configurations, if required; see chapter 14.

6 Use the 5620 SAM to manage devices.

a View, manage, and configure equipment; see chapters 15, 16, and 17.

b Create equipment inventories of managed devices; see chapter 19.

c Create security policies and management access filters for NEs, and create NE user accounts that provide secure NE access using RADIUS or TACACS+ authentication; see chapter 18.

d Configure TCP enhanced authentication between NEs, if required; see chapter 20.

e Perform NE maintenance functions such as backing up and restoring device configurations, upgrading device software, and monitoring deployment of configuration changes to devices; see chapter 21.

f Perform additional device management functions such as the following:

- card migration; see chapter 22
- bulk configuration changes; see chapter 24
- object life cycle management; see chapter 25
- automatic provisioning; see chapter 26

7 Use the 5620 SAM to manage network functions, as required.

a Configure basic NE routing and forwarding; see chapter 27.

b Configure NE protocols; see chapter 28.

c Configure MPLS and LSPs; see chapter 29.

d Configure service tunnels to carry service traffic; see chapter 30.

e Configure NE-specific network functions such as the following:

- Lawful Intercept; see chapter 31
- IPsec; see chapter 32
- ISA-Video; see chapter 33

f Configure 5620 SAM alarm policies, and use alarms to perform fault management; see chapter 34.

g Use OAM diagnostic tools to troubleshoot network problems; see chapter 35.

h Configure redundancy in the managed network using functions such as the following

- VRRP; see chapter 36
- APS; see chapter 37
- MC peer, endpoint, LAG, synchronization, and ring groups; see chapters 38 to 42

8 Create 5620 SAM policies that define the conditions for 5620 SAM management functions that include the following:

- network—ACL filters, auto-tunnel, RMON
- service—QoS, multicast traffic management, residential subscriber
- 5620 SAM—time of day, size constraint, format and range

See chapter 43 for general information about 5620 SAM policy management. See chapters 44 to 59 for information about specific policy types.

9 Use the 5620 SAM to manage customer services and related functions.

a Become familiar with 5620 SAM service management concepts such as SAPs, the TPSDA model, and QoS delivery using shared queue groups; see chapters 60 and 61.

b Configure and manage customers; see chapter 63.

c Configure and manage the residential subscribers of customer services; see chapter 64.

d Configure VLAN services for subscribers connected to 7250 SAS or Telco devices; see chapter 65.

e Configure VLAN groups and paths for 9500 MPR and OmniSwitch devices; see chapter 66.

f Configure VLL Apipe, Cpipe, Epipe, Fpipe, and Ipipe services to provide point-to-point connectivity between customer access ports; see chapter 67.

g Configure VPLS to provide virtual LAN connectivity that connects multiple customer sites in a bridged domain; see chapter 68.

h Create mirror services for troubleshooting customer traffic issues or for use with Lawful Intercept; see chapter 69.

i Configure IES to provide an IP interface between customer traffic and the Internet; see chapter 70.

j Configure VPRN services to provides a virtual IP network that connects multiple customer sites; see chapter 71.

k Configure composite services to connect various types services; see chapter 72.

l Configure Application Assurance to provide deep-packet inspection and application-based subscriber traffic management; see chapter 73.

m Configure 5620 SAM schedules and scheduled tasks to automate 5620 SAM service management functions such as running OAM diagnostics; see chapter 74.

n Use the 5620 SAM Service Test Manager to group OAM diagnostic tests into suites of manual and automatically-generated tests; see chapter 75.

10 Collect 5620 SAM and NE statistics to monitor 5620 SAM, network and service performance, compile equipment usage and billing data, and ensure SLA compliance; see the *5620 SAM Statistics Management Guide*.

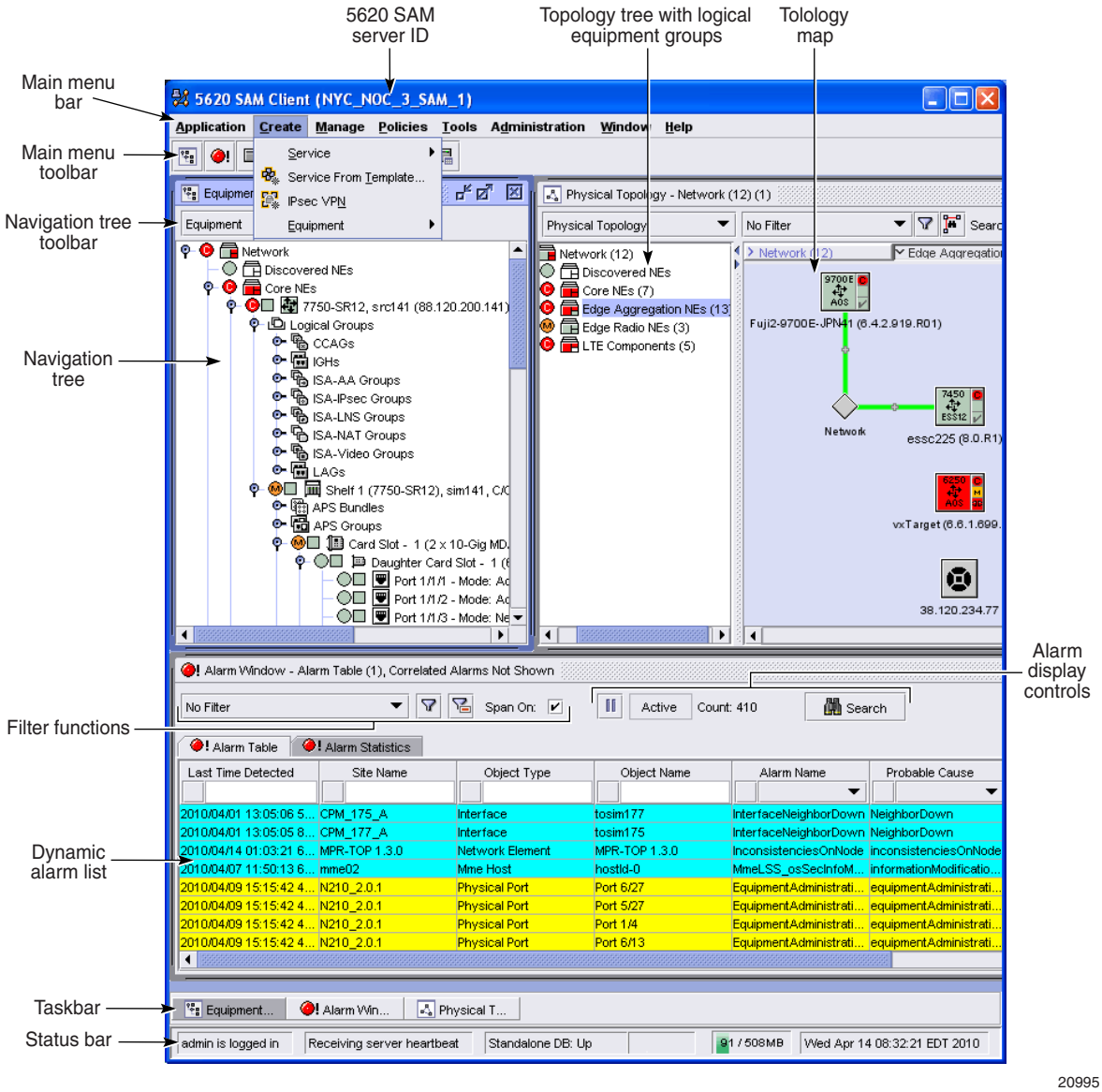
2 — 5620 SAM GUI overview

2.1 5620 SAM GUI overview

The 5620 SAM GUI is a graphical interface on a 5620 SAM client station that allows a NOC operator to perform network management functions. Multiple 5620 SAM GUI clients can connect to a 5620 SAM server.

The main GUI elements, as shown in Figure 2-1, are the navigation tree, alarm window, and map panel. This chapter describes general GUI operations such as managing windows and forms, and performing searches. See chapter 4 for information about map management.

Figure 2-1 Main 5620 SAM GUI elements



The 5620 SAM GUI enables an operator to do things such as the following:

- Display equipment and alarm status information.
- Configure and manage network management applications.
- Simplify the administration and configuration of equipment, customers, services, and subscribers using management forms instead of a CLI.
- Configure, manage, and monitor SLAs and equipment using statistics.
- Create and manage security policies for secure device and 5620 SAM access.

Floating windows

The 5620 SAM GUI uses floating windows that you can move, size, close, and bring to the foreground to provide the optimal working space for performing a task. By default, the navigation tree window appears at the left side of the GUI, the alarm window at the bottom, and the physical topology map is at the right side. If a window is closed or hidden, you can bring it to the foreground by selecting a toolbar icon or Window menu item, or by using shortcut keys. Each toolbar icon is identified by a tool tip that is displayed when the mouse pointer moves over the icon. Navigation tree, and dynamic position and state preferences, such as hidden or visible, are stored on the local file system. Each time you start the GUI, the saved preferences are used.

External windows

A window in the GUI can be used outside the GUI if you select the window and choose Move To External Window from the Window menu or from the menu that is displayed when you right-click on the window title bar.

External windows are managed by the operating system rather than the 5620 SAM. They maintain the window icon that is used within the GUI and are placed into a group of open 5620 SAM windows on the operating system task bar. Any windows launched from an external window appear as separate external windows. The 5620 SAM GUI task bar does not display external windows, but they can be viewed and brought to the front using the Window menu. The Window menu also contains options to Close All Internal Windows or Close All External SAM Windows.

Note — An external window cannot be moved back into the 5620 SAM GUI. You must close the external window and re-open it in the GUI.

Forms

5620 SAM forms are used to do the following:

- configure device and 5620 SAM parameters
- display the status of an object
- perform FCAPS operations

A form can be displayed anywhere in the GUI. A newly opened form is displayed in the foreground. You can do the following:

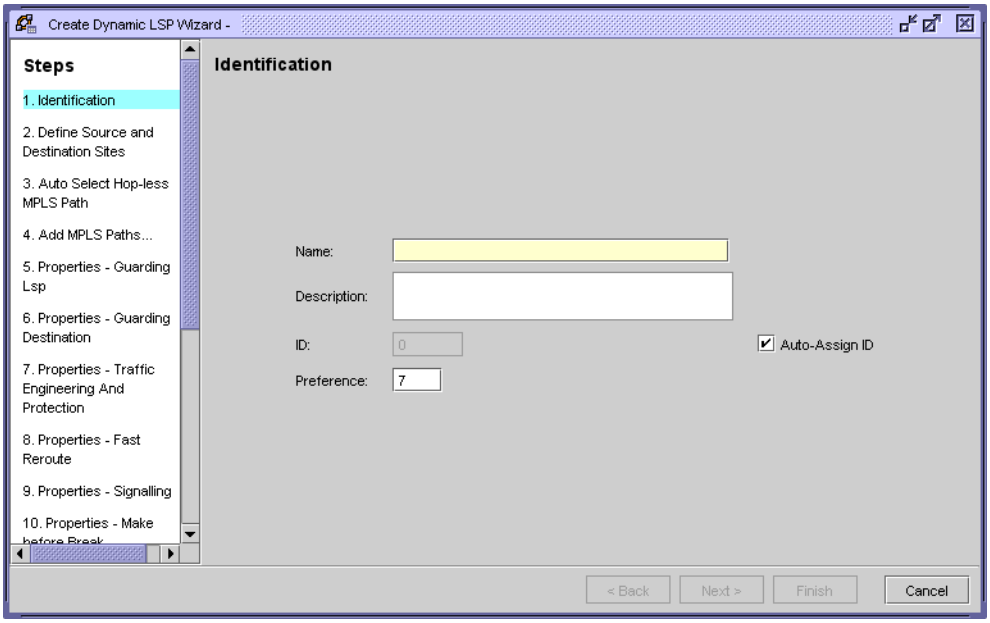
- organize forms according to operator preference
- compare information on multiple open forms
- navigate quickly to another open form by choosing the form from a list

A form has a title bar that displays object information. The displayed object name is the name specified during object creation. If the object is not named, a default name is used. When a form is minimized, a tool tip displays the title bar information. The Window menu lists the open forms.

Some configuration activities lead the operator through a series of forms, each of which represents a step in the configuration process. Such a form is called a step form. You must click on the Next button to proceed to the next step. Figure 2-2 shows the first step in a step form sequence. When the configuration sequence is complete, you must click on the Finish button to commit the changes. Each step must be performed to complete the configuration activity.

Note — Some steps open a new step form. You must complete the steps in the new form before you can return to the previous form. After you click on the Finish button, the previous form reappears.

Figure 2-2 Step form



Using the navigation tree toolbar

The navigation tree toolbar consists of the view selector, the Make Root At Top Level button, and the Copy to Clipboard button. Figure 2-1 shows the navigation tree toolbar. See Procedure 2-17 for information about using the Copy to Clipboard button.

Make Root At Top Level button

The Make Root At Top Level button restores the navigation tree to the default root. For example, in the equipment view, if you redefine the root of the tree as a card and click on the Make Root At Top Level button, the navigation tree refreshes with the default root, which is the network. The Make Root At Top Level button is enabled only when the root is not the network. The Make Root At Top Level button is available only for the equipment view.

Make Root and Make Root In New Tree menu options

The navigation tree contextual menus provide Make Root and Make Root In New Tree menu options that allow you to redefine the root of the tree. These menu options, along with the Make Root At Top Level button, help orient users in densely populated navigation trees. The menu options are available only for the equipment view. See chapter 17 for more information about using these functions.

Copy to Clipboard button and Clipboard window

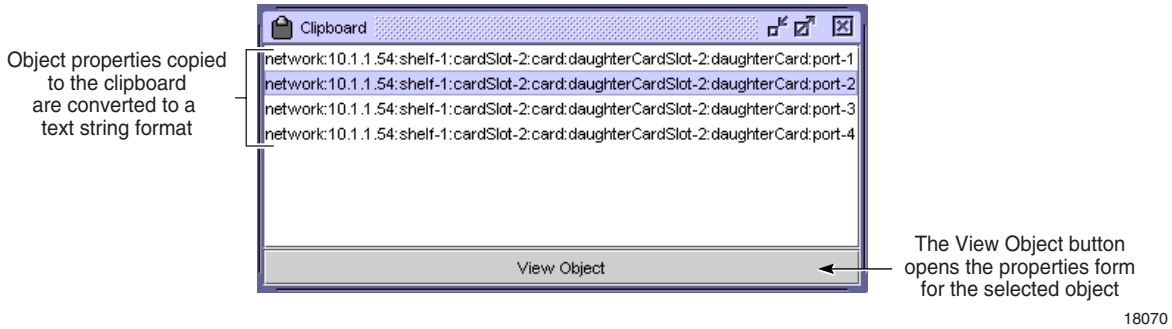
Using the Copy to Clipboard button on the navigation tree toolbar, you can copy the identifier of one or more 5620 SAM objects to the Clipboard window. You can then open the Clipboard window from the Application menu to retrieve the identifier and paste it into another application. You can also choose an object identifier in the Clipboard window and click on the View Object button to open the object properties form. The elements in an object identifier are delimited using colons (:).

The Copy to Clipboard button is in the equipment window, on list forms, and on the list tabs of properties forms. You can use the button to copy configurable and read-only text fields. The button is enabled when at least one object is selected.

Note — The Clipboard window keeps the object identifier from only the most recent copy action. After you copy an object identifier to the clipboard, if you click on the Copy to Clipboard button again to copy another object identifier, the second copy action overwrites the previously copied identifier in the Clipboard window.

Figure 2-3 shows the Clipboard window. See Procedure 2-17 for more information about using the clipboard function.

Figure 2-3 Clipboard window



Paste from Clipboard button

After using the Copy to Clipboard button to copy object identifiers to the Clipboard window, you can use the Paste from Clipboard button on the physical link properties form to set multiple parameters at one time using the copied object identifiers. See Procedure 4-36 for information about using the Paste from Clipboard button.

Localized language support

The 5620 SAM GUI supports localized language display. Localized language display, also known as internationalization, displays 5620 SAM GUI text in a specified language. The localized language setting applies to most 5620 SAM GUI objects except system components and database objects. Contact Alcatel-Lucent support for more information about localized language support.

Note 1 — The 5620 SAM supports localized language settings using predefined strings, and does not translate data to different languages.

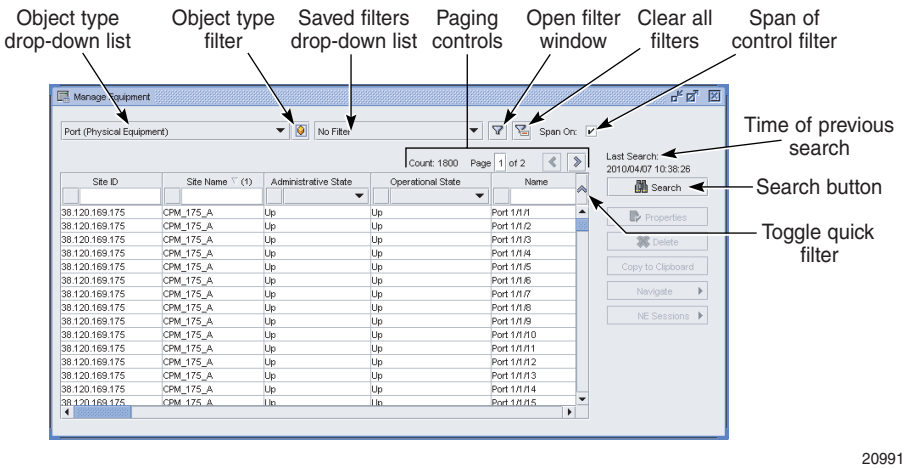
Note 2 — The 5620 SAM-O does not support language localization.

2.2 Using search functions

You can search for many types of objects using list forms, maps, and the navigation tree. After you perform a search, a list form or map enables you to manage the results, for example, view or edit object information, or delete objects. Figure 2-4 shows a filterable list form that displays the following above the listed items:

- number of returned search items
- time of the most recent search
- filter controls for refining the list of returned search items
- paging controls for browsing through multiple pages of returned search items

Figure 2-4 Filterable list form



20991

When the number of search results exceeds the allowed limit, the 5620 SAM displays a dialog box that indicates the number of results returned. You cas use filter options to refine the search criteria and limit the search results.

A search returns one page of results at a time. You can configure the number of items per page on the User Preferences form. The paging controls on a list form become active when the number of items returned exceeds the page limit. You can use these controls to move sequentially through the pages of listed information or jump directly to a specific page.

You can save and reuse multiple search filters in list forms and maps. Only the saved filters of the current object type and ancestor types are available. You can use an advanced filter form to refine the search criteria using literal values, and different kinds of operators, such as arithmetic and Boolean.

Note — A tab that lists timestamped information, such as the Statistics tab of a 5620 SAM properties form, contains a default saved filter for statistics collected in the most recent time period, for example, the last hour. The time period depends on the type of object specified in the object type drop-down list.

See chapter 4 for information about creating map filters.

Using search filters

When you perform a search from a list form, you can configure filters. A filter is based on a combination of attributes, functions, and values. When searching for objects with an ID value, you can search based on LESS THAN, EQUAL TO, or GREATER THAN. For text-type parameters, you can use advanced search functions, such as EQUALS or CONTAINS. Consider the following.

- You can set filters based on letters, numbers, and special characters.
- The search filters are typically case-insensitive; a search on ‘ABC’ and ‘abc’ returns the same list. WILDCARD searches, however, are case-sensitive.

Table 2-1 describes the operation of 5620 SAM search functions that are available for different parameter types.

Table 2-1 Search functions

Parameter type	Operator	Description
A parameter that has a pre-determined value, such as Administrative State	EQUALS	When set to EQUALS, the search returns only items that equal the value; for example, Administrative State set to ‘Down”.
	NOT EQUAL	When set to NOT EQUAL, the search returns only items that do not match the selected criteria.

(1 of 2)

Parameter type	Operator	Description
A parameter that has multiple pre-determined property values, such as State Cause	MATCHES ALL	When set to MATCHES ALL, the search returns only items that equal the property values selected; for example, if Monitored Access(es) Down and Site(s) Down are selected, the search returns only items that match all of the selected property values.
	MATCHES ANY	When set to MATCHES ANY, the search returns only items that equal at least one of the property values selected; for example, if Monitored Access(es) Down and Site(s) Down are selected, the search returns only items that match one or more of each of the selected property values.
A parameter that has an ID, such as Service ID	EQUALS	When set to EQUALS, the search returns only items that equal the value; for example, Administrative State set to 'Down".
	NOT EQUAL	When set to NOT EQUAL, the search returns only items that do not match the specified criteria.
	GREATER OR EQUAL	When set to GREATER OR EQUAL, the search returns only items that have a value greater than or equal to the specified criteria.
	GREATER THAN	When set to GREATER THAN, the search returns only items that have a value greater than the specified criteria.
	LESS OR EQUAL	When set to LESS OR EQUAL, the search returns only items that have a value less than or equal to the specified criteria.
	LESS THAN	When set to LESS THAN, the search returns only items that have a value less than the specified criteria.
A parameter that has a value specified by the user, such as Description or Last Time Detected	EQUALS	When set to EQUALS, the search returns only items that equal the value; for example, Description set to 'In Service".
	APPROXIMATELY EQUAL	When set to APPROXIMATELY EQUAL, which applies to timestamp fields, such as the Last Time Detected field in the Alarm Window, the search returns only items that match the specified time criterion, which you can specify using 1m resolution.
	NOT EQUAL	When set to NOT EQUAL, the search returns only items that do not match the selected criteria.
	IN THE PAST	When set to IN THE PAST, which applies to timestamp fields, such as the Last Time Detected field in the Alarm Window, the search returns only items that have a timestamp that is between the specified time and the present. Click on the clock icon beside the column heading filter field to specify a time criterion.
	CONTAINS	When set to CONTAINS, the search uses the entered value as a wildcard with wildcards automatically added to the end of the specified string, and returns only items where the parameter value is contained. For example, a Description CONTAINS search of 'AB' returns 'ABC Industries' and 'Calgary, AB'. Any empty CONTAINS search returns all items.
	WILDCARD	When set to WILDCARD, you can use the ? character as a single-character wildcard, and * as a multi-character wildcard. For example, a Description WILDCARD search of 'VPRN ?' returns 'VPRN 4' and 'VPRN 8', but not 'VPRN Texas'.

(2 of 2)

Searches using Boolean operators

You can perform advanced searches that use multiple criteria to obtain more precise results. Boolean operators are used to limit and expand searches to the criteria that are specified in the search expressions. Boolean operators can be nested to combine several search expressions into one search expression.

Table 2-2 lists and describes the Boolean search operators.

Table 2-2 Boolean search operators

Boolean operator	Description
AND	When set to AND, the search returns only items that meet all of the specified search criteria.
OR	When set to OR, the search returns only items that meet at least one of the specified search criteria.
NOT	When set to NOT, the search returns only items that do not meet the specified search criteria.

Invalid attributes or values

When a saved search filter contains attributes or values that are not available for the object being searched, the invalid attributes or values are displayed in red text in the filter window. As long as invalid attributes or values exist, the Save button of the filter window are disabled. When a filter with invalid attributes or values is applied, the invalid attributes are not evaluated. For information about using the filter window, see Procedure 2-27.

When a saved search filter contains an invalid attribute, the attribute, function, and value are all displayed in red text in the filter window. The attribute are is surrounded by "**". Both the attribute and value are displayed as a best effort string and may not be internationalized.

When an invalid attribute is selected, the Attribute drop-down is displayed a best effort string that may not be internationalized. If the attribute is not recognized, the Functions drop-down and the Value field display only the corresponding values that are displayed in the filter window. These values cannot be changed until a different attribute is chosen from the Attribute drop-down, at which point they are updated accordingly.

When a saved search filter contains only an invalid value, only the value itself is displayed in red text. The value is surrounded by "**" and may not be internationalized. The Value drop-down does not display a value, but is populated with valid values that can be used to update the filter.

When a saved search filter contains invalid attributes, the filter name is displayed in red text in the saved filters drop-down of a list form. When a filter with invalid attributes is applied from the saved filters drop-down, the invalid attributes are not evaluated. For information about using the saved filters drop-down list, see Procedure 2-38.

Preset filters

When a preset filter is ready to be applied, the saved filters drop-down menu displays an italicized No Filter. Opening the filter window displays the preset filter. Clicking on the Search button applies the filter, and clicking on the Clear All Filters button clears the filter.

Span of control filters

A 5620 SAM GUI user can filter the objects that a map or list form displays, based on the user span of control. By default, the GUI displays only the objects that are in the View Access and Edit Access spans of the user.

Most 5620 SAM list forms contain a configurable Span On parameter. When the parameter is enabled, the displayed objects are limited to the Edit Access span objects. The parameter setting overrides, on the current form only, the global span of control filter setting on the User Preferences form. When the Span On parameter is displayed on a list form that allows filter creation, the associated filter form contains a drop-down menu that has the following options:

- Span: On—Only Edit Access span objects are displayed.
- Span: Off—View Access and Edit Access span objects are displayed.
- Span: User Preference—The User Preferences span filter setting determines which objects are displayed.

The Span On parameter setting in a list form defaults to the User Preferences span filter setting. 5620 SAM topology maps, however, do not contain the Span On parameter; instead, they automatically filter the NEs according to the User Preferences span filter setting.

See chapter 8 for information about spans of control. See Procedure 2-24 for information about configuring the global span of control filter on the User Preferences form.

2.3 5620 SAM GUI workflow

1. Start the 5620 SAM GUI and manage objects using 5620 SAM main menu options, the alarm and map windows, and the navigation tree. See Section 2.4.
2. Configure the way that the GUI operates for one or more users. See Section 2.5.
3. Use list forms to perform filtered searches that return information, and optionally save the filters and listed information to files. See Section 2.6.

2.4 Basic 5620 SAM GUI operation procedures

The following procedures describe how to operate and navigate the 5620 SAM GUI.

Procedure 2-1 To start the 5620 SAM client GUI on a Windows single-user client station

Perform this procedure to start the 5620 SAM single-user client software on a Windows station and begin using the client GUI.

Note 1 — You can have more than one client installed on a station, but you can run only one client instance at a time. For example, you can have a Release 6.0 R1 client and a Release 7.0 R1 client running on the same station, but you cannot have two Release 7.0 R1 clients running on the same station.

Note 2 — The user that starts a 5620 SAM Windows client must be one of the following:

- the user that installed the client software
- a user with sufficient permissions on the client files and directories, such as a local administrator

1 To start the client GUI using a web browser, perform the following steps.

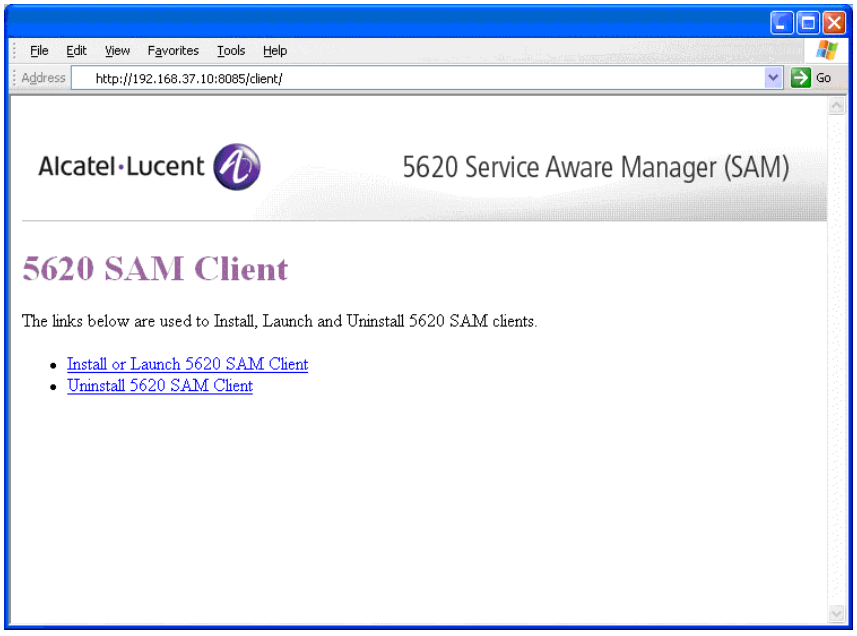
i Navigate to the following URL on the 5620 SAM main server:

http://*server*:8085/client

where *server* is the IP address or hostname of the 5620 SAM main server

The page shown in Figure 2-5 is displayed.

Figure 2-5 5620 SAM client page



ii Click on the “Install or Launch 5620 SAM Client” link.

iii If you did not use a web browser to install the client, a form opens and prompts you for the client installation location. Use the form to specify the client installation directory, for example, C:\5620sam\client.

iv The 5620 SAM login form opens. Go to step 5.

2 To start the client GUI using a desktop shortcut, perform the following steps.

i Double-click on the 5620 SAM Client App icon on the Windows desktop. The 5620 SAM client login form opens.

ii Go to step 4.

3 To start the client GUI using a CLI, perform the following steps.

Note — Using a CLI to start the client GUI allows you to specify one or more client startup options.

i Open a command window.

ii Navigate to the 5620 SAM client installation directory. Enter the following commands at the CLI prompt in the order shown:

drive_ID ↵

cd *install_dir*\nms\bin ↵

where
drive_ID is the drive on which the 5620 SAM client is installed, for example, C:
install_dir is the 5620 SAM client installation location, typically \5620sam\client

iii Enter the following at the CLI prompt to start the 5620 SAM client using one or more startup options:

nmsclient.bat *option* ↵

where *option* is one or more of the startup options listed in Table 2-3

For example, to force a client update, enter the following:

nmsclient.bat update ↵

Table 2-3 5620 SAM client startup options for Windows

Option	Description
nms_version	Displays the client software version
baseLocale	Starts the client using the base OS locale for string resources such as language, number, date, and time formats
secure	Starts the client using HTTPS to connect to the server

(1 of 2)

Option	Description
server <*server*:*port*;*server*:*port*...>	Starts the client and specifies the 5620 SAM servers that the client is to check for an update where *server* is an IP address or a DNS name *port* is an HTTP or HTTPS port on the server
update	Starts the client and forces the download and installation of the updated client files. This overrides the local client configuration to ensure that the client and server configurations match. This option is useful for restoring a corrupted client installation. You can restore local configuration variances after the update.
retryCount	Starts the client and specifies the number of times to attempt to download a client update
noupdate	Starts the client without performing an update. This option is useful for preserving a specific client configuration that differs from the server configuration.
keepConfig	Starts the client and performs an update, but does not permit the overwriting of the nms-*.xml configuration files in the *install_dir*\nms\config directory where *install_dir* is the 5620 SAM client installation directory, typically C:\5620sam\client After this option is specified, it remains in effect until the client is started using the "update" option, which then remains in effect.
keepSpecified	Specifies that the files listed in *install_dir*\nms\config\keepFile.txt are not to be overwritten during a client update where *install_dir* is the 5620 SAM client installation location, typically C:\5620sam\client The keepFile.txt file must contain only one file entry per line, and each entry must be an absolute file path.
connectTimeout [*timeout*]	Specifies a timeout value, in ms, that the client uses for a download-server connection attempt. If the client cannot connect to a server within the timeout period, the operation is aborted. The default is 3000, which specifies 3s. The maximum connection timeout in Windows is 20s.
readTimeout [*timeout*]	Specifies a timeout value, in seconds, that the client uses for a download-server file read attempt. If the client cannot obtain a server response to a file request within the timeout period, the file request is aborted. The default is 3000, which specifies 3s. The maximum read timeout in Windows is 20s.
help	Displays the nmsclient.bat usage information and options

(2 of 2)

The 5620 SAM client login form opens.

4 Choose the 5620 SAM server that you want to log in to from the Server drop-down list.

Note — Before the login form can display multiple servers in the Server drop-down list, you must configure the client to support multiple server options. See chapter 5 for more information.

5 Enter the Login name and Password information required for the server.

Note 1 — If this is the first time that a client connects to the server, you must use admin as the Login Name. Contact your Alcatel-Lucent technical support representative for the default 5620 SAM user account information.

Note 2 — The login name and password used depend on whether client GUI users are authenticated locally or remotely, as determined by the system administrator. Use the login name and password provided by your system administrator. See chapter 8 for more information.

6 Click on the Login button. The 5620 SAM GUI opens.

7 If the 5620 SAM server is at a higher major release level than the client, the auto-update function may display a dialog box that asks whether you want to remove an older version of JRE. If this occurs, perform one of the following.

a If there is no longer a need for the client to connect to a main server at the older 5620 SAM release level, click on the Yes button. The older JRE version is removed.

b If the client is required for connecting to a a main server at the older 5620 SAM release level, click on the No button. The older JRE version is retained.

If you have trouble opening the GUI, see the Troubleshooting 5620 SAM Client GUIs chapter of the *5620 SAM Troubleshooting Guide*.

Procedure 2-2 To start the 5620 SAM client GUI on a Solaris single-user client station

Perform this procedure to start the 5620 SAM single-user client software on a Solaris station and begin using the client GUI.

Note 1 — You can have more than one client installed on a station, but you can run only one client instance at a time. For example, you can have a Release 6.0 R1 client and a Release 7.0 R1 client running on the same station, but you cannot have two Release 7.0 R1 clients running on the same station.

Note 2 — The user that starts a 5620 SAM Solaris client must be one of the following:

- the user that installed the client software
- another user that has read, write, and execute permissions on the client files and directories

1 To start the client GUI using a web browser, perform the following steps.

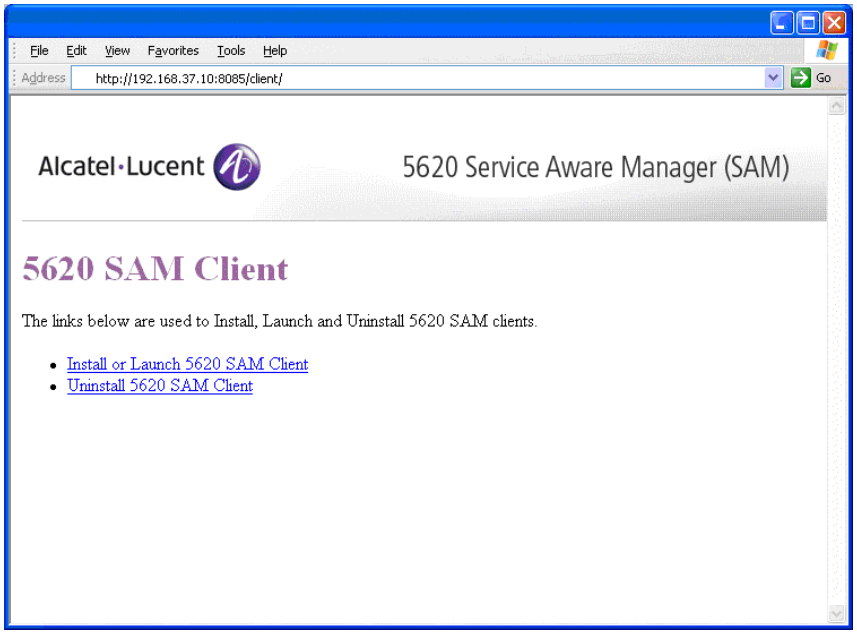
i Navigate to the following URL on the 5620 SAM main server:

http://*server*:8085/client

where *server* is the IP address or hostname of the 5620 SAM main server

The page shown in Figure 2-6 is displayed.

Figure 2-6 5620 SAM client page



ii Click on the “Install or Launch 5620 SAM Client” link.

iii If you did not use a web browser to install the client, a form opens and prompts you for the client installation location. Use the form to specify the current client installation directory, for example, /opt/5620sam/client.

iv The 5620 SAM login form opens. Go to step 5.

2 To start the client GUI using a desktop shortcut, perform the following steps.

i Double-click on the 5620 SAM Client App icon on the desktop. The 5620 SAM client login form opens.

ii Go to step 4.

3 To start the client GUI using a CLI, perform the following steps.

Note — Using a CLI to start the client GUI allows you to specify one or more client startup options.

i Open a bash console window on the client station.

ii Enter the following at the CLI prompt to navigate to the 5620 SAM client installation directory:

cd *install_dir*/nms/bin ↵

where *install_dir* is the 5620 SAM client installation location, typically /opt/5620sam/client

iii To specify one or more client startup options, enter the following at the CLI prompt:

./nmsclient.bash *option* ↵

where *option* is one or more of the startup options listed in Table 2-4

For example, to force a client update, enter the following:

./nmsclient.bash update ↵

Table 2-4 5620 SAM client startup options for Solaris

Option	Description
nms_version	Displays the client software version
baseLocale	Starts the client using the base OS locale for string resources such as language, number, date, and time formats
secure	Starts the client using HTTPS to connect to the server
server <*server*:*port*;*server*:*port*...>	Starts the client and specifies the 5620 SAM servers that the client is to check for an update where *server* is an IP address or a DNS name *port* is an HTTP or HTTPS port on the server

(1 of 2)

Option	Description
update	Starts the client and forces the download and installation of the updated client files. This overrides the local client configuration to ensure that the client and server configurations match. This option is useful for restoring a corrupted client installation. You can restore local configuration variances after the update.
retryCount	Starts the client and specifies the number of times to attempt to download a client update
noupdate	Starts the client without performing an update. This option is useful for preserving a specific client configuration that differs from the server configuration.
keepConfig	Starts the client and performs an update, but does not permit the overwriting of the nms-*.xml configuration files in the *install_dir*/nms/config directory where *install_dir* is the 5620 SAM client installation directory, typically /opt/5620sam/client After this option is specified, it remains in effect until the client is started using the "update" option, which then remains in effect.
keepSpecified	Specifies that the files listed in *install_dir*/nms/config/keepFile.txt are not to be overwritten during a client update where *install_dir* is the 5620 SAM client installation location, typically /opt/5620sam/client The keepFile.txt file must contain only one file entry per line, and each entry must be an absolute file path.
connectTimeout [*timeout*]	Specifies a timeout value, in ms, that the client uses for a download-server connection attempt. If the client cannot connect to a server within the timeout period, the operation is aborted. The default is 3000, which specifies 3s.
readTimeout [*timeout*]	Specifies a timeout value, in seconds, that the client uses for a download-server file read attempt. If the client cannot obtain a server response to a file request within the timeout period, the file request is aborted. The default is 3000, which specifies 3s.
help	Displays the nmsclient.bash usage information and options

(2 of 2)

The 5620 SAM client login form opens.

4 Choose the 5620 SAM server that you want to log in to from the Server drop-down list.

Note — Before the login form can display multiple servers in the Server drop-down list, you must configure the client to support multiple server options. See chapter 5 for more information.

5 Enter the Login name and Password information required for the server.

Note 1 — If this is the first time that a client connects to the server, you must use admin as the Login Name. Contact your Alcatel-Lucent technical support representative for the default 5620 SAM user account information.

Note 2 — The login credentials that are required depend on whether local or remote user authentication is used for the GUI client. Use the login name and password provided by your system administrator. See chapter 8 for more information.

6 Click on the Login button. The 5620 SAM GUI opens.

7 If the 5620 SAM server is at a higher major release level than the client, the auto-update function may display a dialog box that asks whether you want to remove an older version of JRE. If this occurs, perform one of the following.

a If there is no longer a need for the client to connect to a main server at the older 5620 SAM release level, click on the Yes button. The older JRE version is removed.

b If the client is required for connecting to a a main server at the older 5620 SAM release level, click on the No button. The older JRE version is retained.

If you have trouble opening the GUI, see the Troubleshooting 5620 SAM Client GUIs chapter of the *5620 SAM Troubleshooting Guide*.

Procedure 2-3 To start the 5620 SAM client GUI through a client delegate server

Perform this procedure to open a 5620 SAM client GUI using the 5620 SAM client delegate software on another station.

1 If you are not in the same physical facility as the client delegate server, log in to the facility using the appropriate third-party access tool, for example, Citrix software.

2 Log in to the client delegate server using an account with local user privileges.

3 Open a bash console window on the client delegate server station.

4 Use the appropriate UNIX commands to redirect the display to the station that you are using.

5 Enter the following at the CLI prompt to navigate to the 5620 SAM client installation directory on the client delegate server:

cd *install_dir*/nms/bin ↵

where *install_dir* is the 5620 SAM client installation location, typically /opt/5620sam/client

6 Perform step 3 of Procedure 2-2.

Note — You must be logged in as the samadmin user on a client delegate server to use a client startup option that updates the client software configuration or upgrades the client software. If you attempt such an operation as a user other than samadmin, the operation fails.

7 Enter the Login name and Password information on the 5620 SAM client login form.

Note 1 — If this is the first time that a client connects to the server, you must use admin as the Login Name. Contact your Alcatel-Lucent technical support representative for the default 5620 SAM user account information.

Note 2 — The login credentials that are required depend on whether local or remote user authentication is used for the GUI client. Use the login name and password provided by your system administrator. See chapter 8 for more information.

8 Click on the Login button. The 5620 SAM client GUI opens.

If you have trouble opening the GUI, see the Troubleshooting 5620 SAM Client GUIs chapter of the *5620 SAM Troubleshooting Guide*.

Procedure 2-4 To view the 5620 SAM user documentation from the 5620 SAM GUI

Perform this procedure to open the 5620 SAM user documentation from the client GUI. The following must be present on the 5620 SAM client or client delegate server station:

- Adobe Reader 4.0 or later
- a browser application

1 Choose Help→5620 SAM User Documentation from the 5620 SAM main menu. A browser window opens to display an HTML index of the available documentation.

2 Scroll through the list of available documentation. See the Preface for descriptions of the documents.

3 Click on a document link to open the document. The document opens.

You can:

- Open the *5620 SAM User Guide* in Adobe Reader, then click on the blue links in the document to view the detailed information in the *5620 SAM Parameter Guide*.
- Print the documents for future reference.
- Use the information in the documentation to write NOC-specific procedures.
- Use Adobe Reader to search for a word or phrase in the PDF file.

Procedure 2-5 To close the 5620 SAM GUI

1 Choose Application→Exit from the 5620 SAM main menu. A dialog box appears.

2 Click on the Yes button. The GUI application closes.

Procedure 2-6 To configure the default client time zone

Perform this procedure to specify which time zone the 5620 SAM client will use by default.

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Default Client Time Zone parameter.

3 Click on the OK button. The User Preferences form closes and a dialog box appears.

4 Click on the OK button.

Procedure 2-7 To configure the current client time zone

Perform this procedure to specify which time zone the 5620 SAM client will use currently.

1 Click on the Current Client Time Zone button in the bottom right hand corner of the GUI. The Current Client Time Zone form opens.

2 Perform one of the following:

- **a** Select Use Default Client Time Zone.
- **b** Select Use Specific Client Time Zone and choose a time zone from the list.

3 Click on the OK button. The Current Client Time Zone form closes and a dialog box appears.

4 Click on the OK button.

Procedure 2-8 To open the navigation tree or alarm window

The navigation tree and alarm window position and state preferences are stored in the local file system so that each time the GUI is opened using the same user account, the saved preferences are used.

1 Start the 5620 SAM client GUI.

2 Open a hidden window or bring these windows to the foreground using one of the following methods:

- **a** Choose the Navigation Tree or Alarm Window icon from the toolbar.
- **b** Choose *View*-Network or Alarm Window from the Window menu.
- **c** Use the Navigation Tree or Alarm Window shortcut key.
- **d** Choose the icon that represents the window from the task bar. The task bar is located just above the status bar.

Procedure 2-9 To go to a window

1 Perform one of the following:

- **a** Copy a window identifier link to the clipboard. See Procedure 2-17 for more information.
- **b** Save a window identifier link to the clipboard. See Procedure 2-18 for more information.

2 Choose Application→Go To Window from the 5620 SAM main menu. The Go To Window window opens.

3 Click on the Paste button or press CTRL+V. The window link identifier appears in the Label area.

4 Perform one of the following:

- **a** Click on the OK button. The Go To Window window closes and the window specified in step 1 opens.
- **b** Click on the Apply button. The window specified in step 1 opens.

Procedure 2-10 To use menus, the toolbar, or shortcuts

1 Start the 5620 SAM GUI.

2 Perform one of the following to open an object.

- **a** Choose an option from the main menu. A shortcut icon for the menu option is shown beside the option text.
- **b** Click on the menu equivalent in the toolbar. Scroll over the toolbar icons to view a tool tip that describes the icon function. See Procedure 2-20 for information about modifying or hiding the toolbar.
- **c** By typing the appropriate ALT+*Key* shortcut; the underlined letter in a main menu item is the shortcut key. For example, ALT+P opens the Policies menu.

Note — Using the CTRL+F4 key to close a form or window may cause problems if the parent form is open. Alcatel-Lucent recommends that to close a form or window, you use the Close button and respond to the subsequent prompt, or click on the X button in the top right corner of the form or window.

Procedure 2-11 To use menus, windows, and forms to configure or view parameters

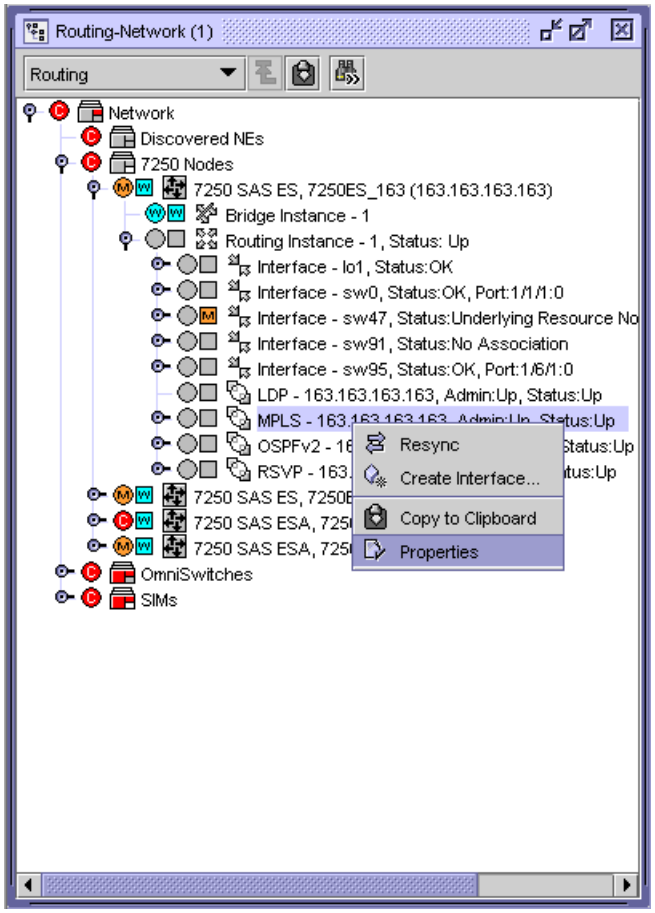
1 Start the 5620 SAM client GUI.

2 Open a configuration form using one of the following methods.

- **a** Double-click on the lowest-level navigation tree object to open the object properties form. When you double-click on an object that has child objects, the child object is revealed; when you double-click on an object that has no child objects, the object properties form opens.
- **b** Choose the appropriate 5620 SAM main menu or submenu option.
- **c** Double-click on an object, for example, a customer in a list of customers.
- **d** Click on the task bar icon that represents the form.
- **e** Right-click on an object in the navigation tree or Alarm Window and choose the appropriate option from the contextual menu.

  Figure 2-7 shows an example of a right-click contextual menu in the navigation tree.

Figure 2-7 Right-click contextual menu example



The appropriate form opens.

3 Configure or view the parameters on the form, as required, using the following methods.

Note — A parameter that has a yellow background is mandatory and must be configured before you can go to the next form or apply the changes on the current form.

a Enter information beside the parameter, as appropriate. For example, type in text to configure the Description parameter.

b Use the drop-down menu to choose an option from a list. For example, choose Access as the port mode on a port configuration form.

c If the configuration form is a step form, follow the form prompts.

d Double-click an object in a row to open a new view or set of configurations. For example, from a list of ports double-click on a row to open the configuration form for that port.

e Right-click on an object in the navigation tree to display additional contextual menu choices, as shown in Figure 2-7.

See the *5620 SAM Parameter Guide* for a list of the configurable parameters.

4 Click on the Apply button to save the configuration changes without closing the form.

5 Click on the appropriate button to complete the configuration.

a Click on the OK button to save the changes and close the form, if the form is other than a step form.

b Click on the Finish button to save the changes in a step form.

c Click on the Turn Up button to activate the object.

d Click on the Shut Down button to deactivate the object.

e Click on the Cancel button to close the form without saving the changes.

f Click on the Close button to close the form without saving the changes.

Note — Using the CTRL+F4 key to close a form or window may cause problems if the parent form is open. Alcatel-Lucent recommends that to close a form or window, you use the Close button and respond to the subsequent prompt, or click on the X button in the top right corner of the form or window.

g The Resync button to ensure that the 5620 SAM and managed devices are synchronized. Resynchronization does not affect the contents of the historical statistics database.

Procedure 2-12 To arrange multiple open forms

1 To arrange multiple open forms so that they overlap, choose Window→Cascade from the 5620 SAM main menu. The forms are displayed in the top left area of the GUI with the form that is farthest to the right in the foreground.

2 To arrange multiple open forms so that they do not overlap, perform one of the following.

- **a** Choose Window→Tile Vertical from the 5620 SAM main menu. The forms are displayed beside each other.
- **b** Choose Window→Tile Horizontal from the 5620 SAM main menu. The forms are displayed above each other.
- **c** Choose Window→Tile Square from the 5620 SAM main menu. The forms are displayed beside and above each other to fill the GUI workspace.

3 To move an open form to the foreground, perform one of the following.

- **a** Click on the task bar icon that represents the open form.
- **b** Choose Window→*form_name* from the 5620 SAM main menu

  where *form_name* is the name of the form that you want in the foreground

Procedure 2-13 To close one or all open forms

Note — When there is unsaved information on a form, you are prompted to save the changes before you close the form.

1 To close one form, perform one of the following.

- **a** Click on the X in the top-right corner of the form.
- **b** Click on the Close button.
- **c** Right-click on a form in the task bar and choose Close from the contextual menu.

2 To close all open forms, choose Window→Close All from the 5620 SAM main menu.

Procedure 2-14 To configure the 5620 SAM Task Manager

The Task Manager allows 5620 SAM operators to monitor progress of operational tasks. Only the 5620 SAM administrators can configure task monitoring parameters. The Task Manager monitors the following:

- all write operations that are performed from the 5620 SAM GUI; for example, when you click on the Apply or OK buttons
- all write operations that are performed using the OSSI
- some read operations; for example, when you click on the Resync or Collect All buttons

Note — The Task Manager is operational with the default values.

1 Log in to the 5620 SAM main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config for Solaris, or C:\5620sam\server\nms\config for Windows.

3 Open the nms-server.xml file using a text editor.

4 Find and configure the parameters to fit your operational requirements.

- maxNumRetainedTasks
- numTasksToPurgeWhenFull
- successfulTasksPurgeInterval
- failedTasksPurgeInterval

Note — If one or more of the parameters are changed from their default values, you must restart the 5620 SAM server for the changes to take effect.

5 Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config for Solaris, or C:\5620sam\client\nms\config for Windows.

6 Open the nms-client.xml file using a text editor.

7 If required, configure the autoRefreshInterval parameter. The parameter does not take effect until the 5620 SAM client is restarted.

8 If required, export a report to a file, as described in Procedure 2-33.

9 If required, save the table preferences, as described in section 2.2.

10 Close the form. See Procedure 2-15 to view the Task Manager.

Procedure 2-15 To view the 5620 SAM Task Manager

See Procedure 2-14 to configure the Task Manager.

Note — You can send the tasks that the Task Manager displays to a file using the OSSI findToFile method. See the *5620 SAM-O OSS Interface Developer Guide* guide for more information.

1 Choose Application→Task Manager from the 5620 SAM main menu. The Task Manager form opens.

Note — The Task Manager button appears by default in the toolbar under the 5620 SAM main menu. You can also click on the Task Manager button to open the Task Manager form. Figure 2-8 shows the Task Manager button.

Figure 2-8 Task Manager button

The All Users check box appears for only the 5620 SAM administrators. If you are a 5620 SAM administrator or a user with an assigned administrator scope of command role, go to step 2 to monitor tasks for all users. Otherwise, go to step 3.

2 Enable the All Users check box to monitor operations that are performed in the 5620 SAM server by all 5620 SAM users. The default is Disabled.

3 If required, configure the filter and click on the Search button. The following appear in the Task Manager:

- all write operations that are performed from the 5620 SAM GUI; for example, when you click on the Apply or OK buttons
- all write operations that are performed using the OSSI
- some read operations; for example, when you click on the Resync or Collect All buttons

Note — The Task Manager automatically refreshes when the value of the autoRefreshInterval parameter is reached. The default is 20 s. You can also click on the Search button to refresh the list of tasks.

4 Double-click on a task to view more information about the task. The Task - Top Level window opens.

5 Click on the Tree tab button to view a hierarchical display of the tasks.

6 Click on the Sub-Tasks tab button to view the sub-tasks that are associated with the task.

7 Close the form.

Procedure 2-16 To send a text message

1 Choose Application→Text Message from the 5620 SAM main menu. The Text Message window opens.

2 Type the text message in the text area.

Note — You can also press CTRL+V to paste information from the clipboard into the text area. For example, pasting a window link identifier creates a link which the recipient can click to launch the window. For more information about copying to the clipboard, see Procedures 2-17 and 2-18.

3 Click on the Send To... button. The Select Session window opens.

4 If necessary, configure the filter criteria.

5 Click on the Search button. The results list is displayed based on the filter.

6 Choose a session from the list and click on the OK button.

Procedure 2-17 To use the clipboard

1 Select one or more objects to copy from one of the following locations.

- **a** To copy objects from the equipment view of the navigation tree, go to step 2.
- **b** To copy objects from a generated or displayed list, go to step 2.
- **c** To copy objects from a read-only field on a configuration form, go to step 6.

2 Click on the Copy to Clipboard button. The object properties are copied to the clipboard.

3 Choose Application→Clipboard from the 5620 SAM main menu. The Clipboard window opens displaying the copied object properties in a text string format.

4 Perform one of the following:

a Copy and paste the properties text string to an external application.

i Select the properties text string that you want to copy and press CTRL+C.

Only one text string can be selected and copied at a time.

ii Paste the properties text string into an external application.

b View the property form for a copied object.

i Select the properties text string for the object that you want to view.

ii Click on the View Object button. The properties form for the object opens.

5 Repeat steps 1 to 4 to copy additional objects, or close the Clipboard window.

For information about using the clipboard function to create physical links, see Procedure 4-36.

6 Highlight a read-only field to copy and press CTRL+C.

7 Paste the copied read-only field into another form or application by pressing CTRL+V.

Note — You cannot copy a password field.

Procedure 2-18 To save a window to the clipboard

1 Open a configuration form.

2 Choose Application→Save Window To Clipboard from the 5620 SAM main menu. The window identifier link is saved to the clipboard.

2.5 5620 SAM GUI configuration procedures

The following procedures describe how to configure 5620 SAM GUI operation.

Procedure 2-19 To configure the GUI inactivity timeout

A 5620 SAM user with an admin scope of command role can configure a GUI inactivity check that applies to all client GUIs, or to sets of users based on the associated user groups.

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 To change the GUI inactivity check for all 5620 SAM GUI users, perform the following steps.

- **i** Configure the Client Timeout (minutes) parameter.
- **ii** Click on the Apply button.

3 To change the GUI inactivity check for all users in a user group, perform the following steps.

- **i** Click on the User Groups tab. A list of user groups is displayed.
- **ii** Choose a user group from the list and click on the Properties button. The User Group *name* (Edit) form opens.
- **iii** Enable the Override Global Timeout parameter.
- **iv** Configure the Client Timeout (minutes) parameter.
- **v** Click on the OK button. A dialog box appears.
- **vi** Click on the Yes button. The User Group (Edit) form closes.

4 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-20 To show, hide, or modify the toolbar

Icons that represent a subset of the main menu functions are available in the toolbar.

1 Start the 5620 SAM GUI. By default, toolbar icons are displayed under the 5620 SAM main menu.

2 To show the toolbar when it is hidden, perform the following steps.

- **i** Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.
- **ii** Select the Show Toolbar parameter and click on the OK button.

3 To modify the toolbar, right-click on an empty section of the toolbar. The toolbar contextual menu is displayed.

4 Perform one of the following:

a To add icons to the toolbar, select the icons in the contextual menu. The icons are added to the toolbar.

b To remove icons from the toolbar, deselect the icons in the contextual menu. The icons are removed from the toolbar.

c To hide the toolbar, choose Hide Toolbar from the contextual menu. The toolbar is removed from the display.

5 Click on an empty section of the GUI to close the toolbar contextual menu.

Procedure 2-21 To enable or disable containing window warnings

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Suppress Containing Window Warning parameter.

3 Click on the OK button. The User Preferences form closes.

Procedure 2-22 To enable or disable template generation messages

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Suppress Template Generation Message parameter.

3 Click on the OK button. The User Preferences form closes.

Procedure 2-23 To configure child object loading for service forms

Perform this procedure to configure the 5620 SAM to do one of the following.

- Load all child objects of a service, such as access interfaces and sites, before the service configuration form is displayed.
- Load all child object information of a service only when the appropriate tab button on the service configuration form is selected.

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Populate Entire Properties Form on Opening parameter.

3 Click on the OK button. The User Preferences form closes.

Procedure 2-24 To enable or disable a global span of control filter

Perform this procedure to configure which objects the 5620 SAM client GUI displays in frames that include list forms, maps, and the Alarm Window. By default, the GUI displays all objects that are in your View Access and Edit Access spans.

You can temporarily override the global filter setting in a list form or window using the Span On check box, and can include your span of control in an advanced filter window. See section 2.2 for information about performing searches using list forms and span of control filters.

Note — This procedure affects the GUI display of only the user that performs the procedure, and not other users.

1 Choose Application→User Preferences. The User Preferences form opens with the General tab displayed.

2 Configure the Apply User Span of Control parameter.

3 Click on the OK button. The User Preferences form closes.

Procedure 2-25 To save the GUI workspace preferences

You can save the GUI workspace preferences for a 5620 SAM client GUI session. When the user that saves the workspace preferences logs in to the client using the same user account on the same station, the GUI opens using the saved preferences.

1 Start the client GUI.

2 Configure the GUI workspace according to your preferences.

3 Choose Application→Save Workspace from the 5620 SAM main menu. The following GUI workspace preferences are saved:

- location of the navigation tree, alarm window, and physical topology
- whether to enable or disable audible alarm notifications
- toolbar settings

Note 1 — On a single-user client station, the GUI workspace preferences are saved in the following file:

- *user_home_dir*/5620SAM/guiPreference/*SAM_account_name*.guiPreferences on Solaris
- *user_home_dir*\5620SAM\guiPreference*SAM_account_name*.guiPreferences on Windows

where

user_home_dir is the UNIX or Windows home directory of the current user

SAM_account_name is the login name of the current 5620 SAM user

Note 2 — On a client delegate server station, the GUI workspace preferences are saved in the following file:

- *user_home_dir*/5620SAM/guiPreference/*SAM_account_name*.guiPreferences

where

user_home_dir is the UNIX home directory of the current user

SAM_account_name is the login name of the current 5620 SAM user

2.6 5620 SAM GUI search procedures

The following procedures describe how to use the 5620 SAM to search for and display information.

Procedure 2-26 To perform a simple search using column headings

1 Open a list form.

2 If available, choose an entry from the object drop-down list.

Note — If you click on the Search button without selecting a specific object type from the list, a default entry may be used.

3 If the filter has not been pre-populated, configure the filter criteria using the filter area of any column heading.

Note 1 — Entering a value into a filter area of a column heading without specifying an operation from an operation drop-down menu causes a default operation to be automatically selected.

Note 2 — The following operators are available for filtering a list by object timestamp. Each operator allows you to specify the time criteria using the clock icon beside the column heading filter:

- APPROXIMATELY EQUAL, which allows you to specify a time with 1m resolution rather than the default 1ms timestamp resolution
- IN THE PAST, which allows you to specify an amount of time before the present as the filter range, for example, the past 3 hours

Note 3 — Selecting NONE in an operation drop-down menu clears the filter area of the associated column heading.

Note 4 — Clicking on the Toggle Quick Filter button toggles the visibility of the filter areas on or off.

Note 5 — The filter areas of the column headings are disabled if a filter was applied using the filter window, if the filter window is open, or if a saved filter was loaded using the saved filter drop-down list. See Procedure 2-27 for more information about performing an advanced search.

4 Click on the Search button. The results list is displayed based on the filter.

5 To refresh the search results using the currently defined filter, click on the Search button. If applied, the current filter is used even when the filter areas are hidden or closed.

6 Close the List Form.

Procedure 2-27 To perform an advanced search

1 Open a List Form.

2 Click on the Filter button at the top of the form. The filter window opens.

Note — The filter areas of the column headings in a List Form are disabled if a filter is applied using the filter window, if the filter window is open, or if a saved filter was loaded using the saved filters drop-down list. See Procedure 2-26 for more information about performing a simple search using column headings.

3 Configure the filter properties.

i Choose an item from the Attribute drop-down menu.

ii Choose an item from the Function drop-down menu.

iii Choose an item from the Value drop-down menu.

iv Choose a Boolean Operator from the Operators drop-down menu.

v Click on the Add button.

4 Do one of the following.

a To filter additional properties, repeat step 3.

b To modify the search filter, go to step 5.

c If you are finished filtering properties, go to step 6.

5 Modify the search filter, if required.

a Replace a Boolean operator.

i Select a Boolean operator in the summary area.

ii Choose an item from the Operators drop-down menu to replace the selected Boolean operator.

Note 1 — If an entire bracket is selected, all Boolean operators within are replaced at once.

Note 2 — If multiple filtered properties exist, replacing a Boolean operator wraps the properties associated with that operator in brackets.

b Exclude filtered properties.

i Select a filtered property in the summary area.

ii Click on the NOT button to exclude any matching entries from the search results.

Note 1 — If an entire bracket is selected, all filtered properties within are excluded at once.

Note 2 — Selecting an excluded property or a bracket and clicking on the NOT button includes the property or bracket again.

c Replace filtered properties.

i Select a filtered property in the summary area.

ii Configure the filter properties, as described in step 3.

iii Click on the Replace button.

d Delete filtered properties.

i Select a filtered property or a bracket in the summary area.

ii Click on the Delete button to remove the selected filtered properties from the search filter.

Note — Multiple filtered properties can be selected and deleted at once.

e Wrap filtered properties in brackets.

i Click the left mouse button and drag over multiple filtered properties in the summary area to select them.

ii Click on the brackets button to wrap the selected filtered properties in brackets.

Note 1 — Selecting properties that are already wrapped in brackets and clicking on the brackets button unwraps the selected properties.

Note 2 — Properties can only be wrapped or unwrapped if all Boolean operators contained within are matching.

6 Click on the Apply button or the OK button. The results list is displayed based on the filter.

7 If the filter window is open, click on the Close button. The filter window closes.

8 Close the List Form.

Procedure 2-28 To perform a search using the navigation tree

You can use the navigation tree to find specific objects. These objects include nodes, shelves, ports, and more.

1 Click on the Find... button on the navigation tree or press CTRL+F. The Find panel opens.

2 Configure the parameters as necessary. The parameters that are available for configuration vary depending on the view that has been selected.

3 Click on the Find button or press Enter. The first matching object is selected and expanded in the navigation tree.

4 To find additional matching objects, click on the Next button or press F3. The next matching object is selected and expanded in the navigation tree.

5 To return to the previous matching object in the navigation tree, click on the Previous button or press Shift+F3.

6 If required, click on the Clear button to clear all parameters configured in step 2.

7 Click on the Find... button or press CTRL+F to close the Find panel.

Procedure 2-29 To perform a search by specifying endpoints

Use the following procedure to find objects such as service tunnels, MPLS paths, and LSP paths by specifying endpoints.

1 Choose one of the following menu options from the 5620 SAM main menu:

- Manage→MPLS→MPLS Paths
- Manage→MPLS→Dynamic LSPs
- Manage→MPLS→Static LSPs
- Manage→Service Tunnels

The Manage filter form opens.

2 Click on the Filter button. The filter window opens.

3 Choose Endpoints from the Select Filter Type drop-down menu. Endpoints is the default option.

Note — If a saved filter is selected or the filter areas of the column headings are populated, Advanced Filter is the default option.

4 Deselect the Any Source check box to pick a source IP address as a search filter. Otherwise, leave the Any Source check box selected to search by any source IP address.

5 Deselect the Any Destination check box to pick a destination IP address as a search filter. Otherwise, leave the Any Destination check box selected to search by any destination IP address.

6 Click on the Apply button. The results list is displayed based on the filter.

7 Click on the Close button to close the filter window.

8 Close the List Form.

Procedure 2-30 To filter object types

When an object drop-down list contains more than 10 items, you may click on the Filter for Object Type button to refine your search.

1 Open a List Form.

2 Click on the Filter for Object Type button. The Select Object Type form opens.

3 Configure the filter criteria using the filter area of any column headings.

Note — You can click on the Filter button on the Select Object Type form to open the filter window. See Procedure 2-27 for more information about performing an advanced search.

4 Click on the Search button. The results list is displayed based on the filter.

5 Select an object from the list and click on the OK button. The Select Object Type form closes and the List Form reappears with the new Object Type selected in the Object Type drop-down.

Procedure 2-31 To filter using span of control

On some List Forms, you can create and save a span filter to display objects for your specific span of control. For example, if you only want to see objects within the span of control that has been assigned to you, create a span filter. You can also configure user preferences to automatically filter out objects that are not in your span of control.

1 Open a List Form.

2 If available, choose an entry from the object drop-down list.

3 Do one of the following.

a To search using Span of Control from a List Form, go to step 4.

b To search using Span of Control from the filter window, go to step 5.

4 Click on the Span On check box. The results list is displayed based on the filter. Go to step 9.

5 Click on the Filter button. The filter window opens.

6 Choose an entry from the Span drop-down list.

Note — An entry from the Span drop-down list is selected based on the Span On check box on the List Form.

7 Click on the Apply button. The results list is displayed based on the filter and the Span On check box is updated.

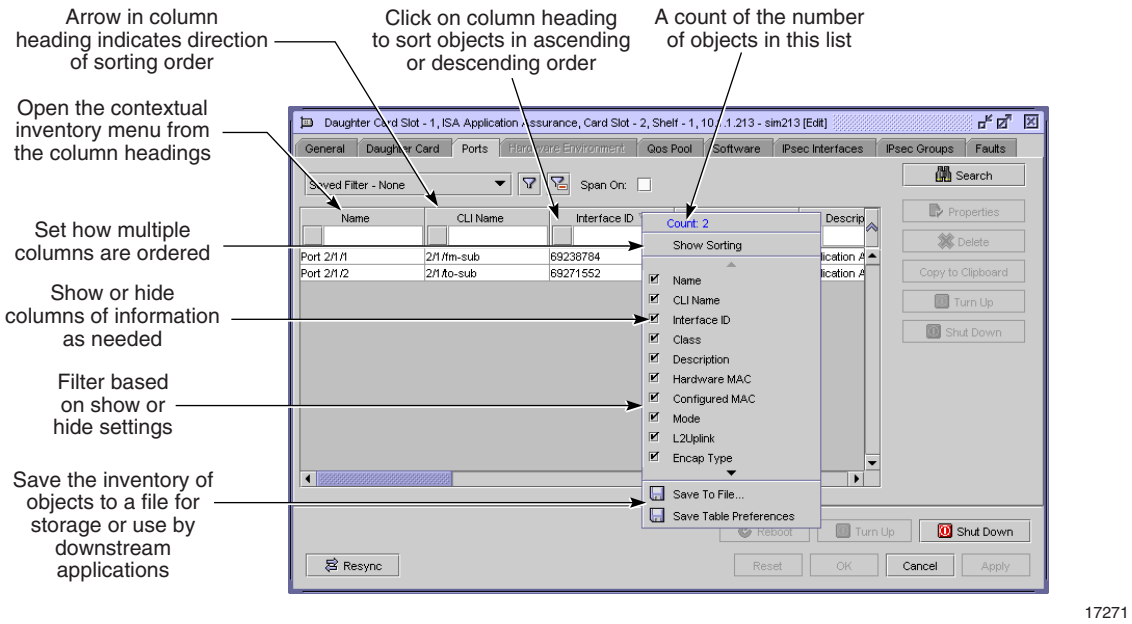
8 Click on the Close button. The filter window closes.

9 Close the List Form.

Procedure 2-32 To view and manage listed information

Many of the windows and forms are lists of network objects, for example, lists of ports from the equipment window, displaying all the ports on a specific card. Figure 2-9 shows the major elements of a list.

Figure 2-9 List elements



On most lists, you can:

- generate inventories of the listed data
- reorganize the information from most important to least important
- remove columns of data that are not of interest
- sort listed information in ascending or descending order

1 Generate a list.

2 Perform an action on the list.

a To generate an inventory of data, right-click on the list heading. The Count indicates the number of objects in the list.

b To reorganize the information, click on a column and drag the column to the right or left and drop the column in the appropriate location.

c To remove columns, right-click on the column heading and deselect the column from the check mark list. The column disappears from the display.

d To sort in ascending or descending order, click on the column heading. The arrow direction changes, indicating the order in which the data is sorted.

Note — To navigate quickly through a long sorted list, type a letter to move directly to the first item in the list that starts with that letter.

Table 2-5 describes the order in which different types of data are sorted from the top of the column to the bottom, based on the direction of the arrow in the column header. Figure 2-10 shows an example of information sorted in a column according to the down arrow in the column header.

Table 2-5 Sorting listed information

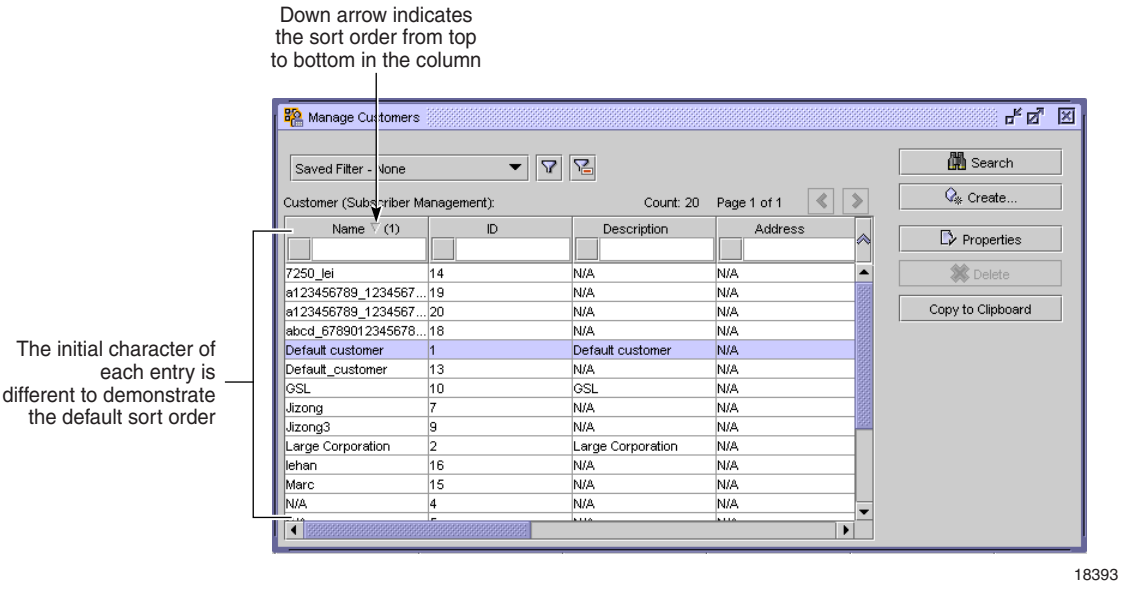
Entry type	Down arrow	Up arrow
Numbers only	Sorted from the lowest number to the highest number	Sorted from the highest number to the lowest number
Letters	Sorted left to right, character by character, from A to Z. Letters are sorted from uppercase to lowercase. Entries that begin with an uppercase letter are sorted from A to Z before entries that begin with a lowercase letter, which are sorted from a to z.	Sorted left to right, character by character, from Z to A. Letters are sorted from lowercase to uppercase. Entries that begin with a lowercase letter are sorted from z to a before entries that begin with an uppercase letter, which are sorted from Z to A.
Alphanumeric	Sorted left to right, character by character, in the following order: 0 to 9, A to Z, and a to z	Sorted left to right, character by character, in the following order: z to a, Z to A, and 9 to 0

(1 of 2)

Entry type	Down arrow	Up arrow
Special characters	Sorted left to right, character by character. The following characters are sorted in the following order before numbers, and uppercase and lowercase letters in a list: (space) ! # $ % & ‘ ( ) * + , . / The following characters are sorted in the following order after numbers in a list, but before uppercase and lowercase letters: : ; < = > ? @ The following characters are sorted in the following order after numbers, and uppercase and lowercase letters in a list: { | } ~	Sorted left to right, character by character. The following characters are sorted in the following order before numbers, and uppercase and lowercase letters in a list: ~ } | { The following characters are sorted in the following order before numbers in a list, but after uppercase and lowercase letters: @ ? > = < ; : The following characters are sorted in the following order after numbers, and uppercase and lowercase letters in a list: / . , + *) (‘ & % $ # ! (space)
Blanks	Blank entries are placed first at the top of the list.	Blank entries are placed last at the bottom of the list.

(2 of 2)

Figure 2-10 List sort order example



Procedure 2-33 To save listed information to a file

After you list information, as described in Procedure 2-32, you can save a copy of the list for purposes such as the following:

- record keeping
- inventory management
- processing by another application

1 Generate a filtered list, as required.

2 Right-click on a list column heading and choose Save To File from the contextual menu. The Save As form opens.

Note — The 5620 SAM uses the user home directory as the default location for saved files.

3 Use the form to specify the name and location of the file that is to contain the listed information. You can save the information in the following formats:

- plain text
- HTML
- CSV

4 Click on the Save button. The information is saved as specified and the Save as form closes.

Procedure 2-34 To configure the maximum number of objects on a list form

Perform this procedure to specify the maximum number of objects to display per page on a list form.

1 Choose Application→User Preferences. The User Preferences form opens with the General tab displayed.

2 Configure the Specify # of Items per Page parameter.

3 Click on the OK button. The User Preferences form closes.

Procedure 2-35 To save results list preferences

You can save results list preferences, so when similar searches on similar objects are performed, the output of the list is organized according to your preferences.

1 Open a List Form.

2 Organize the results list according to preference, for example, whether to sort columns of data in ascending or descending order.

3 Right-click on a results list column heading and choose Save Table Preferences from the contextual menu. A dialog box appears to confirm that you want to save the current filter preferences.

Note — Choosing Save Table Preferences from a contextual menu does not save any filter configurations.

4 Click on the Yes button. The results list format is saved.

Each time a similar list is generated for similar objects, for example, if you configured a table preference for generating lists of ports, then each time you list ports, results are displayed according to preconfigured table formats.

5 Close the List Form.

Procedure 2-36 To save search filters

List Forms allow you to save filters for object types. The filters created only apply to the specific object type against which the filter is created and saved, and that object type's descendant objects.

1 Open a List Form

2 Define filter properties, as described in Procedure 2-26 and click on the Filter button, or define filter properties, as described in Procedure 2-27. The filter form opens.

3 Click on the Save... button. The Save Filter form opens.

4 Configure the parameters:

- Filter Name
- Description
- Public

Note — These parameters have pre-populated values when a saved search filter is loaded or selected from the saved filters drop-down list, or if the filter was previously saved.

5 Click on the Save button. The Save Filter form closes. The defined filter is saved for a future search on a similar object type and the configured parameters are populated in the filter window.

6 Click on the Apply button of the OK button to use the filter. The results list is displayed based on the filter.

7 If the filter window is open, click on the Close button. The filter window closes.

8 Close the List Form.

Procedure 2-37 To clear a search filter

Use the following procedure to clear search filters from a List Form or the filter window.

1 Open a List Form.

2 Define filter properties as described in Procedure 2-26 or 2-27.

3 Do one of the following.

a To clear all search filters from a List form, go to step 4.

b To clear the search filter of the filter window, go to step 7.

4 Do one of the following.

a Click on the Clear all Filters button. Any filtered properties are cleared.

Note — Clicking on the Clear all Filters button does not clear or refresh search results.

b Choose No Filter from the saved filters drop-down list. Any filtered properties are cleared and the results list is displayed based on the empty filter. Go to step 11.

5 Click on the Search button. The results list is displayed based on the empty filter.

6 Go to step 11.

7 Click on the Filter button. The filter window opens.

8 Click on the Clear button. Any filtered properties are cleared from the filter window.

9 Click on the Apply button or the OK button. The results list is displayed based on the empty filter.

10 If the filter window is open, click on the Close button. The filter window closes.

11 Close the List Form.

Procedure 2-38 To load a saved search filter

Use the following procedure to load search filters from a List Form or the filter window. See Procedure 4-20 for information about loading a saved filter on a topology map.

1 Open a List Form.

2 Do one of the following.

- **a** To load search filters from a List Form, go to step 3.
- **b** To load search filters from the filter window, go to step 4.

3 Choose an entry from the saved filters drop-down list. The results list is displayed based on the filter. Go to step 11.

Note 1 — Choosing an entry from the saved filters drop-down list disables the filter areas of the column headings.

Note 2 — Only saved filters that are applicable to the current object type and its ancestor types appear in the saved filters drop-down list.

Note 3 — Selecting None from the saved filters drop-down list clears any filtered properties on the current form and immediately refresh the results list.

Note 4 — The contents of the filter window are updated based on the entry selected from the saved filters drop-down list.

4 Click on the Filter button. The filter window opens.

5 Click on the Saved Filters button. The Saved Filters window opens and displays filters that have been saved for the current object type and its ancestor type(s).

6 Select a saved filter in the list.

7 Click on the Load button. All the properties of the filter window are replaced with the contents of the saved filter.

8 If desired, modify the filter and click on the Save button to save it.

Note — The filter is saved using the current object type, regardless of the object type of the saved filter that was loaded.

9 Click on the Apply button or the OK button to use the filter. The results list is displayed based on the filter.

10 If the filter window is open, click on the Close button to close the filter window.

11 Close the List Form.

Procedure 2-39 To delete a saved search filter

Use the following procedure to delete saved search filters from the filter window.

1 Open a List Form.

2 Click on the Filter button. The filter window opens.

3 Click on the Saved Filters button. The Saved Filters window opens.

4 Select a saved filter in the list.

5 Click on the Delete button. The filter is deleted.

6 Close the form.

7 Close the filter window.

8 Close the List Form.

3 — 5620 SAM features

3.1 New for 5620 SAM Release 8.0

Table 3-1 lists the features and functions added in 5620 SAM Release 8.0.

Note 1 — See the *5620 SAM LTE ePC User Guide* for information about LTE ePC features and functions.

Note 2 — See the *5620 SAM LTE RAN User Guide* for information about LTE RAN features and functions.

Note 3 — See the *5620 SAM Optical User Guide* for information about features and functions that are specific to optical device support.

Table 3-1 5620 SAM Release 8.0 features

Feature or function	Description	Reference for more information
Release 8.0 R7 features		
Timezone Management	The 5620 SAM allows the configuration of default and current time zones for a client.	See chapter 2 for more information.
Support for Local DHCP Server and Local User Database in 7450	The 5620 SAM supports the configuration of Local DHCP Servers and Local User Databases on 7450s.	See chapter 64, 70, and 71 for more information.
Support for 7210 SAS series Release 3.0	The 5620 SAM supports the 7210 SAS Release 3.0.	See section 11.1 for more information.
BFD support for 7210 SAS-M and 7210 SAS-X	The 5620 SAM supports BFD for the 7210 SAS-M and the 7210 SAS-X release 3.0 on the following interfaces: • network • OSPF • ISIS	See chapters 27, 28, and 71 for more information.
Q in Q support for 7210 SAS-M and 7250 SAS-X	The 5620 SAM supports Q in Q encapsulation on the 7210 SAS-M and the 7210 SAS-X Release 3.0.	See chapter 17 for more information.
Bypass LSP support for 7210 SAS-M and 7250 SAS-X	The 5620 SAM supports the configuration of bypass LSPs on the 7210 SAS-M and the 7210 SAS-X Release 3.0.	See chapters 29 and 30 for more information.
5620 SAM user security enhancements	The span of control function is expanded to include transport services, including the 1830 PSS family of network elements.	See Table 8-3 in chapter 8 for more information.
Physical topology map	The functionality of the physical topology map is extended to include the display of optical links.	See Table 4-1 in chapter 4 for more information.
Restrict active sessions per user group	The number of active user sessions for a user group can be limited to a specified number.	See the Maximum User Sessions Allowed (maxUserSessionsAllowed) parameter in section 128.1 for more information.
Windows 7 client support	The 5620 SAM supports the installation and operation of GUI clients on Windows 7 (32 and 64-bit).	See chapter 2 for more information.
Cflowd Type parameter for VPRN	The 5620 SAM supports the configuration of the Cflowd Type parameter on L3 access interfaces on VPRN. Supported on the 7750 SR, 7450 ESS (mixed mode), and 7710 SR.	See chapter 71 for more information.

(1 of 22)

Feature or function	Description	Reference for more information
VPLS support on 7705 SAR 4.0 R1	The 5620 SAM supports VPLS service on the 7705 SAR 4.0 R1. VPLS support on the 7705 SAR excludes the following 5620 SAM functionality: B-VPLS, I-VPLS, M-VPLS, BGP, GSMP, IGMP Snooping, MLD Snooping, PIM Snooping, and STP. The 5620 SAM supports PPPoE Circuit ID tag processing on L2 access interfaces on VPLS sites on the 7705 SAR 4.0 R1. If a 7705 SAR daughter card has L2 access interfaces for a VPLS service, then the access ingress fabric profile policy associated with that daughter card must be configured for Aggregate mode.	See chapter 68 for more information.
MC ring enhancement for VPLS	The 5620 SAM supports MC ring node assignment on VPLS services. Ring node can be set on an L2 access interface on VPLS (L2, I-L2, B-L2 interfaces) and M-VPLS (L2, I-L2, B-L2 interfaces). Supported on the 7750 SR, 7450 ESS, and 7710 SR, version 8.0 R6 and later.	See chapter 68 for more information.
2-Port Gig Ethernet MDA with SyncE support on the 7210 SAS-M	The 5620 SAM supports the 2-Port Gig Ethernet MDA on the 7210 SAS-M 3.0 R1 and later devices. This MDA provides 2 x 10Gig Ethernet ports with SyncE.	See chapter 15 for more information about daughter card support. See Procedure 17-27 for information on how to assign a card type.
Ethernet Ring Protection (G.8032) support on the 7210 SAS	The 5620 SAM supports Ethernet Ring Protection (G.8032) on the 7210 SAS 3.0 R1 and later devices (exception: not supported on the 7210 SAS-X 24F 2XFP in 3.0 R1). Ethernet ring protection is provided by Ring Protection Links (RPL) employed to protect the ring and help achieve high reliability and network stability.	See chapter 11 and Procedures 30-7 and 30-8 for more information.
CESoP Cpipe for CES MDA support on the 7210 SAS-M	The 5620 SAM supports CESoP Cpipe on the 7210 SAS-M 3.0 R1 and later devices. Circuit Emulation Services (CES) is supported on the 7210 SAS-M devices using the CES for T1/E1 interfaces on the optional CSE MDAs which may be installed on the 7210 SAS devices.	See Procedure 67-8 for information on how to create a VLL Cpipe service. See Procedure 17-74 for information on how to configure a TDM DS1/E1 port on a CES 2-Port Gig Ethernet MDA card
802.1ab Link Layer Discovery Protocol (LLDP) support on the 7210 SAS	The 5620 SAM supports 802.1ab Link Layer Discovery Protocol (LLDP) on the 7210 SAS 3.0 R1 and later devices. The following LLDP functions are provided: • LLDP Protocol Configuration • Physical Map Discovery • Physical Map enhancements • LLDP support for GNE • Checkpoint functionality • Accurate visual representation of the link type (Hub/Broadcast, LAG, MC-LAG) • Alarm reporting for mismatched links and the ability to find the root cause of the alarms • Data overlay support • Support for Nearest Customer Bridge and Nearest non-TPMR Bridge transmission scope addressing • Checkpoint functionality • CPAM integration Additionally, the processing of the 7210 SAS node-specific VLAN Uplink object uses the LLDP node configuration.	See chapters 11, 17, 27 and Procedure 17-48 for more information.
Release 8.0 R5 features		

(2 of 22)

Feature or function	Description	Reference for more information
5620 SAM User Guide content reorganization	The *5620 SAM User Guide* has a simplified volume and chapter structure in a hierarchical format. The volumes are organized by functional area, in the following order: • Introduction—5620 SAM system overview, operation, and configuration • 5620 SAM system management—system redundancy, database management, and security • Device management—preparation for 5620 SAM management, security, and equipment-related information • Network management—routing and IP/MPLS infrastructure, network fault management, and network component redundancy • Policy management—5620 SAM policy configuration and management • Service management—customer, subscriber, and service configuration, QoS management, and service-based fault management	See the *5620 SAM User Guide*.
Mid-session changes for PPPoE subscriber hosts	The 5620 SAM supports mid-session changes to subscriber profile, SLA profile, and application profile information on PPPoE subscriber hosts.	See chapter 64 and Procedure 64-31 for more information.
Support for disconnected subscribers	The 5620 SAM maintains a record of subscribers that are deleted at the NE. The disconnected subscriber record is maintained in an inactive state in the 5620 SAM database.	See chapter 64 and Procedures 64-35 and 64-36 for more information.
IPv6 subscriber management for routed CO	The 5620 SAM supports configuration of IPv6 for ESM over Ethernet services, in conjunction with existing IPv4 configuration: • IPv6 forwarding on subscriber interfaces on IES and VPRN • IPv6 router advertisement on the group interface on IES and VPRN • DHCPv6 support on group interface on IES and VPRN Supported on the 7750 SR and 7450 ESS in mode C or D, running an IOM3-XP.	See chapter 70 and Procedures 70-7 and 70-8 for more information on IES configuration. See chapter 71 and Procedures 71-10 and 71-11 for more information on VPRN configuration.
Subscriber multicast over PPPoE	The 5620 SAM supports subscriber multicast over PPPoE on IES and VPRN services on the 7750 SR.	See Procedures 70-4, 71-4, 28-36, 64-19, and 64-2 for more information.
Routed residential subscriber with PPPoE and DHCP support for BGP	The 5620 SAM supports routed residential subscribers with PPPoE and DHCP support for BGP. Support is implemented through a BGP peering policy under the residential subscriber policy manager, and a dynamic peer option on a VPRN service.	See chapter 64 and Procedures 64-20 and 28-4 for more information.
Diameter policy support	The 5620 SAM supports diameter policy configuration on the 7750 SR, 7450 ESS, and 7710 SR.	See chapter 64 and Procedure 64-21 for more information.
PAP/CHAP user name re-writing	The 5620 SAM supports PAP/CHAP user name re-writing options when configuring subscriber authentication policies for the 7750 SR, 7450 ESS, and 7710 SR.	See chapter 18 and Procedure 18-12 for more information.
DHCP vendor options for IPoE user name	The 5620 SAM supports the use of DHCP vendor options 60 and 61 as an IPoE user name when configuring subscriber authentication policies for the 7750 SR, 7450 ESS, and 7710 SR.	See chapter 18 and Procedure 18-12 for more information.
Weighted scheduler groups for Port Scheduler Policies	The 5620 SAM supports the application of a scheduling weight to groups of subscriber host queues competing at the same priority level as a Port Scheduler Policy.	See chapter 44 and Procedure 44-17 for more information.

(3 of 22)

Feature or function	Description	Reference for more information
Subscriber aggregate rate adjustment	The 5620 SAM supports the adjustment of subscriber aggregate rate based on the average frame size.	See Procedure 64-2 for more information.
Virtual ports	The 5620 SAM supports the creation of virtual ports on the egress context of an Ethernet port.	See chapter 62 for more information.
External windows	The 5620 SAM supports the ability to externally manage windows used within the GUI.	See chapter 2 for more information.

(4 of 22)

Feature or function	Description	Reference for more information
OmniSwitch support	• Stacking IP multicast VLAN service is supported on OS 6400, OS 6850, OS 6855, OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E, Release 6.4.3 or later, and on OS 6250 (Metro), Release 6.6.2 or later. • Enterprise IP multicast VLAN service is supported on OS 6250 (SME), and OS 6250 (Metro), Release 6.6.2 or later. • Advanced loopback test configuration on OmniSwitch ports is supported on OS 6400, OS 6850, OS 6855, OS 9600, OS 9700,and OS 9800, Release 6.4.3 or later, and on OS 6250 (Metro), and OS 6250 (SME), Release 6.6.2 or later. • Support for 802.1ag version 8.1 Ethernet OAM-CFM functionality on OS 6400, OS 6850, OS 6855, OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E, Release 6.4.3 or later, and on OS 6250 (Metro), Release 6.6.2 or later. • Support for 802.3ah - UNI Loopback on OS 6400, OS 6850, and OS 6855, Release 6.4.3 or later, and on OS 6250 (Metro), Release 6.6.2 or later. • Support for Dying Gasp - Power Loss, at the NE level, only on OS 6250 (Metro), Release 6.6.2 or later. • Port/queue statistics support on OS 6250 (Metro) and OS 6250 (SME), Release 6.6.2 or later. • Ip statistics for routing instances support on OS 6400, OS 6850, OS 6855, OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E, Release 6.4.3 or later, and on OS 6250 (Metro), and OS 6250 (SME), Release 6.6.2 or later. • L2 MAC tunneling action on OS 6250, OS 6400, OS 6850, OS 6855, OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E, Release 6.4.3 or later. • MVRP support onOS 6400, OS 6850, OS 6855, OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E, Release 6.4.3 or later. • Ingress/egress filtering/advanced policy conditions and actions/rule stats (QoS List) on OS 6400, OS 6850, OS 6855, OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E, Release 6.4.3 or later, and on OS 6250 (Metro), and OS 6250 (SME), Release 6.6.2 or later. • Y.1731 fault management and performance monitoring: CFM two way delay test and CFM one way delay test on OS 6400, OS 6850, OS 6855, OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E, Release 6.4.3 or later, and on OS 6250 (Metro), Release 6.6.2 or later. • Full hybrid support for Ethernet OAM functionality (CFM continuity check, CFM loopback, CFM link trace, CFM one way delay, and CFM two way delay tests) on both 802.1ag and Y.1731 platforms on OS 6400, OS 6850, OS 6855, OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E, Release 6.4.3 or later, and on OS 6250 (Metro), Release 6.6.2 or later. • SAA generic L2 Ethernet OAM support: ICMP Ping, CFM loopback, and CFM two delay tests on OS 6400, OS 6850, OS 6855, OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E, Release 6.4.3 or later, and on OS 6250 (Metro), Release 6.6.2 or later. MAC ping support on OS 6250 (Metro), Release 6.6.2 or later. • CPE SLA test ahead support only on OS 6250 (Metro), Release 6.6.2 or later.	See Procedure 65-7 for more information. See Procedure 17-57 for more information. See chapter 35 for more information. See Procedures 17-55, 17-56, 17-58, and 17-59 for more information. See Procedure 48-1 for more information. See Procedure 44-35 for more information. See Procedures 35-9, and 35-8 for more information. See Procedure 75-5 for more information. See Procedures 28-51, and 17-62 for more information.

(5 of 22)

Feature or function	Description	Reference for more information
GNE profile enhancements	Improvements to generic network element (GNE) handling in the 5620 SAM. • Login confirmation prompt handling in GNE CLI. • Customizable GNE icons in 5620 SAM GUI	See chapter 12 and Procedure 12-4 for more information.
IPv6 addressing for DHCP host on local user database	The 5620 SAM supports configuration of an IPv6 address and/or IPv6 prefix for a DHCP host on a local user database. Supported on the 7750 SR and 7450 ESS Mixed Mode.	See chapter 64 and Procedure 64-34 for more information.
SDIC multi-drop data bridge on 7705 SAR 3.0 R3	Support on RS232 channels for multi-drop data bridge, S-bit signalling, and configuration of HCM data position.	See chapter 11 for more information about 7705 SAR support in the 5620 SAM.
Auxiliary alarms daughter card on 7705 SAR 3.0 R3	The 5620 SAM supports an auxiliary alarm daughter card on the 7705 SAR version 3.0 R3 or later.	See chapter 15 for more information about 7705 SAR equipment management in the 5620 SAM.
X21 port type on 7705 SAR 3.0 R3	The 5620 SAM supports the X21 port type on the 12 port serial data interface daughter card on the 7705 SAR version 3.0 R3 or later.	See chapter 11 for more information about 7705 SAR support in the 5620 SAM.
Y.1731 Dual Ended Loss Test on 7705 SAR 3.0 R3	The 5620 SAM supports the Dual Ended Loss Test as part of the CFM Continuity Check on the 7705 SAR 3.0 R3.	See chapter 35 and Procedure 35-4 for more information about the Dual Ended Loss Test.
Timing reference quality on 7705 SAR 3.0 R1	The 5620 SAM supports timing reference quality level configuration for Reference One, Reference Two, and External timing references.	See chapter 17 and Procedure 17-34 for more information.
STM enhancements	The 5620 SAM STM includes the following: • test and CFM object management using Service and Composite Service flat maps • NE-specific MEP ID range configuration • test-related alarm indication on tested entity • modified CFM test structure to accommodate new tests and potential CCM protocol enhancements • CFM frame-rate limiting as extension of DoS protection • large-scale NAT static port forwarding, in which internal and external IP addresses and ports are statically associated • CFM test creation flow modifications • retention of test results after deletion of associated test suite • automatic CFM test updates in response to service topology changes • MAC address configuration for unmanaged MEPs • removal of obsolete trace test definitions from test suites	See chapters 4 and 75 for more information.
Alarm management enhancements	5620 SAM alarm management support now includes the following: • alarm history access from the 5620 SAM Alarm Window • inclusion of additional alarm properties in alarm history records • automatic deletion of correlated alarms in response to manual deletion or clearing of correlating alarm	See chapter 34 for more information.
Network performance TCAs	The 5620 SAM supports the configuration of threshold-crossing alarms for network objects such as physical ports.	See chapter 34 for more information.

(6 of 22)

Feature or function	Description	Reference for more information
NE backup history	The 5620 SAM can retain a configurable number of NE configuration backups on the 5620 SAM main server file system.	See chapter 5 for more information.
9500 MPR support	The following 9500 MPR features are supported: • MSS-4 4-slot shelf for ETSI 2.1 • MSS-8 8-slot shelf for ANSI 1.2, 2.2.1, and ETSI 2.1 • core-B card for ANSI 1.2.0 • core-enhanced card for ETSI 2.1 • 1 x radio modem (MD300) card for ANSI 1.2, 2.2.1, and ETSI 2.1 • 32 xDS1/E1 card (DS1 support only) for ANSI 1.2, and 2.2.1 • 32 xDS1/E1 card (E1 support only) for ETSI 1.2 • 2+2 x Ethernet (EAS) card with MPT support for ETSI 2.1 • VLAN paths and VLAN groups for ANSI 1.2, 2.2.1, and ETSI 2.1 • Cpipe for ANSI 1.2, 2.2.1, and ETSI 2.1 • Epipe for ANSI 1.2, and 2.2.1 • Apipe for ETSI 2.1 • Composite services for Cpipe and Epipe with 7705 SAR NEs for ANSI 1.2, and 2.2.1 • Composite services for Cpipe and Apipe with 7705 SAR NEs for ETSI 2.1 • dot1Q cross connect (SCP) for ETSI 1.3 or later • performance management, fault management, service aggregator, and error recovery for ANSI 1.2, 2.2.1, and ETSI 2.1 • analog performance management for ANSI 2.2, 2.2.1, and ETSI 1.3 or later • port segregation configuration enhancement for all ANSI and ETSI releases • loopback test configuration on DS1, ES1, and radio modem ports for ANSI 2.2 or later and ETSI 1.3 or later • dot 1Q VLAN service for ETSI 1.3 or later • light weight (9400 AWY, MSS-1c, and MPT-sa) generic NE management • cross launch of MPT-sa and MSS-1c J-USM manager	See chapters 11, 34, 66, 67, and 72 for more information. See Procedures 17-64, 17-69, 17-70, 17-71, 65-8, 12-4, 12-5, and 12-6 for more information.
Enhanced copying and moving SAPs between ports	The copy and move SAP function is enhanced to include endpoints with ATM encapsulation on the 7750 SR, 7450 ESS, and 7710 SR.	See "Moving and copying SAPs between ports" in chapter 15 for more information.
New IMM support	The 7750 SR and 7450 ESS support the following: • 1-port 100GE CFP IMM • 12-port 10GE SF IMM	See Table 15-1 in chapter 15 for more information.
DWDM enhancements	The 5620 SAM supports the 1-Port OC768 OTU3 Long Reach DWDM Tunable IMM on the 7750 SR.	See Procedure 17-61 for more information.
APS enhancements	Any port on a channelized or non-channelized SDH card on a 7750 SR or 7710 SR, Release 8.4 or later, can be selected as a working or protection channel on a unidirectional APS group. The 7750 SR-c4 supports configuration of unidirectional 1+1 signaling data. The APS MLPPP bundles support APS channels in network mode.	See chapter 37 for more information about APS.

(7 of 22)

Feature or function	Description	Reference for more information
	The uni1plus1 switching mode is supported on the following 7750 SR-c4 and 7750 SR-c12 ASAP cards: • 4 x Channelized OC3 ASAP • 1 x Channelized OC12 ASAP	—
Latitude and Longitude NE configuration	Configuration of latitude and longitude of any NE is supported.	See Procedure 17-8 for more information.
Synchronization enhancements	The 7750 SR-c4 provides clock for timing synchronization to all downstream elements. The timing source selection is based on best quality level at the reference source for the 7450 ESS, 7710 SR, 7750 SR, and 7750 SR-c4.	See Procedure 17-34 for more information.
	Port-level changes include the following parameters: • SSM Code-Type • Tx DUS/DNU	See chapter 168 for more information.
7750 SR-c4 support	The 7750 SR-c4 is a 4-slot chassis that supports a 40 Gb/s forwarding capacity and up to 4 CMAs or 2 MDAs.	See chapters 11 and 15 for more information.
Soft reset enhancements	IOM3 and IMM cards on the 7750 SR and 7450 ESS, Release 8.0 R1 or later, support soft reset.	See Procedure 21-9 for more information.
VLL redundancy enhancements	The 5620 SAM supports HSDPA offload fallback for VLL Apipe and Epipe services on the 7450 ESS, 7710 SR, and 7750 SR by allowing fallback from an active PW on a primary spoke SDP to a secondary SAP.	See chapter 67 for more information.
Alarm removal	Any EquipmentRemoved and ContainingEquipmentRemoved alarms generated by an earlier 5620 SAM release are cleared when you upgrade the 5620 SAM to Release 8.0 R5 or later. In Release 8.0 R5 or later, these alarms are generated only when a card is removed from a slot or an IOM.	—
Auto-provisioning enhancement	The 5620 SAM supports auto-provisioning on the 7705 SAR, Release 3.0 or later.	See chapter 26 for more information.
Automatic create of all channels	The 5620 SAM supports automatic creation of all of the channels on OC3, OC12, and DS3/E3 ASAP ports.	See Procedure 17-85 for more information.
SAP migration	The 5620 SAM supports the ability to retain the SAPs that are created on access ports during a migration from access to hybrid mode on Ethernet and SC LAG ports.	See Procedure 15-2 for more information.
AA subscriber policy override	The 5620 SAM supports the configuration of ASO characteristics for an AA subscriber using an AA subscriber policy override.	See chapter 73 and Procedure 17-17 for more information.
AA group policy enhancements	The 5620 SAM supports a Policy Sync Group menu option to designate an AA group policy as the master policy and add one or more AA group policies to policy sync group members.	See chapter 73 and Procedure 73-4 for more information.
Ipipe enhancements	Ipipe service supports application profile configuration on an L2 access interface and spoke SDP binding.	See chapter 67 and Procedures 67-7 and 67-11 for more information.
TCP/UDP application usage	The 5670 RAM provides a comparative analysis of TCP and UDP application usage.	See chapter 73 and Procedure 73-3 for more information.
Application performance index analysis	The 5670 RAM performs an application performance index analysis on an AA application.	See chapter 73 and Procedure 73-3 for more information.
LDP transport destination address	The 5620 SAM supports the configuration of a transport destination address for LDP.	See Procedures 30-1 and 30-2 for more information.

(8 of 22)

Feature or function	Description	Reference for more information
Automatic bandwidth allocation for RSVP dynamic LSPs	Automatic bandwidth allocation is supported on an RSVP dynamic LSP that has CSPF and MBB enabled.	See chapter 29 and Procedures 29-2 and 29-8 for more information.
IPv6 support on VLL Ipipe	IPv6 capability is supported on a VLL Ipipe service, on the 7750 SR (chassis mode C and above), 7450 ESS in mixed mode (chassis mode D and above), and on the 7710 SR (chassis mode C and above).	See chapter 67 and Procedures 67-7 and 67-11 for more information.
Routed VPLS support	The 5620 SAM supports the binding of an L3 access interface within an IES or VPRN service to a VPLS on the same site.	See chapters 68 and 72, and Procedures 68-1, 70-1, 71-2, and 72-1 for more information.
RSVP P2MP I-PMSI template	The 5620 SAM supports an RSVP-based P2MP LSP template for MVPN I-PMSI creation.	See chapters 28 and 29, and Procedures 28-32 and 29-23 for more information.
Multicast P2MP LDP	LDP support for P2MP can be enabled on an LDP interface. LDP configuration is supported on a tunnel interface under a base routing instance and protocols such as PIM and IGMP.	See chapter 28, and Procedures 27-1, 28-18, and 28-19 for more information.
Multi-homing for L3 services	Two new types of routing interface are introduced: Multi-Homing Primary and Multi-Homing Secondary. These are loopback interfaces used in multi-homing resiliency for a pair of protected routers. This applies to both IP and VPN traffic.	See Procedure 27-1 for more information.
Ethernet Rings	The ability to create and configure Ethernet Rings is introduced. Ethernet ring protection is provided by Ring Protection Links (RPL) employed to protect the ring and help achieve high reliability and network stability.	See Procedures 30-7 and 30-8 for more information.
Ethernet CAC enhancements	The ability to reserve tunnel bandwidths (on B-VPLS) and allocate service bandwidth (on I-VPLS) for CAC-enabled VPLS was introduced.	See Procedures 68-1 and 68-11 for more information.
Tunnel selection enhancements	Tunnel Selection Profiles and Steering Parameters introduced to assist in assigning transport tunnels for VLL, VPLS, and VPRN services.	See chapters 67, 68, and 71, and Procedures 30-1, 30-3 and 30-4 for more information.
VPRN route threshold alarms	New alarms introduced for: High Threshold Level Routes Reached, Maximum Number of Routes Reached, and Mid Threshold Level Routes Reached	See the Troubleshooting Guide for more information.
BGP VPLS Multi-homing	The 5620 SAM supports the configuration of BGP-based VPLS multi-homing between PE and CE sites.	See chapter 68, and Procedures 17-8 and 68-7 for more information.
Service modification from the topology view	The 5620 SAM supports the creation of service components such sites, access interfaces, endpoints, and SDP bindings directly from the service topology view. Sites can also be automatically fully-meshed or added to an existing mesh from this view. VPLS, VPRN, VLL, IES, and Composite services are supported.	See Procedures 4-34, 67-19, 68-24, 68-24, 70-13, 71-19, and 72-4 for more information.
Script Editor and GUI Builder enhancements	The Script Editor and GUI Builder forms have been combined into one form to improve the usability of building and modifying scripts and templates. By default, the Script Editor displays a split view of the GUI Builder and code windows. You can also choose to have the Property Selector form open, which is an optional window that is only applicable for XML API configuration templates.	See chapter 3 in the *5620 SAM Scripts and Templates Developer Guide* for more information.
Modification templates	The 5620 SAM supports the creation of two types of templates—creation and modification. You can specify the type of template using the Command Type parameter.	See section 5.2 for more information.

(9 of 22)

Feature or function	Description	Reference for more information
Service segmentation view	A service segmentation view is available to aid in conceptualizing complex services. Segments are logical grouping of interconnected sites, services, and bindings. VPLS, VLL, and composite services are supported.	See chapter 4 for more information.
VPRN Route Target on Topology view	Route targets for VPRN services can now be displayed in the topology view for the service.	See Procedure 71-19 for more information.
BGP-to-LDP label stitching	This feature allows LDP-capable PE devices to advertise LDP prefixes, thereby allowing them to offer services to PE routers in areas or domains where BGP-labelled routes are not supported.	See Procedure 28-5 for more information.
Specifying intermediate services	This feature allows you to view and specify intermediate services inserted into ethernet tunnel paths.	See Procedure 30-6 for more information.
PW template modification and re-evaluation	This feature provides a push-button evaluation of modifications you make to a PW template, including the altering of associated Route Targets. BGP-enabled VPLS services are supported.	See Procedures 49-1 and 68-8 for more information.
Configurable labels for LLDP Discovered Physical Links	LLDP Discovered Physical Links can now be assigned names and descriptions.	See Procedure 4-40 for more information.
Configurable identification label for generic LLDP far-end devices	A Chassis MAC Object ID identifier can now be associated with a non-Alcatel-Lucent far-end device that is running LLDP. This provides a configurable label on the physical topology map.	See Procedure 12-4 for more information.
7210 SAS-X 24F 2XFPRelease 2.0	The 7210 SAS-X 24F 2XFP Release 2.0 supports a single fixed slot chassis supporting one card and one MDA (24 fixed 1 Gig ports and 2 fixed 10G ports), in addition to all of the features of the 7210 SAS-M version 2.0 R4 except for the following: • 4 x Channelized DS1/T1 CES MDA • Cpipe • syncE	See section 11.1 for more information.
Out-of-band management support on 7210 SAS-E, 7210 SAS-M, and 7210 SAS-X 24F 2XFP	The 5620 SAM supports out-of-band management on the 7210 SAS-E, version 2.0 R2 or later, 7210 SAS-M version 2.0 R2 or later, and 7210 SAS-X 24F 2XFP.	See chapter 12 and Procedure 12-9 for more information.
CES MDA support on 7210 SAS-M	The 5620 SAM supports the 4 x Channelized DS1/E1 CES MDA on the 7210 SAS-M, version 2.0 R2.	See chapter 15 for more information about daughter card support.
Cpipe service on 7210 SAS-M	The 5620 SAM supports the creation of a VLL Cpipe with point-to-point CEM encapsulation on the 7210 SAS-M, version 2.0 R2.	See chapter 67 and Procedures 67-8 and 67-11 for more information.
Y.1731 performance monitoring support on 7210 SAS-M and 7210 SAS-X 24F 2XFP	The 5620 SAM supports time stamping on the 7210 SAS-M version 2.0 R2 and the 7210 SAS-X 24F 2XFP.	See chapter 35 for more information.
Y.1731 fault notification support	The 5620 SAM supports fault notification through AIS on the 7210 SAS-E, 7210 SAS-M, and 7210 SAS-X 24F 2XFP.	See chapter 35 for more information.
MPLS LDP protocol on 7210 SAS-M and 7210 SAS-X 24F 2XFP	The 5620 SAM supports LDP protocol on the 7210 SAS-M, version 2.0 R2 and the 7210 SAS-X 24F 2XFP.	See chapter 28 for more information.
Line timing using syncE on 7210 SAS-M	The 5620 SAM supports line timing of ethernet ports using syncE on the 7210 SAS-M, version 2.0 R3.	—

(10 of 22)

Feature or function	Description	Reference for more information
H-Metering on 7210 SAS-M and 7210 SAS-X 24F 2XFP	The 5620 SAM supports H-Metering on the 7210 SAS-M, version 2.0 R4, and the 7210 SAS-X 24F 2XFP.	See Procedure 68-3 for more information.
Network Domain Queue Optimization RFE	The 5620 SAM supports Network Domain Queue Optimization on the 7710 SR,7450 ESS and 7750 SR.	See chapters 11, 27, 30, 191 for more information.
Enhanced BGP configuration	The 5620 SAM supports additional configuration options for global-level, group-level, and peer-level BGP.	See Procedures 28-2, 28-4, and 28-5 for more information.
Policy policer override	The 5620 SAM supports override functionality for policy policers.	See Procedure 44-40 for more information.
Queue override	The 5620 SAM supports override functionality for queues.	See Procedure 44-40 for more information.
Policer control policy override	The 5620 SAM supports override functionality for policer control policies.	See Procedure 44-40 for more information.
Release policies from a list form	The 5620 SAM supports the release of policies from a list form.	See Procedure 43-1 for more information.
View trap metrics information	The 5620 SAM supports the ability to view trap metrics information from a new form.	See Procedure 21-22 for more information.
View devices and quantities licensed	The 5620 SAM supports the ability to view licensed devices and licenses remaining.	—
Burst limit	The 5620 SAM supports the explicit shaping of burst size for a queue.	See Procedures 44-1, 44-3, 44-21, and 44-22 for more information.
Category map policies	The 5620 SAM supports the creation of category map policies.	See Procedure 64-4 for more information.
Credit control policies	The 5620 SAM supports the creation of credit control policies.	See Procedure 64-5 for more information.
Credit reset	The 5620 SAM allows the manual reset of a subscriber host's credit.	See Procedure 64-6 for more information.
Insertion blocks	The 5620 SAM supports the creation of insertion blocks on ACL IP filters and ACL IPv6 filters.	See Procedures 45-1 and 45-2 for more information.
RADIUS authentication custom record	The 5620 SAM supports the customization of accounting information for RADIUS accounting policies.	See Procedure 54-1 for more information.
Release 8.0 R3 features		
CFMA integration	The SAM-CFMA adapter for CFMA 2.1 translates SAM alarms into alarms for CFMA.	See the *5620 SAM Integration Guide* for information about integration components.
SSO integration	Single sign on (SSO) technology enables a user to access all resources within a given domain after having entered their credentials just one time.	See the *5620 SAM Integration Guide* for information about integration components.
Graceful restart for RSVP on MPLS interfaces on 7210 SAS-M	The 5620 SAM supports graceful restart functions for RSVP on MPLS interfaces on the 7210 SAS-M version 2.0 or later.	See Procedure 28-28 for more information.
Mesh SDP binding for VPLS on 7210 SAS-M	The 5620 SAM supports mesh SDP binding for VPLS service on the 7210 SAS-M version 2.0 or later. All validation tests for spoke SDP bindings on the 7210 SAS-M apply to mesh SDP bindings as well.	See Procedure 68-4 for more information.

(11 of 22)

Feature or function	Description	Reference for more information
IP interface for VPLS service on 7210 SAS-E	The 5620 SAM supports IP interfaces for VPLS service on the 7210 SAS-E version 2.0 or later, with a limit of one IP interface for a VPLS service. ICMP Ping on the management interface is also supported on 7210 SAS-E version 2.0 or later.	See Procedure 68-2 for more information.
Y.1731 Ethernet OAM enhancements on 7210 SAS-E	The 5620 SAM supports EthTest, One Way Delay, Two Way Delay, and Single Ended Loss tests on the 7210 SAS-E version 2.0 or later.	See chapter 35 for more information.
DDM on SFP enabled ports on 7210 SAS-E	The 5620 SAM supports Digital Diagnostics Monitoring (DDM) on SFP enabled ports on the 7210 SAS-E and 7210 SAS-M version 2.0 or later.	See "Digital diagnostics monitoring" and Procedure 17-61 for more information.
Q in Q Ethertype configuration on 7210 SAS-E	The 5620 SAM supports Q in Q Ethertype parameter configuration on the 7210 SAS-E version 2.0 or later. The Q in Q Ethertype parameter is configurable when the port Encap Type parameter is set to Q in Q.	See Procedure 17-61 for more information.

Support for 7705 SAR 3.0 R1	The 5620 SAM supports the following new functions on the 7705 SAR Release 3.0 R1:
	• Two-port channelized OC3/STM1 daughter card enhancements:
	  • CEM encapsulation for DS0 channel groups
	  • Unframed mode for DS1/E1 channels
	• One-to-one LSP fast reroute
		See chapter 11 for more information about 7705 SAR support in the 5620 SAM.
		See the *5620 SAM NE Compatibility Guide* for information about compatible and supported device releases.

Web-based client installation and uninstallation	You can install and uninstall 5620 SAM clients using a web browser that opens a URL on a 5620 SAM main server.	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.
Support for 7705 SAR 3.0 R2	The 5620 SAM supports the following new functions on the 7705 SAR Release 3.0 R2: • 1+1 APS on the four port OC3/STM1 daughter card. Support is consistent with that of Release 8.0 of the SR-c12 NEs, with the following exceptions: Multichassis protection groups not supported. Unidirectional mode (except Uni1Plus1) not supported. Access mode channels not supported. Working and protection channels on the same MDA not supported. • Six-port E&M daughter card. • Expanded IES service support.	See chapter 11 for more information about 7705 SAR support in the 5620 SAM. See the *5620 SAM NE Compatibility Guide* for information about compatible and supported device releases.
IGMPv3 snooping on 7210 SAS-E	The 7210 SAS-E Release 2.0 or later supports IGMP snooping with a default version of IGMPv3.	See chapter 28 and Procedure 28-36 for more information.
OS 6855 U24X	Stackable version of the OS 6855. Up to four OS 6855 U24X, Release 6.4.2 chassis are stackable.	See chapter 11 and Procedure 17-39 for more information.
OmniSwitch UDP relay and DHCP Option-82 and snooping	UDP relay and DHCP Option-82 and snooping on the default routing instance for Release 6.4.2 or later of the OS 6400, OS 6850, OS 6855, OS 9600, OS 9700, and OS 9800. This feature applies to the default routing instance of the OS 9700E and OS 9800E NEs. Only UDP Relay service applies to VRF instances of the OS 9700E and OS 9800E NEs.	See chapter 27 and Procedure 27-3 for more information.
PIM support in VRF mode on OS 9700E and OS 9800E	PIM under each VRF instance (to a maximum of eight instances, including the default routing instance) is supported on OS 9700E and OS 9800E NEs, Release 6.4.2.	See Procedures 27-1, 28-32, and 28-34 for more information.

(12 of 22)

Feature or function	Description	Reference for more information
OmniSwitch release support	• Release 6.4.2 for OS 6400, OS 6850, OS 6855, OS 9600, OS 9700, and OS 9800. • Release 6.6.2 for OS 6250M (Metro) and OS 6250SME (Enterprise) (OAM tests are not supported)	See chapters 11 and 35 for more information.
Fallback authentication on RADIUS failure	The 5620 SAM supports pre-defined options for subscriber authentication if the RADIUS server fails. The 5620 SAM supports a default option for MSAPs if a RADIUS server is not configured.	See Procedures 18-12, 64-8, and 64-34 for more information.
Default DNS configuration	The 5620 SAM supports the configuration of an IP address (IPv4 format) of a primary or secondary DNS server on a VPRN subscriber interface. The 5620 SAM supports default DNS configuration on a VPRN and IES subscriber interface for PPPoE hosts that have a static IP address.	See Procedures 70-7 and 71-10 for more information.
Authentication policy AVP enhancements	The 5620 SAM supports enhancements on subscriber authentication policies and RADIUS-based accounting policies to include additional AVP values.	See Procedures 18-12 and 54-1 for more information.
RADIUS accounting message attributes	The 5620 SAM supports RADIUS accounting message attributes.	See chapter 54 for more information.
Lawful intercept subscriber host activation via RADIUS	The 5620 SAM supports LI subscriber host activation using RADIUS. The 5620 SAM displays LI subscriber host information in a mirror service context.	See chapter 31 for more information.
AA group policy management enhancements	The 5620 SAM supports a simplified process for the deletion of an AA application, application group, or custom protocol.	See Procedure 73-11 for more information.
Pseudo-wire redundancy for mirror service	The 5620 SAM supports the following functions for mirror services on the 7750 SR, 7450 ESS and 7710 SR, Release 8.0 or later: • endpoint • redundant SAP • redundant mirror SDP binding • forced switchover capability • remote source ICB	See chapter 69 for more information.
9500 MPR support	The following 9500 MPR features are supported: • Cpipe for ETSI 1.4, ANSI 2.1, and ANSI 2.2 • Epipe for ANSI 2.1 and ANSI 2.2 • Apipe for ETSI 1.4 • dot1Q VLAN service for ETSI 1.4 • 1 × radio modem card (MD300) for ANSI 2.2 • Backup/restore for 9500 MPR NEs • Cross launch of 9400 AWY J-USM manager	See chapters 11, 67, and 72 for more information. See Procedure 21-3 for more information. See Procedure 65-8 for more information. See procedure 12-6 for more information.
BGP VPLS	The 5620 SAM supports the configuration of BGP VPLS. A service configured as BGP VPLS can interconnect with another BGP VPLS across different VPLS domains.	See Procedure 68-6 for more information.
Dry contact relay inputs	The 5620 SAM supports the configuration of dry contact sensors for the 7210 SAS-M24F2XFP [ETR]	See Procedure 17-78 for more information.
Egress SAP statistics and ingress SAP stats accounting records	The 5620 SAM supports the collection of egress SAP statistics and ingress SAP stats accounting records on the 7210 SAS-E.	See Procedures 67-11 and 68-3 for more information.
LACP tunneling in VLL service	The 5620 SAM supports LACP tunneling in VLL services for the 7210 SAS-M and 7210 SAS-M24F2X NEs.	See Procedure 17-23 for more information.

(13 of 22)

Feature or function	Description	Reference for more information
Service MTU check	The 5620 SAM supports performing a service MTU check for the 7210 SAS-M and 7210 SAS-M24F2X NEs in VPLS and VLL Epipe services.	See Procedures 67-1 and 68-1 for more information.
Link loss forwarding	The 5620 SAM supports link loss forwarding (LLF) functions for the 7210 SAS-M and 7210 SAS-M24F2X NEs in VLL Epipe services.	See Procedure 67-11 for more information.
7210 SAS-M24F2XFP [ETR] chassis support	The 5620 SAM supports the 7210 SAS-M24F2XFP [ETR] chassis.	The 7210 SAS-M24F2XFP [ETR] designation has been added throughout the User and Parameter guides, where applicable.
Egress queue statistics	The 5620 SAM supports the collection of egress queue statistics on the 7210 SAS-E.	See Procedure 17-61 for more information.
Consolidated glossary	A new standalone glossary has been created. This new guide is a consolidation of all previous glossaries that were components of the individual guides in the 5620 SAM documentation suite.	—
Release 8.0 R1 features		
In-band and out-of-band management enhancements	Changes to labeling of device management IP addresses for in-band and out-of-band device management.	See chapter 12 for more information about device management.
Device discovery and management over IPv6	The 5620 SAM supports IPv6 addresses in discovery rules, as well as management addresses. IPv6 device management includes: • SNMP trap handling • management access filter support • SNMP error retrieval • Telnet support • ping policy support • FTP support • software distribution and upgrade • accounting statistics • CLI scripting	See chapters 12 and 13 for more information about device discovery and management using IPv6.
Layer 2 Tunneling Protocol support	The 5620 SAM supports the following L2TP configuration and management on the 7750 SR, Release 7.0 and 8.0, and on the 7450 ESS in mixed mode: • protocol sites • tunnel group profiles • tunnel profiles	See chapter 28 for more information about configuring L2TP.
Network Address Translation	The 5620 SAM supports subscriber-based NAT configuration for the 7750 SR on the following: • base NE routing instances, for use in IES • VPRN routing instances	See chapters 27, 70, and 71 for more information.
Cflowd	The 5620 SAM supports the configuration of cflowd collectors for the 7710 SR, 7750 SR, and the 7450 ESS in mixed mode, on the base routing instance and on ISA-AA groups.	See chapters 27 and 73 for more information.
ESM enhancements for L2TP	The local user database supports the configuration of L2TP.	See Procedure 64-34 for more information.
L2TP Access Concentrator support	The 5620 SAM supports the LAC on the 7750 SR, Release 7.0 and 8.0, and the 7450 ESS in mixed mode.	—

(14 of 22)

Feature or function	Description	Reference for more information
L2TP Network Server support	The 5620 SAM supports the LNS on 7750 SR, Release 8.0. You can configure an IES or VPRN group interface to terminate LNS PPP sessions.	See Procedures 70-8 and 71-11 for more information.
ISA-LNS group	The 5620 SAM supports the creation and configuration of ISA-LNS groups. ISA-LNS groups are created to provide LNS PPP sessions termination. You can add broadband application MDAs to an ISA-LNS group, and up to four ISA-LNS groups on each NE.	See section 15.9 and Procedure 17-19 for more information.
ISA broadband application MDA support	Supports the configuration of the ISA broadband application MDA on 7750 SR IOM3 XP cards.	See section 15.16 for more information about daughter card support.
Dynamic ARP host type	A dynamic ARP host is configurable on a VPLS SAP, and an IES or a VPRN group interface. You can configure an ARP host on a VPRN subscriber interface when the interface is a retailer interface. The 5620 SAM supports the following functions: • retrieving and displaying ARP hosts • listing managed routes for ARP hosts • collecting statistics for the number of ARP triggers, and the number of created and deleted ARP hosts	See chapter 64 for more information about ARP hosts. See Procedures 64-33, 68-3, 70-8, 71-10, and 71-11 for more information.
Policy distribution scalability enhancements	The 5620 SAM supports improved policy distribution. To improve policy performance, multi-threading is introduced for policy distribution, global policy releasing, and global policy creation by the first local policy discovery.	See chapter 43 for more information.
DHCP options in RADIUS authentication request	A new RADIUS attribute allows for DHCP options to be included in RADIUS VSAs of authentication requests and responses.	See Procedure 18-12 for more information.
Traffic mapping based on Exp bits	Support for LspExp rules on the 7750 SR, 7450 ESS, and 7710 SR Release 8.0R1. LspExp rules map ingress traffic to ingress queues based on the value in the Exp field.	See chapter 44 for more information.
Queue specific WRED support extended to 7750 SR-c12.	The 5620 SAM supports Queue specific WRED support on IOM3 and IMM cards on 7750 SR, as introduced in 5620 SAM Release 7.0 R4. For 5620 SAM Release 8.0 R1, support is extended to 7750 SR-c12 NEs.	—
Common software images for multiple devices	Support for applying a common software image to 7450 ESS, 7750 SR, and 7710 SR devices	See Procedures 21-11 and 21-18.
Multiple NE types as script targets	You can specify multiple types of devices as the targets of a CLI script.	See the *5620 SAM Scripts and Templates Developer Guide* for more information.
Down MEP creation on Ethernet Subscriber Group Interface SAPs	You can create Down MEPs on relevant Ethernet VPRN and IES Subscriber Group Interface SAPs when creating a new service binding in Global Maintenance Association.	See Procedure 64-25 for more information.
Support for CFM diagnostic tests	CFM diagnostic tests are supported by VLL and VPLS test policies and test suites.	See chapter 35 for more information.
Extended MEP support	• Down MEPs may be created on Ipipe SAPs • Up MEPs may be created on Epipe SAPs and Ethernet spoke SDP binding Epipe	See chapter 44 for more information.
MEP Fault Propagation	You can configure Fault Propagation when configuring a MEP on a SAP or an SDP Binding.	See Procedures 64-25 and 64-26 for more information.

(15 of 22)

Feature or function	Description	Reference for more information
Support for 7705 SAR, Release 3.0	The 5620 SAM supports the following new functions on the 7705 SAR, Release 3.0: • Four port DS3/E3 ASAP daughter card • IP service tunnels: see procedure 30-1 for more information. • VLL switching sites • VPRNs • Synchronous Status Messages (SSM) • Active/standby VLL Redundancy • Y.1731 Ethernet OAM enhancements Support for EthTest, One Way Delay, Two Way Delay, and Single Ended Loss tests on the 7705 SAR. See chapter 35 for more information. • Sixteen member IMA bundles: support for up to 16 members per IMA bundle on the 7705 SAR 16 port DS1/E1 ASAP daughter card. • Two tier scheduling on Ethernet MDA: support for Egress Scheduler Mode for network ports on the 7705 SAR8 port Ethernet daughter card. See procedure 17-61 for more information. • Routing policies: support for community, damping, and AS path policies. • ACL IP Filter Entry Statistics: support for Ingress Hit Byte Count within the Hit Count record for ACL IP Filter Entries. • Route Statistics: support for route aggregation and BGP statistics within the Route Stats record of VPRN sites and the routing instance. • DHCP Relay on network interfaces. See procedure 27-4 for more information. • Routing instance AS number: support for an autonomous system number on the Routing tab of the Routing Instance properties page. • Route aggregation: support for various properties associated with AS numbers under the Route Aggregation tab of the Routing Instance properties page. • IP Addresses: support for the Broadcast Address Format property for VPRN L3 access interface addresses. • Border Gateway Protocol	See chapter 11 for more information about 7705 SAR support in the 5620 SAM. See the *5620 SAM NE Compatibility Guide* for information about compatible and supported device releases.
Hierarchical policing support	The new policer control policy object provides a control hierarchy for policer objects configured on SAPs or subscriber contexts. Supported on IOM3 cards on the 7750 SR and 7450 ESS.	See chapter 43 for more information.
Hybrid port mode	The 5620 SAM supports the configuration of hybrid ports on the 7710 SR, 7750 SR, and on the 7450 ESS in mixed mode. A hybrid port can function as a network port and an access port simultaneously.	See chapter 15 for more information.
Multiple IS-IS instances	You can configure multiple IS-IS instances on an NE base routing instance.	See chapter 27 for more information.
Client GUI enhancements	The 5620 SAM client GUI improvements include the following: • increased efficiency of JMS event processing and database queries to increase responsiveness • time of previous search shown in list tables • more user-friendly layouts in configuration forms • auto-population of all selection lists	—

(16 of 22)

Feature or function	Description	Reference for more information
9500 MPR support	The 5620 SAM supports ETSI 1.2.2 or later and ANSI 2.0.1 or later versions of the 9500 MPR. • trusted manager support provides SNMP registration in the persistence memory for discovered 9500 MPR NEs and is supported for ETSI 1.3 or later • performance monitoring using IMA counters per group and ATM counters per VPI/VCI (Historical statistics collection is not supported for ETSI 1.3.0.) • 16 x E1 ASAP Access card (ETSI 1.3.0) • IMA support for ETSI 1.3.0 • Apipe for ETSI 1.3.0 • CBR, UBR, and UBR+ flows (ATM QoS policy) support for ETSI 1.3.0 • Port Segregation • 2 x DS3 card for ANSI 2.0.1 or later • MPT support via the 4+4 x Ethernet (EAS) card, for ANSI 2.0.1 or later • Cpipe for ANSI 2.0.1 or later and ETSI 1.3.0 • Epipe for ANSI 2.0.1 • Service Aggregator • Composite services for Cpipe, Apipe, and Epipe with 7705 SAR NEs • Error recovery mechanism on 9500 MPR NEs	See chapters 11, 15, 17, 67, and 72 for more information. See Procedure 17-70 for more information. See Procedure 44-30 for more information. See Procedure 34-10 for more information.
7210 SAS-M cards	The 7210 SAS-M is available in two variants: • 7210 SAS-M24F (renamed from 7210 SAS-M) • 7210 SAS-M24F2XFP (new as of 5620 SAM, Release 8.0)	—
7210 SAS-M enhancements	The 7210 SAS-M, Release 1.1 R6 or later, supports the configuration of IGMP snooping for VPLS.	See Procedure 68-3 for more information.
New card support	The 5620 SAM supports the 48 × Gig Ethernet Extended Performance Tx MDA on the 7750 SR-12, 7750 SR-7, 7450 ESS-12, 7450 ESS-7, 7450 ESS-6, and 7450 ESS-6v.	–
ISA-Video on IOM 3 cards	The 5620 SAM supports the ISA-Video MDA on IOM 3 cards on the 7450 ESS-6, 7450 ESS-7, 7450 ESS-12, 7750 SR-7, and 7750 SR-12.	See section 15.11 for more information about ISA-Video support.
7450 ESS mixed mode chassis support	The 7450 ESS-6v, 7450 ESS-7 and 7450 ESS-12 support the 7750 SR IOM3-XPs and associated MDAs and IMMs. When the 7450 ESS is in legacy mode, the IOM3-XPs and associated MDAs and IMMs function as 7450 ESS cards. When the 7450 ESS is in mixed mode, the IOM3-XPs and associated MDAs and IMMs function as 7750 SR cards.	See the Mixed Mode State on Chassis Enabled parameter in section 163.1 for more information.
ISA-AA partitions	The 5620 SAM supports the configuration of ISA-AA partitions. You can partition an AA group into AA policy partitions with one partition for each VPN-specific AA service.	See Procedures 73-1, 73-2, 73-3, and 73-5 for more information. See section 15.7 and Procedure 17-17 for more information.
ISA-AA groups	The 5620 SAM supports up to seven ISA-AA groups to allow AA resource partitioning and reservation for different types of AA services.	See section 15.7 and Procedure 17-17 for more information.
Custom pattern-based AA protocol support	You can identify operator-specific or customer-specific custom-built applications that cannot be uniquely identified using Alcatel-Lucent global scope protocol signatures.	See Procedure 73-3 for more information.

(17 of 22)

Feature or function	Description	Reference for more information
Protocol shutdown for new signature upgrade	The 5620 SAM supports signature upgrades without automatically affecting policy behavior. All post-R1 new signatures are disabled by default during an upgrade to ensure that no policy or service impacts occur.	See chapter 73 for more information.
Application filter expression match extensions	The 5620 SAM provides greater flexibility in application definition.	See Procedure 73-3 for more information.
5620 SAM user security enhancements	The span of control function is extended to customers and services, and special spans can be applied to block access to objects. Also, you can use policies called span rules to automatically assign new services to spans.	See chapter 8 for more information.
Capacity-cost based load balancing	Capacity-cost based load balancing allows a cost to be assigned to diverted SAPs using an application profile. The cost is used for load balancing SAPs between ISAs and for a threshold that notifies the user if capacity planning is exceeded.	See Procedures 17-17 and 73-3 for more information.
Spoke SDPs	The 5620 SAM supports the diversion of spoke SDPs to the ISA-AAs. Application profiles are assignable to a spoke SDP for diversion from the following service types: VPLS, IES, VPRN, and Epipe.	See Procedures 67-1, 68-5, 70-6 and 71-8 for more information.
Spoke SDP AA performance and real-time statistics	The 5620 SAM supports AA performance and real-time statistics collection on diverted spoke SDPs.	See chapter 10 for more information. See Procedures 73-7 and 73-8 for more information.
ISA-AA only upgrade	ISA-AA only upgrades are independent of CPM ISSU restrictions, and are therefore allowed from any load to any other load.	—
MC endpoint group	Supports grouping of multiple spoke SDPs with two MC endpoint peers to ensure that only one spoke SDP is active and therefore eliminates traffic loops in a VPLS.	See chapter 39 for more information.
7750 SR-c12 enhancements	The 7750 SR-c12, Release 8.0 R1 or later, supports PBB access dual-homing and MAC naming.	—
FRF.12 interleaving	Supports a mode of operation for the fragmentation of the FR SAP in the transmit direction. High-priority frames and fragments of low-priority frames can be interleaved.	See chapters 67, 68, 70, and 71 for more information.
Wavelength tracker and OTU support	Tracks optical power and the identity of DWDM wavelengths across the optical network, and adjusts and balances the optical power at each point in the transport network.	See Procedure 17-61 for more information.
OS 6250, OS 9700E, and OS 9800E	OS 6250M (Metro) and OS 6250SME (Enterprise):Layer 2+ Fast Ethernet Stackable LAN family of switches for the enterprise and Ethernet access segments. Supports OS 9700E and OS 9800E that are high performance switches offering eight and 16 slots respectively for Gigabit Ethernet and/or 10-Gigabit Ethernet network interface modules.	See chapter 11,chapter 15, chapter 16, Procedure 17-38, and Procedure 17-39 for more information.

(18 of 22)

Feature or function	Description	Reference for more information
OS 9700E and OS 9800E	Additional OS 9700E and OS 9800E features: • ISSU support for Release 6.4.2 R1 • OSPFv2, RIP routing protocols • Multicast protocols: IGMP and PIM • Multiple VRFs using SNMPv3 NE management • MPLS, LDP, Static LSPs • VPLS	See Procedure 21-13 for more information. See Procedure 27-1 for routing instance information, including VRFs. See chapter 28 for routing protocol and LDP information. See chapter 29 for MPLS and LSP information. See chapter 30 for service tunnel information. See chapter 68 for VPLS information.
Task Manager enhancements	The Task Manager supports: • tracking of additional tasks; for example, bulk changes, resynchronizations, and collecting statistics • Task Name column displays the user-friendly name of the task; for example, MC Peer Group, [Create] • navigation tree for each task	See Procedures 2-14 and 2-15, and the *5620 SAM-O OSS Interface Developer Guide* for more information.
IPsec VPN	Supports the creation and management of the association between IPsec components, public and private services, to form a secured VPN.	See chapter 32 for more information.
BFD for static LAN-to-LAN IPsec tunnels	Support for BFD for static LAN-to-LAN IPsec tunnels on the 7750 SR7, and 7750 SR12.	See chapter 32 for more information.
Service CAC on PBB	Support for CAC on the 5620 SAM is extended to PBB Epipes.This extended support enables the 5620 SAM to monitor bandwidth usage in the network to automatically select the best tunnel based on the number of active links and on the available bandwidth.	See chapter 60 for more information.
IGH support	Supports the ability to group multiple IP links and POS links into a fate-sharing group. If a configured number of links go out of service for any reason, all of the remaining links in the fate-sharing group go out of service and can be rerouted to an alternate path.	See section 15.13 for more information.
LAG enhancements	The number of ports that can be added to or removed from a LAG on IOM3 and IMM cards in chassis mode D is increased to 16 ports. LAG hashing provides consistent per-service forwarding for frames that belong to an Ethernet service. The number of MC LAG peer groups is increased to 20.	See section 15.12 for more information. See section 68.5 for more information. See section 38.1 for more information.
CPM filters and queues	The 7750 SR-c12 supports CPM filters and queues.	See Procedure 18-2 for more information about CPM filters and queues.
APS enhancement	The 7750 SR-c12 supports configuration of unidirectional 1+1 signaling data.	See Procedure 37-1 for more information.

(19 of 22)

Feature or function	Description	Reference for more information
OSPFv3 authentication	IPsec static security associations provide OSPFv3 authentication.	See Procedure 32-3 for information about creating IPsec static security associations. See Procedure 28-11 for information about configuring OSPF on a routing instance. See Procedure 28-16 for information about configuring virtual links.
7210 SAS-M24F2XFP Release 1.0	The 7210 SAS-M24F2XFP Release 1.0 supports 2 x 10 GigE ports, in addition to all of the features of the 7210 SAS-M.	See section 11.1 for more information.
GUI map enhancements	The client GUI map improvements include the following: • filtering functions • mouse-over detail display for map elements • support for up to 500 elements in a topology group • next/previous function to sequentially change the object focus for multiple search results • panning	See chapter 4 for more information.
Support for vi editor in GUI CLI windows	The UNIX vi editor is available in NE CLI windows that you open using the client GUI.	See chapter 2 for more information.
Remote user session limits	You can configure the maximum number of concurrent OSS or GUI user sessions that the 5620 SAM allows for the same account.	See chapter 8 for more information.
5620 SAM database security enhancements	During a 5620 SAM database installation or upgrade, you must assign a password to the Oracle management user; also, the permissions on the files and directories associated with the Oracle management user account are more strictly applied.	—
LSP-ping and LSP-trace for P2MP RSVP LSP	Introduces new OAM tests: LSP-ping and LSP-trace for P2MP RSVP LSP.	See chapters 29, 35, and 75 for more information.
Ethernet SAP OAM (AIS, CC, ELMI) mapping	Introduces “fault propagation” for a MEP. OAM mapping enables a method of deploying OAM end-to-end in a network where different OAM tools are used in different segments. Also introduced support for a MAC address on a MIP.	See chapters 64, 67, 68, 70, and 35 for more information.
BFD for T-LDP	Introduced for BFD support on SR 7750/7450/7710 to implement a mechanism that provides for sub-second IGP convergence.	See chapters 27 and 28 for more information.
GR helper for PE-CE protocols	Introduces support for Graceful Restart functions for CE-PE routing protocols for 7750 SR and 7710 SR.	See chapter 28 for more information.
BFD support of OSPF CE-PE adjacencies	Introduces support for bi-directional forwarding in VPRN services.	See chapter 71 for more information.
Spoke termination for IPv6 IES and 6VPE	Introduces support for IPv6 spoke termination on IES and VPRN services by modifying the Tunnel Termination Site parameter.	See chapter 14 for more information.
Support for MPLS hash label	Introduces support for the MPLS hash label, which allows LSR nodes in a network to load balance labelled packets in a more granular fashion than by simply hashing on the standard label stack.	See chapters 67, 68, 70, 71, and 43 for more information.
Multiple loopback for LDP and T-LDP	Introduces the ability to configure and initiate multiple T-LDP sessions on the same system using different LDP LSR-ID, and to use the LDP local interface address as the LSR-ID for the LDP sessions, instead of the system address.	See chapters 28 and 35 for more information.

(20 of 22)

Feature or function	Description	Reference for more information
RSVP LSP Primary and LDP LSP backup within a SDP	Introduces support to allow you to enable a “mixed mode” of both RSVP and LDP on an SDP starting from a release 8.0 SR or ESS NE.	See chapters 30 and 43 for more information.
“Make-before-break” re-signalling of primary RSVP-TE paths	Support for “make-before-break” procedures that allow you to manually replace an existing MPLS path under the primary or secondary LSP path with a new path	See chapter 29 for more information.
CLI command to enable/disable the “no-propagate-ttl” capability	Provides an option to specify if an LSP shortcut should operate in Uniform or Pipe mode. This allows you to hide or reveal the hops of your MPLS network when your customer packets are carried over an LSP shortcut.	See chapters 28 and 29 for more information.
Downstream on demand label for LDP (Tunnel only)	Introduces support for Downstream on-Demand (DoD) label allocation as per RFC 5036. It is only enabled on a link level LDP session, and applies to prefix labels only, not service labels.	See chapter 28 for more information.
Precedence support for LSP secondary paths	Introduced to support the path revert behavior when both standby and non-standby secondary LSP paths are configured.	See chapter 29 for more information.
LDP Shortcut feature for IP forwarding over MPLS	This feature allows forwarding of IP packets to IGP-learned routes using an LDP LSP.	See chapter 27 for more information.
Increase LDP adjacencies	Introduces support for increased scaling of LDP adjacencies required in backhaul networks.	See chapter 28 for more information.
G.8031 Ethernet tunnels for L2/L3 SC-access (L2 P1, same-fate SAPs)	Support for load sharing and for the creation of “same-fate SAPs” on an Ethernet tunnel. Same-fate SAPs allow operational control of multiple service SAPs by the control tags of an Ethernet Tunnel Endpoint.	See chapters 67 and 68 for more information.
IPVPN - VRF id based on strings	Introduced to allow service administrators to add an optional Service Name to services within the SR 7x50 and 7710 SR platforms (including Sparrow nodes).	See chapter 14 for more information.
Diff-Serv Class type change during failures	Introduces an option to configure a main Class Type and a backup Class Type for the primary path of a Diff-Serv TE LSP.	See chapter 29 for more information.
Full IGP Shortcuts and Forwarding Adjacencies	Introduced to allow forwarding of packets to IGP-learned routes using an RSVP-TE LSP.	See chapters 28 and 29 for more information.
IP pseudowire L3 termination	Support to allow termination of an Epipe/Ipipe into a L3 service, such as IES or VPRN.	See chapters 70 and 71 for more information.
T-LDP status TLV (Active/standby)	This feature enhances the fault propagation between PE devices in a spoke SDP termination between an Epipe/Ipipe and IES/VPRN service.	See chapter 67 for more information.
IS-IS and OSPF TE bandwidth updates triggered by threshold crossing events	Introduced to reduce the surge of TE updates in a network caused by LSP setup and removal, by defining threshold levels of TE update per interface.	See chapter 28 for more information.
IMPLICIT NULL label option support on egress LER	Introduced to allow a 7x50 egress LER to receive MPLS packets from the previous hop without the outer LSP label.	See chapters 28 and 29 for more information.
“AS-path multipath-relax” to load-share multiple BGP paths	Introduced to allow the AS-path comparison to be disabled on a per address family basis. This allows BGP routes which do not have equal AS paths to be considered equal, and therefore become load-balanced across more BGP routes.	See chapter 27 for more information.

(21 of 22)

Feature or function	Description	Reference for more information
PBB (MMRP) Scalability for inter-domain services	Introduced to limit the scope of MMRP advertisements to a specific network domain using ISID-based filters for both MMRP control plane and BVPLS data plane.	See chapters 43 and 68 for more information.
Traffic leaking to the GRT from a VPRN	Packets within a VRF are now able to perform a parallel lookup against a Global Route Table (GRT) as well as within the local VRF table.	See chapter 71 for more information.
Support for RFC3107 BGP label for L2 services	Introduces a new SDP option based on BGP route tunnels to support inter-AS VPLS/VLL service based on option C for SR 7x50.	See chapters 30 and 43 for more information.
IGP overload on switch fabric failure	Introduces an option to place IGP into overload on the failure of switch fabric.	See chapters 27 and 71 for more information.
PCP (dot1p) and DE bits transparency for PBB	This feature provides the ability to preserve the dot1p priority information of the incoming data and control traffic for PBB EPIPE and I-VPLS services.	See chapters 67 and 68 for more information.
RSVP Shortcut for BGP Next-Hop Resolution	Introduces a shortcut that allows forwarding of IPv4 packets to routes resolved to a BGP next-hop using an RSVP-TE LSP.	See chapter 28 for more information.
BGP Rapid Update for Multicast VPN Address Families	BGP Rapid Update capability is introduced to rapidly send BGP updates for C-multicast routes between PEs to improve join/prune latency.	See chapter 28 for more information.

(22 of 22)

3.2 5620 SAM Release 7.0 features

Table 3-2 lists the features and functions added in 5620 SAM Release 7.0.

Table 3-2 5620 SAM Release 7.0 features

Feature or function	Description	Reference for more information
Release 7.0 R6 features		
Network policy enhancement for the 7210 SAS-M. See the *5620 SAM Release 7.0 R6 Release Notice* for more information.		
Release 7.0 R5 features		

(1 of 18)

Feature or function	Description	Reference for more information
Support for 7705 SAR, Release 2.1	The 5620 SAM supports the configuration of MC MLPPP on the 7705 SAR on DS1/E1 channelized ASAP daughter cards.	See Procedure 17-101 in chapter 17 for more information about how to configure MC MLPPP.

	The 5620 SAM supports the following OAM functions on the 7705 SAR:
	• Support for 802.1ag CFM, identical to the functions supported for the 7750 SR, Release 6.0, except for the following:
	  • The 7705 SAR also supports the options 10 ms and 100 ms for the CCM Interval parameter.
	  • The Explicit option for the MHF-Creation parameter is not configurable.
	  • The Direction parameter cannot be set to Up.
	• Support for 802.3ah on Access ports (7705 SAR, Release 2.1 R2 or later) and disabling EFM OAM Tunneling on Access mode ports (7705 SAR, Release 2.1 R2 or later).
	• Support for the configuration of Forwarding Profile and Forwarding Class parameters on ICMP ping service assurance tests.
		See chapter 109 for more information about 802.1ag CFM parameters.
		See chapter 75 for more information about service assurance tests.

	The 5620 SAM supports the following daughter cards on the 7705 SAR: • 2 × Channelized OC3/STM1 ASAP SFP • 12 × Serial Data You can configure no more than two 2-port OC3/STM1 ASAP SFP daughter cards on a 7705 SAR. Each OC3/STM1 port supports channelization down to the DS0 channel group. You cannot configure channel groups that you create on this daughter card as management IES SAPS. You can configure up to 32 IMA bundles on the 2 × Channelized OC3/STM1 ASAP SFP daughter card. On the 12 × Serial Data daughter card, you must create a channel under each port, and a channel group under each channel. The following configuration restrictions and limitations apply to ports and channels on this daughter card: • maximum of one channel on each port • maximum of one channel group on each channel • channel groups must be in access mode and with CEM encapsulation type • channel group MTU is not configurable	See chapter 15 for more information about supported daughter cards. See Procedure 17-87 in chapter 17 for more information about how to configure SDH sub-channels. See Procedure 17-99 in chapter 17 for more information about how to configure IMA group bundles.
	The 7705 SAR supports Network mode with PPP Auto encapsulation for channels on the 4-port OC3/STM1 ASAP daughter card.	—

(2 of 18)

Feature or function	Description	Reference for more information
Support for 7705 SAR, Release 2.1 (continued)	The 5620 SAM supports the following routing functions on the 7705 SAR: • IS-IS • MPLS SRLG • SGT QoS—dot1p marking • SGT QoS—DSCP mapping The IS-IS support is identical to the support on the 7750 SR, Release 6.0. However, the 7705 SAR does not support the following: • Graceful Restart • Graceful Restart Helper • Unicast Import • Multicast Import • Multi-topology • IPv6 configuration	See chapter 28 for more information about IS-IS. See chapter 29 for more information about MPLS SRLG. See chapter 27 for more information about dot1p marking and DSCP mapping.
	The 5620 SAM supports the following policy functions on the 7705 SAR: • **Routing policy enhancements** You can use the 5620 SAM to configure existing global routing policy parameters and values associated with IS-IS on the 7705 SAR local routing policy. • **MC MLPPP Access egress policy** You can use the 5620 SAM access egress policy to configure MC MLPPP access egress policies.	See chapter 27 for more information about how to configure routing policies. See chapter 43 for more information about how to configure access egress policies.
	The 5620 SAM supports the following service functions on the 7705 SAR: • Epipe LLF • Epipe SAP-to-SAP In addition, the 5620 SAM supports the binding of ingress ACL IP Filters to the L2 Access Interfaces on an Epipe or Ipipe on the 7705 SAR.	See chapter 29 for more information about how to configure Epipes.
	The 7705 SAR supports the configuration of timed loopback for Ethernet ports.	See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports.
	You can use the 5620 SAM to configure the 7705 SAR as a client for IEEE 1588 PTP. The 7705 SAR supports the configuration of a PTP application within a DSCP application marking on routing instances.	See Procedure 17-34 in chapter 17 for more information about how to configure PTP. See Procedure 27-1 in chapter 27 for more information about how to configure DSCP application marking settings.
	The 7705 SAR supports the configuration of the Radius Authorization Algorithm parameter for NE RADIUS authentication policies.	See chapter 18 for more information about how to configure NE RADIUS access.
Auto-provisioning enhancements	Enhancements include: • A source configuration file can be imported from the 7705 SAR. • A backup can be performed from the Auto-Config Source Node Profile. • The supported VLL services include Ipipes. • The IS-IS routing protocol is supported	See chapter 26 for more information.

(3 of 18)

Feature or function	Description	Reference for more information
7210 SAS-E enhancements	The 7210 SAS-E, Release 1.0 R5 or later, supports egress port rate limiting and frame-based accounting.	See chapter 17 for more information.

7210 SAS-M Release 1.1 R3 support	The 5620 SAM supports the following features on the 7210 SAS-M, Release 1.1 R3 or later:
	• 24 × 10/100/1000 Ethernet SFP ports
	• in-band management
	• egress port rate limiting
	• frame-based accounting
	• services
	  • VLL Epipe
	  • VPLS (ELAN)
	  • Spoke SDP binding
	• STM OAM: CRM, EFM, CPE Ping, LSP Ping, MAC Ping, SDP/Tunnel Ping, MTU Ping, VCCV Ping, ICMP Ping, SVC Ping, DNS, LSP Trace, MAC Trace, MAC Populate, MAC Purge, and ICMP Trace
	• QoS policies:
	  • 7210 Access Ingress
	  • 7210 Access Egress
	  • 7210 Network Queue
	  • 7210 Slope
	  • 7210 Port Scheduler
	• discovery management
	• configuration backup and restore
	• policy audit
	• remote CLI
	• security management
	• software upgrade
	• span of control
	• statistics collection and graphing
	• alarm management
	• routing
	  • static routes
	  • IS-IS
	  • OSPF
	• IP/MPLS
	  • TLDP
	  • RSVP
		See chapters 11, 12, 15, 17, 35, 44, 67, and 68 for more information.

Topology map enhancements	The map layout is enhanced to include the following: • Circular and Smart Organic layouts • Links Shown button • Select Attached menu item	See chapter 4 for more information.
Generic NE alarm enhancements	Generic NE alarm mappings can include one or more transform functions that dynamically define the alarm name, probable cause, and severity properties using SNMP trap varbind values.	See chapters 11 and 12 for more information.

(4 of 18)

Feature or function	Description	Reference for more information
ISA multi-service daughter card support	You can assign one of the following MDAs to an ISA-MS equipped slot: • ISA-IPsec • ISA-Video • ISA-AA After you assign the MDA to the slot, the MDA can be used for the MDA-specific application. Some configuration changes require that you reboot the IOM; for example, you must reboot the IOM when you switch from ISA-AA to ISA-Video.	See section 15.16 in chapter 15 for more information about daughter card support.
Support for the 9500 MPR	The 5620 SAM supports ETSI 1.2.2, or later and ANSI 2.0 or later versions of the 9500 MPR. • admission control on ETSI NEs, R1.2.2 or later • 32 x DS1 card, ANSI R 2.0 or later • 4+4 x Ethernet card (ANSI) • port protection • MSS-8 chassis • Core -E module • fault management • performance management • timing synchronization ANSI 2.O NEs do not support service provisioning, including VLAN Groups and Paths.	See chapters 11 and 17 for more information.
Release 7.0 R4 features		
New 7750 SR-c12 chassis	The 7750 SR-c12, which supports up to 12 CMAs or 6 MDAs, has a forwarding capacity of 40 Gb/s, native uplink support, and a faster control plane processor than the 7750 SR. The 7750 SR-c12 has the features that are supported on the 5620 SAM for the 7750 SR, Release 7.0, except for the following: • ISA-AA, ISA-IPSEC, and ISA-Video • IMM • BGP-AD • limited support of DOS filtering and MAC filtering to the CPU The CMAs and MDAs supported on the 7710 SR-c12 are supported on the 7750 SR-c12. You can configure the following card types in the 7750 SR-c12 card slots: • 7750-SRc12 IOM-XP • 7750-SRc12 CFM-XP	See chapter 11 for more information about supported devices.
New card support	The 5620 SAM supports the IMM 5 × 10GE Extended Performance XFP MDA on the 7750 SR-7 and 7750 SR-12, Release 7.0 or later.	See section 15.16 in chapter 15 for more information about daughter card support.
	The 5620 SAM supports the following cards on the 7750 SR-c12 • 20 × 10/100/1000 Ethernet SFP MDA • 10 × 1Gig Extended Performance SFP MDA • 20 × 1Gig Extended Performance SFP MDA	
7710 SR daughter card support	The 5620 SAM supports the 1 × Gig Ethernet XP SFP CMA on the 7710 SR.	

(5 of 18)

Feature or function	Description	Reference for more information
Multi-chassis redundancy enhancements	The MC peer, MC synchronization, MC ring, and MC LAG functions are streamlined for ease of configuration, status viewing and operation.	See chapters 38 to 42 for information.
Card migration utility	The 5620 SAM includes a utility that you can use to transfer the configured objects from one or more IOM 1 and IOM 2 cards on multiple NEs to IOM 3 cards.	See chapter 22 for information about performing card migrations.
ISA-Video	The 5620 SAM supports the ISA-Video MDA on the 7450 ESS-6, 7450 ESS-7, 7450 ESS-12, 7750 SR-7, or 7750 SR-12, Release 7.0 or later.	See section 15.11 in chapter 15 for more information about ISA-Video support.
ISA-AA MDA support	The 5620 SAM supports the ISA-AA MDA on IOM 3 cards.	—
Hard reset prevention on 7710 SR	A hard reset of MDAs, CMAs, and MCMs of the 7710 SR, Release 7.0 or later, is no longer required, after an ISSU upgrade.	See Procedure 21-11 for more information.
Support LDP over RSVP on IS-IS and OSPF	The 5620 SAM support of LDP over RSVP for MPLS tunnels is extended to include IS-IS and OSPF on the 7750 SR, 7710 SR, and 7450 ESS.	See section 28.1 for more information.
MAC subnetting support	The 5620 SAM supports MAC subnetting on the 7750 SR, 7710 SR, and 7450 ESS. This solution for MAC scalability involves MAC learning and MAC switching.	See the MAC Subnet Length (macSubnetLength) parameter in section 4.1 for more information.
SLA-based egress QoS marking	Egress QoS marking can be derived from the egress QoS policy associated with a SAP or from the egress QoS policy associated with the SLA profile.	See Procedure 64-3 for more information.
Queue-specific WRED support	WRED can be enabled on a per queue basis in the egress QoS policy and in the egress queue group template policy for IOM 3 and IMM cards.	See chapters 44 and 17 for more information.
Queue groups	Queue groups are objects created on access or network Ethernet port that allow SAP or IP interface forwarding classes to be redirected from standard queue mapping to a shared queue.	See chapter 61 for more information.
OAM test ID ranges	You can configure a test ID for the OAM tests in multiple server environments. A test ID allows you to identify the source server that initiated the OAM test.	See OAM test ID ranges in section 75.1 for more information.
New premium (HSMDA) daughter card support	The 5620 SAM supports the following premium HSMDAs on the 7750 SR-7, 7750 SR-12, 7450 ESS-6, 7450 ESS-7, and 7450 ESS-12, Release 7.0 R3, or later. • HSMDA 10 Gigabit XFP with 1-port configurations, supported on IOM1, IOM 2 and IOM 3 card slots. • HSMDA Gigabit Ethernet SFP with 10 ports, supported on IOM 3 card slots. For HSMDAs supported on IOM 3 card slots, in addition to HSMDA pool policies, ingress named buffer pool policy is supported. Network ingress, network egress, access ingress, and access egress QoS pool policies, except for MC path management, are configurable.	See chapter 15 and Procedure 17-41 for more information.
New daughter card	The 5620 SAM supports the 10 Gigabit Ethernet MDA with 1-port DWDM tunable optics configurations on the 7750 SR and 7450 ESS.	See Procedure 17-61 for more information.
Egress Secondary Shapers configurable on LAGs of HSMDA ports	Egress secondary shapers can be added to port members of a LAG configured on an HSMDA on the 7750 SR-7, 7750 SR-12, 7450 ESS-6, 7450 ESS-7, and 7450 ESS-12, Release 7.0 R3, or later.	See Procedures 17-23 and 17-61 for more information.

(6 of 18)

Feature or function	Description	Reference for more information
Bulk change support	Modify a large number of objects by setting filter and attribute definitions. Display progress of changes and report success and failures.	See chapter 24 for more information.
Generic NE alarm support	You can configure the 5620 SAM to raise specific alarms in response to specific generic NE SNMP traps.	See chapters 11 and 12 for more information.
Generic NE statistics support	You can use the 5620 SAM to collect statistics from the standard system and interface MIBs on generic NEs. A 5620 SAM deployment that includes the 5650 CPAM allows for the collection of statistics from a number of standard generic NE routing MIBs as well.	See chapters 11 and 12 for more information.
OmniSwitch support enhancements	The 5620 SAM supports the following features for the OmniSwitch: • AOS 6.3.4 • IP multicast VLANs that do not have common access ports can share the same multicast addresses. • For AOS 6.3.4 or later, the maximum number of dynamically learned IGMP group addresses can be limited globally, per port, and per multicast VLAN. You can also specify the action to be taken when the limit is exceeded. • The total number of LAG links per switch is increased to 128 for the OS 9600, OS 9700, and OS 9800.	See Procedures 28-37, 28-51, and 65-11 for more information.
LSP on-demand resynchronization support	On the 7750 SR and 7710 SR, LSPs can be manually resynchronized while the 5620 SAM scheduled resynchronization function is disabled. This function applies to some LSP objects that are associated with poor server performance under certain network failure conditions.	See chapter 29 for more information.
MSAP enhancements	Event logs record the date, time, and state for every state change of an MSAP. You can also view the MSAP creation date and time and the date and time of the last active state change.	See Procedures 64-9 and 64-13 for more information.
STM enhancements	Enhancements to improve the usability of the Service Test Manager include the ability to: • select the type of objects displayed by the STM • view the test results for a tested entity • compare the test results from two tests of the same type • select the test suite results for a tested entity • view validation results for each tested entity	See Procedures 75-3, 30-10, 67-16, 68-22, 71-17, 75-15, and 75-16 for more information.
ESM enhancements	The 5620 SAM supports ESM Dynamic Host Persistence, which provides persistence of subscriber host information that binds a host to a SAP, IP address or MAC address. This provides troubleshooting functions while avoiding unnecessary network queries. This feature is supported on the 7750 SR, 7450 ESS, and the 7710 SR, Release 5.0 or later.	See Procedure 64-33 for more information.
Host tracking	The 5620 SAM supports a host tracking policy and configuration of IGMP host tracking parameters on VPLS, IES, and VPRN service sites and SAPs. The host tracking policy is applied to a residential subscriber profile and allows a subscriber's video traffic (multicast) to be included in the egress rate control for the subscriber. You can collect, view, and clear on-demand host tracking statistics and information.	See Procedures 64-2, 64-18, 64-38, 68-1, 68-3, 70-1, 70-8, 71-1, and 71-11 for more information.

(7 of 18)

Feature or function	Description	Reference for more information
PBB Ethernet (G.8031) tunnel support	The 5620 SAM provides enhancements to the PBB E-PIPE service to ensure 100 millisecond failover over a native Ethernet core in the case of failure of a backbone NE or link. The 5620 SAM supports the creation of Ethernet (G.8031) tunnels, endpoints, and paths.	See Procedures 30-5 and 30-6 for more information.
Generic NE Layer 3 support	The 5620 SAM supports the read-only management of third-party generic NEs using the standard MIBs of Routing Protocols.	See Procedure 12-4 for more information.
PBB Access Dual-Homing enhancements	PBB Access Dual-Homing provides a non-MSTP or non-RSTP solution for black-hole avoidance. The enhancements address both ELINE (E-PIPE) and ELAN (I-VPLS) scenarios when MC LAG is used for access dual-homing. PBB access dual-homing is supported on all 7450 ESS and 7750 SR product lines on the following IOM and MDA cards with chassis mode D restriction: • IOM 3 LAVA • MAGMA Access dual-homing is restricted for use only with MC LAG SAP.	See Procedures 68-11, 40-1, and 17-48 for more information.
SAA Accounting Files	The 5620 SAM supports the configuration of SAA Accounting Files for the collection of test results from NE Schedulable Test Suites.	See sections 75.5 and 75.6 for more information.
Discover into group	The 5620 SAM allows the user to choose the destination Topology Group for all newly discovered NEs.	See the Group Name (topologyGroupPointer) parameter in section 147.1 for more information.
Tabbed info tables	The 5620 SAM allows the simultaneous application of multiple information tables types to any map object.	See "Information tables" in section 4.1 and Procedures 4-13, 4-14, 4-15, and 4-16 for more information.
Restrict active sessions per user account	The number of active sessions that a user account can successfully login can be limited to a specified number.	See the Maximum Sessions Allowed (maxSessionsAllowed) parameter in section 128.1 for more information.
Enhanced information sharing and communication	The 5620 SAM allows users to share information and communicate with each other by saving window information, going to specified windows, and sending text messages.	See Procedures 2-16, 2-18, and 2-9 for more information.
Using sample scripts	The 5620 SAM allows the user to browse sample scripts and create instances of any sample.	See chapter 4 for more information.
Y.1731 (full implementation)	Three new Y.1731 OAM tests have been added, as well as AIS enhancements.	See Procedures 35-4 through 35-8.
Fast channel change and multicast retransmissions for ISA-Video MDA	The ISA Video module supports reliable multicast delivery and fast channel change.	See chapters 33 and 46, and Procedure 17-22.
Ad-Insertion support for ISA-Video MDA	The ISA Video module supports advertisement insertion.	See chapter 33, and Procedures 17-22 and 46-4.
IPv6 PIM ASM	PIM supports IPv6.	See Procedure 28-32 for more information.
Point-to-Multipoint LSP support	The point-to-multipoint LSP, which is based on the dynamic LSP, is introduced.	See chapter 29, and specifically, Procedure 29-14.

(8 of 18)

Feature or function	Description	Reference for more information
Multicast VPN with BGP Control Plane	Enhancements were made to MVPN BGP routing instance routing information distribution.	See Procedures 71-1 and 28-32 for more information.
BGP AD support in B-VPLS	BGP auto-discovery for B-VPLS B-Sites is supported.	See Procedure 68-6 for more information.
Service templates (phase III)	XML API service creation templates are augmented with enhanced object-selection capabilities.	See chapter 5 for more information.
Load sharing for eBGP and MP-iBGP routes	MP-BGP load balancing allows a route to have multiple next hops of different types, for example, IPv4 next hops and MPLS LSPs.	See Procedure 28-2 for more information.
Per LSP and per class statistics solution for LDP	Two new types of accounting statistics were introduced: combined MPLS LSP ingress/egress statistics, and combined LDP LSP egress statistics.	See Procedures 29-2, 29-8, and 28-18 for more information.
CPM/1ag MIP management	The display of MIP information and resynchronization on VPLS SAPs and spoke SDP bindings is enhanced.	See Procedures 68-3, 68-5, and 35-4 to 35-8 for more information.
CPM 802.1ag MEP enhancement	Users can create multiple loopback or link trace tests for a specific MEP.	See Procedures 35-5 and 35-6 for more information.
Release 7.0 R3 features		
New daughter card support	The 5620 SAM supports the 1 × Channelized OC12 CES MDA on the 7750 SR, Release 7.0 R3 or later, and the 1 × Channelized OC12 CES MDA on the 7710 SR, Release 7.0 R3 or later.	See chapter 15 for more information.
New CPM/Switch Fabric 3	The 500 Gb/s CPM/Switch Fabric 3 is supported on the 7750 SR-12 and 7450 ESS-12. The 250 Gb/s CPM/Switch Fabric 3 is supported on the 7750 SR-7, and the 7450 ESS-7.	See chapter 15 for more information.
9500 MPR support	The 5620 SAM supports the following features on the 9500 MPR, Release 1.2 or later: • MSS-4 4-slot shelf • MSS-8 8-slot shelf • core-enhanced card • 1 × radio modem card • microwave links automatically displayed as physical links • 32 × DS1/E1 card (E1 support only) • 1 + 1 EPS core card protection • 1 + 1 FD and 1 + 1 HSB protection for radio modem cards • 1 + 1 EPS protection for 32 × DS1/E1 cards • VLAN groups and VLAN paths • 9500 MPR Cpipe service • 802.1p and DSCP QoS classification • software upgrades • alarms and statistics	—
IGMP Snooping on the 7210 SAS-E	IGMP Snooping can be enabled for VPLS on the 7210 SAS-E, Release 1.0 R4 or later.	See Procedures 68-2 and 68-3 for more information.
OmniSwitch enhancements	The 5620 SAM supports the following features on the OmniSwitch: • static and dynamic LAGs • VLAN groups	See Procedures 17-25 and 17-26 for more information. See Procedures 66-1 and 66-2 for more information.
Support RSVP and LDP simultaneously in auto-bind	Support for the auto-bind capability is extended to include MPLS service tunnels that use RSVP or LDP.	See Procedure 71-1 for more information.

(9 of 18)

Feature or function	Description	Reference for more information
Release 7.0 R1 features		
Chassis mode D support	Chassis mode D is supported on 2 × XP MDA IOM 3 card on the 7450 ESS, Release 7.0 or later. You can configure chassis mode D only if all the IOM cards equipped on the device are 2 × XP MDA IOM 3 cards. You can configure chassis mode D on the 2 × XP MDA IOM 3 card on the 7750 SR, Release 6.1 or later, on the 5620 SAM, Release 6.1 or later.	See chapter 15 for more information about how to configure chassis mode D.
New daughter card support	The 5620 SAM supports the following MDAs on the 7750 SR, 7450 ESS, and 7710 SR Release 7.0 or later. • 10 × 10/100/1000 Ethernet Extended Performance SFP MDA • 1 × 10Gig Ethernet Extended Performance XFP MDA	See chapter 15 for more information.
New daughter card support	The 5620 SAM supports the 4 × Channelized OC3 CES MDAs on the 7750 SR and 7710 SR Release 7.0 or later.	See chapter 15 for more information.
Ethernet interface mode enhancements	You can configure the XGig Mode parameter on 10Gig-base Extended Performance MDAs. When you configure the XGig Mode parameter on a port on a 10Gig Extended Performance XP MDA, the same value is applied to all other ports on the MDA. You can configure the XGig Mode parameter on the 1 × 10 Gig Ethernet MDA in all previous supported releases of the 5620 SAM.	See chapters 17 and 168 for more information about the XGig Mode parameter.
New HSMDA	The 5620 SAM supports the HSMDA 1 × 10 Gig SFP on the 7750 SR and 7450 ESS, Release 7.0 or later. The HSMDA is used to extend subscriber and service density by providing MDA-level of ingress and egress queues, shapers, and schedulers.	See chapter 15 for more information.
IPsec	You can use the 5620 SAM to configure IPsec services on the 7750 SR, Release 7.0 or later. You can create IPsec interfaces on VPRN services and IPsec gateways on IESs to provide IPsec tunneling and encryption between sites.	See chapter 32 for more information.
MLPPP and BPG scalability increases on ASAP MDAs	The range of bundle IDs on a 1xOC12 ASAP MDA is increased for the 7750 SR, and 7710 SR, Release 7.0 or later. The range of BPG/APS bundles is increased for the 7750 SR, Release 7.0 or later.	See Procedures 17-98, 17-99, and 37-4 for more information.
APS support on the 7450 ESS	The 5620 SAM supports single-chassis APS configuration on the 7450 ESS, Release 7.0 or later.	See chapter 37 for more information.

Statistics enhancements	5620 SAM statistics support includes the following:
	• custom service, subscriber, and AA accounting policies that enable you to specify the following:
	  • the statistics counters in a record
	  • threshold values that determine whether a record is created
	• AA per-SAP and per-subscriber statistics for AA troubleshooting
	• real-time graphing of MIB-based accounting statistics
		See chapter 73 and the *5620 SAM Statistics Management Guide* for more information.

(10 of 18)

Feature or function	Description	Reference for more information
Ingress SAP Queue allocation - optimization	Optimization within a LAG for VPLS services which are from the same split horizon group is supported. This optimization allocates sap-ingress queuing between complexes which have SAPs only within the same split horizon group. This feature is supported on the 7750 SR and 7450 ESS, Release 7.0 or later.	See Procedure 17-23 for more information.
Service and transport alarm correlation	An LSP alarm raises a correlated alarm against each child LSP path, and is listed as an aggregated alarm for each SDP that uses the LSP.	See chapter 34 for more information about alarm correlation.
Alarm descriptive information	Each 5620 SAM alarm has a detailed description on the Details tab of the Alarm Info form. The same description is listed in the *5620 SAM Troubleshooting Guide*.	See the *5620 SAM Troubleshooting Guide* to view the alarm descriptions.
Alarm scalability improvements	The 5620 SAM consolidates multiple alarm events that have a common source before it sends an alarm notification to the GUI and OSS clients. This helps to prevent alarm flooding.	See chapter 34 for more information about alarm correlation.
Increased redundancy robustness	A 5620 SAM primary main server in a redundant deployment can be configured to automatically connect to a specified 5620 SAM database. This function helps to ensure that the primary main server and database are in one geographic location after a redundancy failure, which minimizes network latency between the server and database.	See chapter 6 for more information about automatic database realignment.
Configurable interfaces for MC APS group members	You can specify a network interface other than the system interface as the interface for an MC APS group member.	See chapter 37 for more information about configuring MC APS groups and members.
Support for increased subscriber limits	The maximum value of the subscriber limit property for SAP-level subscriber configuration increases to 20 000 for the 7750 SR, 7450 ESS, and 7710 SR, Release 7.0 or later.	See Procedures 68-3, 70-1, 70-8, and 71-11 for more information.
OmniSwitch enhancements	The 5620 SAM supports the following OmniSwitch features: • health monitoring monitors the switch, and at fixed intervals, collects the current values for each resource that is being monitored. You can specify resource threshold limits; traps are sent to the 5620 SAM when a value is greater or less than a configured threshold. • DHCP/UDP relay and DHCP snooping — DHCP agents can be used to centralize DHCP servers, which avoids the need for a DHCP server on each subnet. • OS 9600, OS 9700, and OS 9800 devices • IEEE 802.1AB LLDP, a Layer 2 protocol that allows a network device to advertise its identity and capabilities on the local network • creation of service templates • Ethernet CFM OAM continuity check, loopback, and link trace • scheduling of CFM OAM tests and configuration backup and restore	See Procedure 17-51 for more information. See Procedures 28-51, 17-62, 65-4, 65-6, and 65-7 for more information. See Procedures 17-8 and 17-62 for more information. See the *5620 SAM Scripts and Templates Developer Guide* for more information. See chapter 35 for more information. See chapters 74 and 35 for more information.

(11 of 18)

Feature or function	Description	Reference for more information
7210 SAS-E Release 1.0	7210 SAS-E chassis: • integrated IOM and Ethernet ports • 12 × 100/1000 SFP Ethernet ports, and copper SFPs • 12 × 10/100/1000 TX Ethernet ports	See chapters 11, 15, and 17.
	in-band management	See chapter 12.
	Epipe and VPLS support; IES supported only for in-band management	See chapters 67, 68, and 70.
	STM OAM • ICMP ping and trace • DNS ping • CFM continuity check, loopback, and link trace • EFM OAM	See chapter 35.
	dynamic LAGs	See chapter 17.
	QoS policies: • 7210 Access Ingress • 7210 Access Egress • 7210 Network • 7210 Network Queue • 7210 Slope • 7210 Port Scheduler	See chapter 44.
	configuration backup and restore	See chapter 21.
	scheduled and on-demand software upgrade	See chapter 21.
	statistics collection	See the *5620 SAM Scripts and Templates Developer Guide*.
	alarm management	See chapter 35.
Egress SAP forwarding class and forwarding profile override	The SAP egress QoS policy allows IP-based reclassification rules to override the ingress forwarding class and profile of packets which egress a SAP where the QoS policy is applied. The coverage applies to DSCP, Precedence, and IP match criteria access egress configuration. The function is supported on the 7750 SR, 7450 ESS, and 7710 SR, Release 7.0 or later.	See chapter 44.
VCI-based QoS filter policy on VP-SAP of an ATM-VPC Apipe service	A VCI-based QoS filter, applicable within the Access Ingress QoS policy, can be used to match the VCI field in the received ATM VLL packet of an ATM VLL(Apipe) service of type atm-vpc. This feature provides a new frame type, ATM, and a new parameter, ATM-VCI. It is supported on the 7750 SR, 7450 ESS, and 7710 SR, Release 7.0 or later.	See chapter 44.
Client delegate servers	A 5620 SAM client delegate server can host multiple local and remote 5620 SAM client GUI sessions, and supports the use of third-party remote access tools such as Citrix. Client delegate server installation is supported only on Solaris.	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.
Managed SAP (MSAP)	Automatic SAP enables the automatic creation of a SAP that supports the one subscriber per SAP model for L2 access interfaces. The automatically created SAP is called an MSAP. MSAPs can be used in VPLS, IES, and VPRN configurations.	See section 64.1 for more information.

(12 of 18)

Feature or function	Description	Reference for more information
RCA audits	You can audit VLL, VPLS and VPRN services, and physical links to identify configuration problems. The 5620 SAM corrects the problems for services when you accept the proposed solutions.	See chapter 77 for more information.
Virtual MEPs configured on a B-VPLS sites	You can generate CFM tests on B-VPLS and B-MVPLS sites by configuring a virtual MEP on a MAC address.	See chapter 43 for more information.
Scale policy deployment	You can configure the number of deployers used for policy deployment to maintain system performance.	See chapter 43 for more information.
5650 CPAM menu	The 5650 CPAM menu is accessible from the 5620 SAM main menu. The 5650 CPAM menu is enabled by a valid 5650 CPAM license key. The 5650 CPAM menu path is Tools→Route Analysis.	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information about how to install the 5650 CPAM.
4-port OC3/STM1 ASAP SFP daughter card on 7705 SAR	The 7705 SAR supports the 4-port OC3/STM1 ASAP SFP daughter card, which can be configured for clear channel operation in access mode.	See section 11.1 and section 15.17 for more information.
7705 SAR fabric profile policies	The 7705 SAR supports a fabric profile policy on daughter cards that allows you to define the fabric shaping rate (kb/s) to the daughter card.	See chapters 43 and 44 for more information.

(13 of 18)

Feature or function	Description	Reference for more information

Additional 7705 SAR Release 2.0 support	The 5620 SAM adds support for more functions on the 7705 SAR as follows:
	• OSPF and RSVP protocols
	• configuration of dynamic LSPs and bypass LSPs
	• MPLS:RSVP transport type on service tunnels
	• more properties in the configuration of network interfaces, routing instances, MPLS, and LDP
	• configuration of CPM IP filters
	• enhancements for ACL IP filters
	• up to eight MLPPP bundles per daughter card, which is applicable to the total number of MLPPP bundles (access mode bundles plus network mode bundles) on a daughter card
	• Ipipes
	• Vccv Trace
	• VLL redundancy
	• Hold Time Up and Hold Time Down parameters, for which each physical port on the 16-port DS1/E1 ASAP daughter cards supports the configuration of Hold Time Up and Hold Time Down to debounce changes to the operational status of the port
	• LDP graceful restart
	• configuration of route aggregation on a routing instance
	• routing policy that supports the configuration of:
	  • additional Default Action parameters
	  • additional Policy Statement Entry Accept Action parameters
	  • additional Policy Statement Entry To Criteria parameters
	  • additional Policy Statement Entry From Criteria parameters
	• Access mode bundles with IPCP encapsulation on the 16-port DS1/E1 ASAP daughter card. IPCP encapsulation cannot be configured on DS0 channel groups whose containing DS1/E1 channel is configured for either Unframed mode or Adaptive clock source. Detailed packet discard statistics for these DS0 channel groups and bundles are supported.
		See section 11.1 and chapter 28 for more information about OSPF v2 and RSVP support on the 7705 SAR.
		See chapter 29 for more information about dynamic LSP and bypass LSP support on the 7705 SAR.
		See chapter 27 for more information about Routing policy on the 7705 SAR.
		See chapter 30 for more information about Service tunnel support on the 7705 SAR.
		See section 11.1 and chapter 27 and chapter 29 for more information about Network interfaces, routing instances, MPLS, and LDP on the 7705 SAR.
		See section 18.1 for more information about CPM IP filters support on the 7705 SAR.
		See chapter 45 for more information about ACL IP filters support on the 7705 SAR.
		See Procedure 17-98 for more information about Multilink PPP support on the 7705 SAR.
		See Procedure 67-7 for more information about Ipipe support on the 7705 SAR.
		See section 35.1 for more information about Vccv Trace on the 7705 SAR.
		See section 67.1 for more information about VLL redundancy on the 7705 SAR.

ISA-AA group with up to seven active members and one backup	For each ISA-AA Group, one per applicable NE, there can be up to seven primary members and one backup member in a group. This feature is supported on the 7750 SR-7, 7750 SR-12, 7450 ESS-6, 7450 ESS-7 and 7450 ESS-12, Release 7.0 or later.	See section 15.7 and Procedure 17-17 for more information.
Enhanced topology maps	Enhancements to the topology map provide more flexibility for managing and organizing NEs, including: • filtering • span of control configuration • Global Info Tables Also, flat snapshot maps are renamed flat map.	See chapter 4 for information.

(14 of 18)

Feature or function	Description	Reference for more information
Route Policy	To enhance routing configuration flexibility, the following routing policies can be configured as separate policies or cross-referenced to form a framework of policies depending on the network requirements: • policy statement • prefix list • community • damping • AS path	See chapter 27 for information about configuring routing policies.
Format and range policies	5620 SAM supports the format and range policies. Format policies manage the format of names and descriptions for services, LSPs and L2 and L3 access interfaces. Range policies manage ID numbers for the services, LSPs, and L2 and L3 access interfaces.	See chapter 43 for information about configuring format and range policies.
Unicast RPF Support	Unicast RPF helps to mitigate problems which are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network, by discarding IP packets which lack a verifiable source address. Unicast RPF is supported on the 2 × XP MDA IOM 3 of the 7750 SR and 7450 ESS, Release 7.0 or later.	See Procedures 27-4, 70-1 and 71-2 for more information.
Failure Error Display	When a failed or incomplete deployment or failed SNMP configuration request occurs, a Problems Encountered error form appears automatically. This form displays error information about the failure(s). This feature displays the error dialog when deployment and other errors occur.	See Procedure 21-2 for more information.
MLPPP Magic Number	This feature specifies whether a bundle detects loopback conditions on MLPPP links and takes the links out of service. MLPPP magic number is supported only on channelized ASAP MDAs on the 7710 SR and 7750 SR, Release 7.0 or later.	See Procedure 17-101 for more information.
Routed Subscriber with PPP support for Static Routes	Next Hop IP and MAC Address enables a SAP to accept SRRP advertisements when anti-spoofing is enabled for subscriber hosts on the SAP. The option is available on VPRN and IES group-interface SAPs. This option is supported on the 7710 SR and only on the IOM 2 cards of the 7750 SR-7, and 7750 SR-12, Release 6.1 or later. The Administrative State for static hosts is configurable to allow full or partial static host configuration. This is supported on the 7750 SR, 7450 ESS, and 7710 SR, Release 6.1 or later. The creation of 16 managed routes is supported for each static host on IES and VPRN SAPs on the 7750 SR, 7450 ESS, and 7710 SR, Release 6.1 or later.	See Procedure 64-24 for more information.
Auto-provisioning	Auto-provisioning provides a way to reuse a proven configuration and apply the configuration to multiple NEs of the same type. This function is useful when a large number of similar network elements must be configured. This option is supported on the 7750 SR, version 2.0 or later.	See chapter 26 for more information.
LSP path optimization	5620 SAM allows you to re-signal LSP paths to take advantage of new paths that are less congested, have fewer hops, have a lower metric, and meet least-fill criteria. NEs periodically check the network to determine whether a more efficient path is available and notifies the 5620 SAM when another path is eligible for re-signalling.	See chapter 29 for more information.

(15 of 18)

Feature or function	Description	Reference for more information
LSP paths, dynamic LSPs and SDP tunnel templates	Tunnel template configuration, introduced in 5620 SAM 7.0, allows users to configure dynamic LSPs, LSP paths, and SDPs templates to define common characteristics for a tunnel or templatable tunnel object.	See chapters 29 and 43, and the *5620 SAM Scripts and Templates Developer Guide* for more information.
Improved naming and descriptions for scope of command roles	Scope of command role names and descriptions are improved.	See chapter 8 for more information.
APAC Radius Enhancements	New Radius attributes allow for Calling Station ID and User Name to be included in Radius accounting messages. Users can also specify the Calling Station ID on SAP and L2 forms, as well as select local user databases, specify domain names, and append domain names to user names.	See chapters 18, 64, 68, 70, and 71 for more information.
MLFR	New MCFR Egress and Ingress QoS profiles can be created and configured.	See chapter 43 for more information.
FRF.12	DS0 Channel groups can be configured with FR encapsulation, and FR group bundles can be created and modified on channelized ASAP MDAs. Also, a there is a Frame Relay tab on L2/L3 Access Interface configuration forms.	See chapters 17, 67, 68, 70, and 71 for more information.
Filtering and Finding	5620 SAM filtering is updated to allow the configuration of filter criteria using new filter areas in the column headings of a list form. You can also configure filter criteria using a new advanced filter panel.	See chapter 2 for more information.
AA-ISA based information	5620 SAM Application Assurance Profile policies are referred to as AA Group policies. Other new terminology includes AA Flow Watermark, AA Protocol, and AA Accounting Policy.	See chapter 73 for more information.
SAP based Application Assurance	This feature allows users to select an Application Profile to associate with the L2/L2 access interface of a service.	See chapter 73 for more information.
HTTP app-filter string entry	This feature introduces the Application Filter Expression form and its associated parameters.	See chapter 73 for more information.
802.1ag result enhancements	This feature allows users to identify missing remote MEPs following a CFM Continuity Check using the new Remote MEP DB State tab button on the MEP Entry (Edit) form.	See chapter 35 for more information.
Task Manager	The Task Manager allows SAM administrators and support personnel to monitor progress of operational tasks and SAM administrators to configure task monitoring parameters.	See Procedure 2-14 for more information.
256 subnets per subscriber interface	This feature increases the number of subnets allowed per subscriber interface to 256.	See the IES configuration section in chapter 70 and the VPRN service management overview section in Chapter 71 for more information.
Link Layer Discovery Protocol (LLDP) support	LLDP is a protocol that allows a network device to advertise its identity and capabilities to other stations attached to the same IEEE 801 LAN.	See the LLDP section in chapter 27 and Procedure 17-8, 17-47, 17-61, and 17-62 for more information.
OSPF as CE-PE Protocol for IP-VPN	This feature implements full support for OSPF as CE-PE protocol for IP-VPN for the 7710 SR and 7750 SR product lines. This is accomplished by providing support for sham links.	See the OSPF sham link support section in chapter 71 and Procedure 71-14 for more information.

(16 of 18)

Feature or function	Description	Reference for more information
Four-byte ASNs	This feature implements support for four-byte ASNs and all associated functions and protocols within BGP.	See Procedures 28-2, 28-4, 28-5 (on Disable 4-Byte ASN parameter) and Procedure 71-1 (on Type 2 Route Distinguisher and 4-Byte AS parameters and VRF Targets) for more information.
Conditional Route policies	Conditional Route policies allow specifying a prefix list as part of the static route creation. The system can then determine whether any routes in the list must exist for the static route to be added to the RTM.	See Procedures 27-17 and 71-1 for more information.
IPv6 VRRP for IES and VPRNs	This feature implements support of IPv6 VRRP for both IES and VPRN services for the 7710 SR and 7750 SR. The following functions are supported: • IPv6 VRRP for router interfaces, IES interfaces, and VPRN interfaces • VRRP policy with support for IPv6 address family • Interaction with IPv6 Neighbor Discovery and Router Advertisement • Support for IPv6 Link Local Addresses	See Procedures 36-1 and 36-2 for more information on Backup Addresses; and chapter 51 for IPv6 host support; and Procedures 27-4, 70-1 and 71-2 for Admin Link Local Addresses.
Diff-Serv extensions to MPLS TE	This feature implements support for Diff-Serv classes on RSVP and RSVP Interfaces. This provides the ability to manage bandwidth in an MPLS network on a per-TE class basis.	See the Diff-Serv Traffic Engineering support section in chapter 28 and Procedures 28-27, 28-28, 29-8, 29-9, 29-17, and 29-18 for more information.
L3VPN BGP Next-hop resolution, with static metrics	This feature implements support for the auto-bind capability to include RSVP TE-based LSPs. Paths can be configured to use static metrics if dynamic metrics are not available.	See Procedure 71-1 for more information.
BGP Next-hop resolution to RSVP-TE LSP, with dynamic metrics	This feature controls whether a dynamic LSP is used in the auto-bind capability.	See Procedure 29-8 for more information.
Regular Expression support for extended communities	This feature implements support for Regular Expression matching for extended communities (Route Targets and Route Discriminators).	See the Community member parameter in chapter 85 for more information.
LDP-over-RSVP without ABR stitching point	This feature is an enhancement to the existing LDP-over-RSVP capability. It allows the user to specify which router in a specific area can be used as a stitching point for LDP over RSVP. For customers who may have in excess of 200 or 300 routers in an area, this helps to reduce the number of LSPs, since a full mesh is no longer required. This feature is only applicable to OSPF routers in Release 7.0 R1.	See chapter 29 and Procedure 29-8 for more information.
Per-LSP per-class statistics	This feature introduces three new types of accounting statistics that are available for collection: • Combined MPLS LSP ingress • Combined MPLS LSP egress • Combined LDP LSP egress statistics Per-spoke SDP statistics for L2 (VPLS and VLL) services and aggregate per-SDP statistics are available.	See Procedures 29-2, 29-8, and 4-2 for more information.
VPRN - Option C	This feature implements VPRN Option “C” support for configuration and statistics on all devices that support VPRN services.	See Procedures 28-4 and 28-5 for occurrences of the Advertise Label parameter for more information.

(17 of 18)

Feature or function	Description	Reference for more information
ECMP support for LDP-over-RSVP	This feature provides load balancing across LSPs for LDP-over-RSVP. When ECMP is enabled, all equal-cost LSP endpoints are installed in the routing table by the IGP for consideration by LDP.	See LDP section in chapter 28 for more information.
Aggregate prefix match for LDP	This feature provides the option to have LDP install a prefix binding in the LDP FIB. This is done by performing a longest match against an aggregate prefix in the routing table, as opposed to requiring an exact match of the prefix.	See Procedure 28-18 for more information.
PBB enhancement	This feature implements support for IGMP snooping in IVPLS services.	See the Provider Backbone Bridging in VPLS section in chapter 68 and Procedures 68-12 and 68-14 for more information.
Egress marking (DSCP and EXP) for VPRN Model B L3 boundary interface	This feature implements support for configuration of egress traffic remarking between two different ASNs.	See chapter 44 for more information.
PPPoE for business VPRNs	This feature implements support for PPPoE termination in business VPRNs. This targets applications such as PPPoE VPRN with IP overlap, where there are two participants in the service, typically a Wholesale VPRN and a Retail VPRN.	See chapter 71 more information.
Multicast VPN with BGP Control Plane	This feature implements the next-generation MVPN solution.	See Procedures 71-1 and 28-32 for more information.
Aggregate Routes in VPRNs	This feature implements support for route aggregation to VPRN sites for the 7710 SR and 7750 SR product lines.	See Procedure 71-1 for more information.
CE Router discovery in IPIPE services	This feature implements support for IP VLL services to allow the discovery of CE routers. The support includes configuration options for the discovery of Ethernet CE IP address for VLL Ethernet SAP, VLL FR SAP, VLL ATM SAP, VLL PPP/IPCP and Cisco-HDLC SAP.	See the Ipipe (IP interworking VLL) section in chapter 67 and Procedure 67-7 for more information.
BW-based equal-cost RSVP LSP path selection	This feature provides a method to achieve load balancing of the bandwidth in LSP paths. Typically CSPF includes link utilization as a tie breaker criterion in the path selection. Support is implemented for the “least-fill” path selection algorithm.	See the Bandwidth-based equal cost RSVP LSP path selection section in chapter 29 and Procedures 29-2 and 29-8 for more information.
Static configuration for Shared Risk Link Groups	This feature allows the user to manually enter into the SRLG database a backup secondary LSP path or a FRR LSP path which is disjoint from the path of the primary LSP.	See Procedure 27-16 for more information.
HSDPA Offload resiliency	This feature implements a resiliency capability for HSDPA Offload mobile voice and data service configurations. The feature provides: • Active and backup service configurations • Failure detection and switchover • Service switchback after failure resolution • Licensing	See the HSDPA Offload Resiliency section in chapter 67, and Procedures 67-12 and 67-13 for more information.

(18 of 18)

3.3 5620 SAM Release 6.1 features

Table 3-3 lists the features and functions added in 5620 SAM Release 6.1.

Table 3-3 5620 SAM Release 6.1 features

Feature or function	Description	Reference for more information
Release 6.1 R3 features		

7705 SAR Release 1.1	The 7705 SAR, Release 1.1, new hardware and features:
	• 7705 SAR-F chassis
	  • integrates CSM, 8-port Ethernet v3 MDA, and 16-port DS1/E1 ASAP v2 MDA
	  • both Ethernet SFP ports can simultaneously be configured as timing references
	  • one of ports 1-8 and one of ports 9-16 on the ASAP MDA can simultaneously be configured as timing references
	  • alarm generated for a single fan failure
	• Ethernet Version 2 MDA (7705 SAR-8)
	• local VLL for Cpipes and Apipes
	• IES for in-band management over an ATM network
	• ANSI FDL, Bellcore FDL, and ANSI Payload channel loopbacks
	• SAToP VC Type for Cpipes
	• DSCP for network QoS policies
	• detailed packet discard and adaptive clock recovery statistics
	• adaptive clock history for the preceding 15 minutes for DS1/E1 channels using adaptive clock sources
	• synchronous Ethernet (IEEE 1588) support on Version 2 and 3 MDAs
	• GRE tunnels
		—

OSPFv3 under VPRN	An OSPFv3 routing instance on VPRNs is supported on the 7750 SR (chassis mode C or D) and 7710 SR, Release 6.1 R1 or later.	See Procedure 71-1and 71-3.
MAC MAF and CPM filters	You can configure MAC MAF and MAC CPM match criteria for NE MAF and NE CPM filters. MAC MAF is supported on the 7750 SR, 7450 ESS, and 7710 SR Release 6.1 R4 or later. MAC CPM filters are supported on the 7750 SR and 7450 ESS, Release 6.1 R4 or later.	See Procedure 18-1.
Release 6.1 R1 features		
New IOM card	The 5620 SAM supports the 2 × XP MDA IOM 3 card. The IOM is supported on the 7750 SR and 7450 ESS, Release 6.1 or later. You can configure a new chassis mode, chassis mode D, only in a chassis that is equipped with only 2 × XP MDA IOM 3 cards. Chassis mode D is supported only on the 7750 SR, Release 6.1 or later. The IOM also support chassis modes A, B, and C.	See Procedure 17-33.
IMM card	The 5620 SAM supports the IMM on the 7750 SR, Release 6.1 or later. The IMM is available in four variants: • 4 × 10 Gb XFP • 8 × 10 Gb XFP • 48 × 1 Gb SFP • 48 × 10/100/1000 TX	—

(1 of 3)

Feature or function	Description	Reference for more information
New MDAs	The 5620 SAM supports four new MDAs: • 2 × 10 Gb XP XFP • 4 × 10 Gb XP XFP • 20 × 1 Gb XP SFP • 20 × 1 Gb XP TX	—
2 × XP MDA IOM 3 and IMM multicast	Multicast path management support for the 2 × XP MDA IOM 3 card and IMM.	See chapter 46 and Procedure 17-32.
SSM translation support	You can configure SSM translation on IGMP interfaces.	See Procedure 28-38.
Single fiber passive mode support on the 7750 SR	You can configure single fiber mode on 1 and 10 Gigabit Ethernet ports. This feature is only supported on the 2 × XP MDA IOM 3 or IMM. You can configure network interfaces to strip MPLS labels from incoming IP packets. The network interfaces must be configured on single fiber mode SONET or Ethernet ports. This feature is only supported on the 2 × XP MDA IOM 3 and IMM.	See Procedures 17-61 and 27-4.
MLD	You can configure MLD, an asymmetric protocol used by IPv6 routers to discover the presence of multicast listeners. MLD ensures that multicast packets are delivered to all links where there are listeners interested in such packets.	See Procedures 28-47 to 28-49.
Support for OmniSwitch OS 6400 and OS 6855	The feature set introduced in Release 6.0 for the OS 6850 is supported on the OS 6400 and OS 6855.	—
MC MLPPP QoS profiles	You can create MC MLPPP ingress and egress QoS profiles and apply profiles to MC MLPPP bundles.	See chapters 17, 37, and 46 for information about MC MLPPP.
ISA-IPsec MDA	The 5620 SAM supports the ISA-IPsec MDA on the 7750 SR, Release 6.1 or later. The ISA-IPsec MDA provides IP security for tunneling and encryption functions.	See chapter 15.
Synchronous Ethernet	You can configure timing synchronization on the 7750 SR, 7710 SR, 7450 ESS, and 7705 SAR.	See Procedure 17-34.
Provider Backbone Bridging on VPLS	Provider Backbone Bridging is a technology configuration employed in networks that utilize carrier-grade ethernet as the transport architecture. PBB encapsulates the customer frame in a Provider Ethernet Header. The 5620 SAM supports PBB on VPLS and VLL Epipes. Feature implementation includes enhanced MAC Flush capability.	See Procedures 68-11 to 68-14 and 67-1.
BGP Auto-discovery	BGP Auto-discovery for LDP VPLS enables each VPLS PE router to discover the other PE routers that are part of the same VPLS domain. The 5620 SAM supports BGP AD on VPLS.	See chapters 49 and 68.
CAC on VLL	Implementing CAC provides a method to administratively account for the bandwidth used by VLL services inside an RSVP SDP which consists of RSVP LSPs. The SDP Admin Bandwidth parameter allows you to specify a bandwidth reservation for this SDP binding.	See Procedure 67-1.
APAC RADIUS enhancements	The 5620 SAM supports the inclusion of RADIUS attributes as part of the subscriber Authentication-Request message and the use of RADIUS-based accounting policies for specific subscriber hosts.	See chapters 18 and 54.
7705 SAR, Release 1.0 feature support	The 7705 SAR, Release 1.0, has a subset of features that are supported on the 5620 SAM for the 7750 SR, Release 6.1. See the *5620 SAM NE Compatibility Guide* for more information.	—

(2 of 3)

Feature or function	Description	Reference for more information
LogViewer utility	The 5620 SAM includes a LogViewer utility in GUI and CLI forms. You can use LogViewer to do the following: • View log-file updates in real time. • Filter log entries using regular expressions. • Assign colors to different log-entry debug levels. • Display the contents of multiple current or archived log files simultaneously.	See the *5620 SAM Troubleshooting Guide*.
Streamlined upgrades	An upgrade of the 5620 SAM software requires less user interaction and takes less time than a previous upgrade because of improvements to the 5620 SAM installer utility.	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.
Non-root user privileges for 5620 SAM administration	An installation or upgrade of the 5620 SAM software on Solaris 10 creates a samadmin user account that has a special set of privileges. The samadmin account is required for controlling the 5620 SAM server application and for most other 5620 SAM administrative activities.	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.
Statistics enhancements	Enhancements to statistics includes: • periodic data for accounting statistics • modified 5620 SAM main menu options for statistics • additional Statistics Plotter functions	See the *5620 SAM Statistics Management Guide*.
HSMDA	The 5620 SAM supports the HSMDA on the 7750 SR and 7450 ESS, Release 6.1 or later. The HSMDA is used to extend subscriber and service density by providing MDA-level of ingress and egress queues, shapers, and schedulers.	See chapter 15.
HSMDA policies	You can configure HSMDA policies which extend subscriber and service density by adding a level of ingress and egress queues, shapers, and schedulers.	See chapter 43.
Qualified and unqualified SAPs on the same VPLS	You can configure qualified and unqualified SAPs on the same VPLS site. This feature gives the user full control to pass traffic to the network through a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0 R4 or later; for example, using an unqualified SAP to pass Internet traffic and using a qualified SAP to pass secured traffic.	See Procedure 68-3.
IS-IS routing enhancements	You can: • configure an IS-IS routing instance to advertise only passive interfaces • assign a tag to the IP address of an IS-IS interface and use the tag to control route distribution through the use of administrative policies	See Procedures 27-8, 28-24, and 28-26.
RIP metric propagation in VPRNs	You can configure a VRPN RIP routing instance to map the RIP metric to the MP-BGP MED attribute when RIP is used as the CE to PE routing protocol. This allows the RIP metric to be advertised to far-end RIP neighbors.	See Procedures 71-3 and 28-7.
OSPF as CE-PE protocol for IP VPN	An additional layer of hierarchy in OSPF is provided for VPRN instances of OSPF by using an OSPF super-backbone.	See Procedure 28-11.
Copying and moving SAPs between ports	The copy and move SAP function is enhanced to include L3 service interfaces.	See Procedures 15-5, 15-6 and 15-7.
IOM soft reset	A soft reset of IOMs can be performed on the 7750 SR and 7450 ESS, Release 6.1 R4 or later.	See Procedure 21-9.

(3 of 3)

3.4 5620 SAM Release 6.0 features

Table 3-5 lists the features and functions added in 5620 SAM Release 6.0.

Table 3-4 5620 SAM Release 6.0 features

Feature or function	Description	Reference for more information
Release 6.0 R3 features		
OS 6850 support	The 5620 SAM supports the display of optical transceiver attributes. The attributes are displayed on the Media Adaptor tab of the port properties form. This tab only appears for ports that use optical transceivers.	—
	Software upgrade is supported for Uboot and Miniboot files.	See Procedures 21-8 and 21-13 for more information.
	FTP and SSH file browsers are supported.	See Procedure 21-23 and Procedure 21-24 for more information.
	The 5620 SAM supports the configuration of IGMP snooping on the router instance and individual VLAN sites.	See Procedures 28-37 and 65-11 for more information.
Power supply form changes	Two new attributes on the power supply tray form are: • Power Supply Status—for all 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices • Power Supply Fan Status—for 7250 SAS Release 2.0 or later, and all 7250 SAS-ES and 7250 SAS-ESA devices The 5620 SAM generates an alarm when a power supply unit is not installed and when an installed power supply unit is not functioning properly. In both cases, the alarms clear automatically when normal operation resumes. All attributes that do not apply have been removed from the form.	—
OAM scaling enhancements	The following test policy options are designed to reduce the amount of data collected during OAM tests: • a lightweight execution mode for NE schedulable tests that collects data only for failed tests or for successful tests that generate threshold crossing alarms • the ability to only collect test results and ignore test probe results for all test types	See Procedure 75-4 in chapter 75 for more information.
Lawful intercept	The 5620 SAM supports the lawful interception and monitoring of target subscriber voice and data communications over an IP network by authorized agencies. Target-related call data and content are extracted from the network by configuring LI source objects. The source types supported for LI are: • IP filer • MAC filer • SAP • subscriber	See chapter 31 for more information.
Static route to RSVP-TE tunnel	The 5620 SAM supports the configuration of a static route to forward IP traffic into a RSVP-TE tunnel.	See chapter 27 for more information.

(1 of 11)

Feature or function	Description	Reference for more information
Named buffer pool policies	The 5620 SAM supports named pool buffer policies. Named buffer pool policy is a QoS policy used to manage named pools. It allows you to create named pools to override the default buffer pool behavior by creating and allocating ingress and egress queues. Named pools are configured in the named buffer pool policy and are applied at the MDA and/or port ingress and egress level. Named pools can be further defined in Q1 pools configuration. You can configure and assign queue pools.	See chapter 43 for more information.
ISA-AA MDA support	The 5620 SAM supports the ISA-AA MDA on the 7450 ESS-6, 7450 ESS-7, 7450 ESS-12, 7750 SR-7, or 7750 SR-12, Release 6.0 or later. Target traffic is directed to the ISA-AA MDA using the backplane. A set of AQP rules is applied to the traffic. The rules determine the QoS treatment to be applied.	See chapter 15 for more information.
Application assurance	Application assurance inspects online access traffic, specifically HSI traffic. The application assurance features include: • deep packet inspection of subscriber traffic • subscriber policy and traffic management • application assurance accounting statistics	See chapter 73 for more information.
Release 6.0 R1 features		
Windows Vista support	The 5620 SAM supports client installation on the 32-bit editions of Windows Vista Business and Windows Vista Ultimate.	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for 5620 SAM installation information.
Service templates	Service templates in the 5620 SAM, Release 6.0 or later, are based on XML API configuration scripts. Service templates that were created in previous releases must be converted to XML API configuration templates.	See the *5620 SAM Scripts and Templates Developer Guide* for more information about managing XML API configuration templates.
Script manager GUI builder	You can create user interfaces to configure 5620 SAM objects using the GUI builder in the script manager. The GUI builder automatically generates a Velocity UI header in an XML API script.	See the *5620 SAM Scripts and Templates Developer Guide* for more information about using the GUI builder to create user interfaces.
IPv6 support on channelized ASAP MDAs	The 5620 SAM supports IPv6 configuration on the following channelized ASAP MDAs on the 7710 SR and 7750 SR, Release 6.0 or later: • 4 × Channelized OC3 ASAP • 1 × Channelized OC12 ASAP • 4 × Channelized DS3/E3 ASAP • 12 × Channelized DS3/E3 ASAP IPv6 is supported for the following: • IES • VPRN services • network interfaces	—

(2 of 11)

Feature or function	Description	Reference for more information
IPv6 support for VPRN services	The 5620 SAM supports IPv6 configuration of the following in VPRN services on the 7710 SR and 7750 SR, Release 6.0 R1 or later: • addressing for static routes, L3 access interfaces, and BGP peerings • router advertisement, ICMP, DHCP, neighbor discovery, and ACL filtering	See chapter 71 for more information about using IPv6 in VPRN services.
Bidirectional LMI support on FR NNI links	The 5620 SAM supports bidirectional LMI on FR NNI links for peering with other FR networks.	See chapter 17 for more information.
Digital diagnostics monitoring	The 5620 SAM displays real-time warning or alarm status related to digital diagnostics monitoring of the following: • temperature • supply voltage • TX bias • TX output power • RX received optical power • external calibration Digital diagnostics monitoring is supported on SFP and XFP optical modular transceivers on the 7450 ESS, 7710 SR, and 7750 SR, Release 6.0 or later, and on the 7705 SAR.	See chapters 15 and 17 for more information.
New channelized ASAP daughter card support	The following MDAs can be configured in the daughter card slot of the 2 × 10-Gig MDA IOM 2 card on the 7750 SR, Release 6.0 or later, and on the 7710 IOM on the 7710 SR, Release 6.0 or later: • 4 × Channelized DS3/E3 ASAP • 12 × Channelized DS3/E3 ASAP • 1 × Channelized OC12 ASAP The 16 × Channelized DS1/E1 ASAP daughter card can be configured in the daughter card slot of the 7705 IOM on the 7705 SAR. The 4 × Channelized DS3/E3 ASAP is supported on the 7750 SR, Release 4.0 or later.	See chapter 15 for more information about daughter card support.
Support of the 4 × Channelized OC3 ASAP on the 7710 SR	The 5620 SAM supports the configuration of the 4 × Channelized OC3 ASAP on the 7710 IOM card of the 7710 SR, Release 6.0 or later. The 4 × Channelized OC3 ASAP on the 7750 SR, Release 4.0 or later is supported by the 5620 SAM, Release 5.0 or later.	See chapter 15 for more information about daughter card support.

Support for new CMA on the 7710 SR	The 5620 SAM supports the configuration of the 8 × ATM DS1/E1 CMA on the 7710 IOM card of the 7710 SR, Release 6.0 or later.
	The following functions are supported on the 8 × ATM DS1/E1 CMA:
	• IMA bundles on DS0 channels
	• service support
	  • VLL on ATM
	  • Ipipe VLL
	  • Apipe VLL over IMA
	  • L3 interfaces over ATM interfaces
	  • L3 interfaces over IMA
	  • ATM routed bridged encapsulation
	• ILMI 3.1 and 4.0
	• service mirroring
		See chapter 15 for more information about daughter card support.

(3 of 11)

Feature or function	Description	Reference for more information
Support for the CES module on the 7750 SR and 7710 SR	The 5620 SAM supports the following new daughter cards in the CES module: • 1 × Channelized OC3 CES CMA on the 7710 SR, Release 6.0 or later • 1 × Channelized OC3 CES MDA on the 7750 SR, Release 6.0 or later • 4 × Channelized OC3 CES MDA on the 7750 SR, Release 6.0 or later CEM encapsulation is supported on DS3/E3 channels on the daughter cards. The following functions are supported on the Channelized OC3 CES MDA and CMA: • 1+1 bidirectional APS • 1+1 bidirectional MC APS • VLL Cpipe L2 access interface • VLL Epipe L2 access interface	See chapter 15 for more information about daughter card support.
VLL Cpipe	The 5620 SAM supports the creation of a VLL Cpipe with point-to-point CEM encapsulation on a 7750 SR or 7710 SR, Release 6.0 or later, and on the 7705 SAR, Release 1.0 or later.	See chapter 67 for information about configuring a VLL Cpipe.
Multichassis APS bundles	You can configure an APS bundle with working and protection channels on two independent NEs. Multichassis APS configurations are supported on the 7750 SR and 7710 SR, Release 6.0 or later.	See chapter 37 for more information about APS groups.
Multilink PPP bundle support on APS	The 5620 SAM supports the multilink PPP bundle type on APS bundles on the 7710 SR and 7750 SR, Release 6.0 or later.	See chapter 37 for information about configuring a APS bundles.
Multilink PPP bundle as a network interface	You can configure a multilink PPP bundle as a network interface on channelized ASAP MDAs on the 7710 SR and 7750 SR, Release 6.0 or later.	See chapter 17 for more information about configuring multilink PPP bundles.
Multiclass multilink PPP	The 5620 SAM supports multiclass multilink PPP bundles on the 7710 SR and 7750 SR, Release 6.0 or later. Multiclass multilink bundles fragment packets of various priorities into multiple classes, allowing high-priority packets to be sent between fragments of lower priorities	See chapter 17 for more information about configuring multiclass multilink PPP bundles.
5620 SAM server resource management	The 5620 SAM groups NEs in the managed network according to function for increased network management efficiency.	See chapter 13 for more information.
SNMP trap management	The 5620 SAM supports the configuration of event notification policies to control which SNMP traps the 5620 SAM processes. This function conserves 5620 SAM server resources by filtering out unnecessary SNMP traps.	See chapter 13 for more information.
Alarm management enhancements	Additional functions are added to the Alarm Window, including: • the option to enable or disable showing correlated alarms • the option to filter alarms by OLC or severity state Additional functions are added to the Alarm Info form, including: • Affecting Objects tab button • Correlated Alarms tab button	See chapter 34 for more information about changes to alarm management.

(4 of 11)

Feature or function	Description	Reference for more information
Residential subscriber management enhancements	The 5620 SAM supports the following residential subscriber management functions: • using a SAP identifier as a subscriber identification string • associating a DSLAM identifier with a subscriber host • configuring a default subscriber identification string on a SAP • directly mapping the SLA profile string from a subscriber host to an SLA profile • directly mapping the subscriber profile string from a subscriber host to a subscriber profile	See chapter 64 for more information.
Increased protection from DoS attacks	The 5620 SAM supports the configuration of DoS protection on NEs and the creation of DoS protection policies for subscriber-based VPLS, IES, and VPRN access interfaces.	See chapter 18 for general information about DoS protection and for information about configuring DoS protection policies. See the appropriate service chapter for information about applying DoS protection policies to interfaces.
Subscriber packet mirroring	The 5620 SAM supports the specification of a subscriber or a subscriber host as a packet source for a mirror service.	See chapter 69 for more information about mirror service management.

(5 of 11)

Feature or function	Description	Reference for more information
OS 6850 support	The 5620 SAM supports the following functions on the OS 6850, Release 6.3.1: Equipment management: • variety of 24- and 48-port Ethernet chassis that support 10/100/1000, combo, and PoE Ethernet ports • chassis that can be used individually or connected in a stack of up to eight chassis • alarm and Ethernet port statistics • SNMP v1, v2, and v3	See chapter 15 for information about equipment management. See chapter 17 for information about configuring Ethernet ports.
	Backup and restore of configuration files	See chapter 21 for information about backup and restore.
	Software upgrade	See chapter 21 for information about software upgrades.
	Bridging and STP: • STP (802.1D), RSTP (802.1w), and MSTP (802.1Q 2005) • flat mode STP • 1x1 mode STP	See chapter 28 for information about bridge and STP configuration.
	VLAN service: • standard VLANs • stacked VLANs • IP multicast VLANs	See chapter 65 for information about VLAN configuration.
	IP routing and protocols: • display routing protocol status • configuration and management of routing instances and IP interfaces • configuration and management of static routes	See chapter 27 for information about configuring routing instances, Layer 3 interfaces, and static routes.
	Security: • RADIUS and TACACS+ authentication • learned port security	See chapter 18 for information about configuring RADIUS and TACACS+ server policies. See chapter 28 for information about configuring learned port security.
	OAM: • ICMP ping • traceroute	See chapter 35 for information about configuring ICMP ping and traceroute.
	QoS and ACLs: • Basic QoS—port-based QoS and global QoS polices • ACLs—port, Layer 2, and Layer 3 traffic filtering • UNI and SAP profiles	See chapter 43 for information about configuring UNI, SAP, and QoS policies and ACLs. See chapter 17 for information about configuring port-level QoS.
	Management • ability to start the WebView management tool from the 5620 SAM GUI	See chapter 17 for information about starting and stopping a WebView session.

Feature or function	Description	Reference for more information
7250 SAS-ES support	The 5620 SAM supports the following 7250 SAS-ES 3.0 features.	—
	Hardware: • configuring Ethernet port MTU	See chapter 17 for information about configuring Ethernet ports.
	MPLS: • creating and configuring MPLS interfaces • configuring MPLS routing instance properties • creating and configuring MPLS administrative groups • adding loose hops to an MPLS path • enabling dynamic bypass • creating and configuring secondary LSP paths	See chapter 29 for information about configuring MPLS. See the 7250 SAS-ES or 7250 SAS-ESA device documentation for information about configuring these parameters.
	OSPF routing instance: • viewing OSPF Router ID, Traffic Engineering Support, and Opaque Lsa Support parameters	—
	OAM: • creating and running an MEF MAC ping	See chapter 35 for information about configuring MEF MAC Ping.
	VPLS: • moved MTU configuration from the site configuration form to the spoke SDP configuration form • VC Type parameter is configurable when you configure a spoke SDP	See chapter 68 for information about configuring VPLS.
7250 SAS-ESA support	The 5620 SAM supports this new chassis. In addition to dry contacts, the 7250 SAS-ESA supports all of the 7250 SAS-ES features.	See chapter 17 for information about configuring dry contacts.
ECMP support	The 5620 SAM supports load balancing for LSP- based LDPs using equal cost routing on the 7450 ESS, 7710 SR, and 7750 SR, Release 5.0 or later. Routing configuration Functions that include the following are added: • tree discovery and path probing configuration • tree display of discovered FEC and ECMP paths Additional functions are added to the testing tool including: • LDP Tree Trace • LSP Ping enhancements • LSP Trace enhancements	See chapter 28 for information about configuring ECMP on a router.
Enhanced security management for 5620 SAM client GUI users and user groups	The security framework for 5620 SAM client GUI users and user groups is enhanced to allow you to assign users to a user group that is configured with span of control profiles. The profiles assign access rights to 5620 SAM server objects within a span. You can create span of control profiles to assign access permissions to a functional group of 5620 SAM Server objects. You can assign one or more spans of control to a span of control profile.	See chapter 8 for more information about how to create a span of control and span of control profiles.

(7 of 11)

Feature or function	Description	Reference for more information
Enhanced topology maps	Enhancements to the topology map provide more flexibility for managing and organizing network elements, including: • the ability to use the mouse to zoom in and out of the topology map • object icon size and line thickness is reduced when the map is in the zoom in mode to reduce topology map clutter • flat snapshot topology maps provide the ability to display large numbers of NEs and links. • the ability to select the NEs that are displayed using a filter • the ability to create, save and name a filter tree • addition of a Configure Info Tables button to create info table configuration for any map object • addition of Global Info Tables button to overlay info tables on a topology map • addition of Selected Info Tables button to apply an info table to one map object or a group of map objects • addition of a filter button for the flat snapshot topology maps • administrators can lock the map layout • the addition of a plus sign symbol to identify a group link, and an arrow pointing in the direction of the path to identify a unidirectional link or link group in a flat map topology view	See chapter 4 for information about topology map enhancements.
Rapid withdrawal on BGP	The 5620 SAM supports Rapid withdrawal functions. You can configure BGP messages to be sent immediately to reduce BGP processing load.	See chapter 28 for information about configuring Rapid Withdrawal on BGP.
IPCP on IES services	The 5620 SAM supports IPCP to enable inter-operability with remote networks.	See chapter 70 for information about configuring IPCP on an IES service.
Mac Move Extension support	The 5620 SAM supports Mac Move Extension for marking a VPLS SAP as non-blockable.	See chapter 68 for information about configuring Mac Move Extension.
Ethernet Hold-off Timer enhancement	The 5620 SAM supports a maximum value of 50 seconds for the Hold-off Timer and Hold-down Timer for all Ethernet ports.	See chapter 168 for information about configuring Hold-off Timer and Hold-down Timer.
LDP synchronization timer support	The 5620 SAM supports LDP synchronization timer functions for IS-IS and OSPF routing protocol. The timer can be set to allow IGP and LDP to converge after a failure.	See chapter 27 for information about configuring LDP Synchronization Timing.
BFD on router interfaces and IES and VPRN interfaces	The 5620 SAM supports BFD configuration to identify the status of remote routers. When enabled BFD is able to quickly detect failures.	See chapter 28 for information about configuring BFD.
Forwarding class support	5620 SAM supports forwarding class on MAC Trace, CPE Ping, VPRN Ping and VPRN Trace diagnostic tests	See chapter 35 for information about configuring Forwarding Class.
Link loss forwarding support	5620 SAM supports link loss forwarding on a VLL Layer 2 access interface.	See chapter 67 for information about configuring link loss forwarding.

(8 of 11)

Feature or function	Description	Reference for more information
Apipe and Epipe service enhancement	5620 SAM supports multi-chassis link aggregation and pseudowire redundancy for Apipe and Epipe services.	See chapter 67 for information about configuring MC-LAG and PW for Apipe and Epipe services.
Scheduling enhancements	The following are added to the scheduling function: • a time zone field to display the client and the server time zones. • an option to set the day of the week or month of the year for a schedule to run	See chapter 74 for information about creating schedules.
Egress remarking and traffic management enhancements	The following enhancements have been added to the 5620 SAM policy framework: • ability to classify frames with the DE bit set as in or out of profile. • allow remarking of the DE bit • set the dot1p parameter • allow overbooking of ATM shaped traffic • allow creation and distribution of DSCP remarking policies • allow frame-based accounting	See chapter 43 for more information about policies.
Policy enhancements	The 5620 SAM policy framework includes a policy audit function to identify mismatches between local and global policies.	See chapter 43 for information about configuring a policies audit.
Object life cycle state	5620 SAM supports setting the OLC of the following objects and services: • network element • card slot • daughter card • port • LAG • composite service • service • site You can set the OLC state of the object or service to maintenance or in-service.	See chapter 34 for information about setting the OLC state.
IEEE 802.1ag Connectivity Fault Management (CFM) OAM standard for detecting, isolating and reporting connectivity faults in an Ethernet network	The 5620 SAM supports the IEEE 802.1ag Connectivity Fault Management (CFM) OAM standard. IEEE 802.1ag provides protocols for: • path discovery • fault detection • fault verification • fault notification An Ethernet network can be partitioned into a hierarchical levels to detect connectivity failures.5620 SAM supports end-to-end service management in a Layer 2 network and provides the following diagnostics tests to detect a connectivity failure: • CFM Connectivity Check • CFM Loopback • CFM Link Trace	See chapter 43 for information about how 5620 SAM supports the IEEE 802.1ag standard. See chapter 35 for information about conducting CFM tests.

(9 of 11)

Feature or function	Description	Reference for more information
Support for new PPPoE policy, DHCP server and local user database	5620 SAM supports PPPoE in subscriber networks to encapsulate PPP frames inside Ethernet frames. PPPoE combines the point-to-point protocol used with DSL sessions with the Ethernet protocol used to support multiple subscribers in a local area network. PPPoE takes advantage of the speed of a packet-based Ethernet network with the security and accounting functions of a PPP network. PPPoE allows service providers to use existing Radius authentication.	See chapter 64 for information about configuring a PPPoE policy, DHCP server and creating a local user database.
	5620 SAM supports configuring local DHCP servers on a 7750 SR and 7710 SR, Release 6.0 or later. The local DHCP server leases IP addresses to clients in the network. A local user database is used to authenticate and authorize clients requesting IP addresses from the local DHCP server. If the local DHCP server does not use the local user database, The server can use the GI address to assign free IP addresses.	
	5620 SAM supports configuring a local database on a 7750 SR and 7710 SR, Release 6.0 or later. The local user database is configured and associated with the local DHCP server to provide local authentication.	
Log file consolidation	The 5620 SAM log files are collocated in the *installation_directory*/nms/log directory.	See the *5620 SAM Maintenance Guide* and *5620 SAM Troubleshooting Guide* for more information about the log directory.
5620 SAM statistics enhancements	Enhancements to statistics includes: • configuration and setup of statistics from a single menu • statistics policies accessible from the object configuration form • statistics collection for specific NEs or objects at different collection intervals • real-time statistics collection • graphical view of historical or real-time statistics data	See the *5620 SAM Statistics Management Guide* for information about 5620 SAM statistics.
7705 SAR, Release 1.0 feature support	The 7705 SAR, Release 1.0, has a subset of features that are supported on the 5620 SAM for the 7750 SR, Release 6.0. See the *5620 SAM NE Compatibility Guide* for more information.	—
7705 SAR, Release 1.0 hardware support	The 7705 SAR, Release 1.0, supports the following daughter card types: • 16 × Channelized DS1/E1 ASAP • 6 × 10/100 Ethernet + 2 × 10/100/1000 Ethernet SFP	See chapter 15 for more information.
PIM snooping for VPLS	The 5620 SAM supports PIM snooping for VPLS, which allows a VPLS PE router to build multicast states by snooping PIM protocol packets that are sent over the VPLS.	See chapter 68 for more information.
MLD snooping for VPLS	MLD snooping is basically the IPv6 version of IGMP snooping. The guidelines and procedures are very similar to IGMP snooping as well.	See chapter 68 for more information.
L3 Multicast Load Balancing Enhancement for ECMP	The new ECMP rebalancing scheme is based on bandwidth, which solves problems related to multicast channel distribution over links that are being added or returned to ECMP connections and the joining of ECMP links based on bandwidth	See chapter 28 for more information.
IPV6 PIM-SSM	The current PIM-SSM implementation on the 7750 SR is extended to support the IPv6 address family.	See chapter 28 for more information.

(10 of 11)

Feature or function	Description	Reference for more information
Service Mirroring enhancements	IP-only mirroring and PPP Port-ID mirroring capabilities have been added to service mirrors.	See chapter 69 for more information.
TE Metric	Traffic Engineering (TE) Metric is a new feature introduced in 7750 SR/7450 ESS/7710 SR that allows CSPF to compute the shortest path (SPF) using this new metric.	See chapters 28 and 29 for more information.
Shared Risk Link Groups	SRLGs for the 7750 SR/7450 ESS/7710 SR allows the user to establish a backup secondary LSP path or a FRR LSP path which is disjoint from the primary LSP path.	See chapters 27 and 29 for more information.
RSVP-TE Refresh Reduction	Three mechanisms are introduced to improve scalability, reliability and performance of the RSVP TE protocol. They are RSVP message bundling, reliable message delivery, and summary refresh.	See chapter 28 for more information.
Control Word for VPLS	The control word feature provided to add a control word for VLL service packets supports the same functions for an Ethernet PW used as a mesh or spoke SDP in a VPLS.	See chapter 68 for more information.
Redundant Spoke-SDP Connection to VPLS	The redundant spoke SDP to VPLS service feature provides active/standby PWs into VPLS services. It provides data flow control for dual-homing with spoke-sdp access without using STP.	See chapter 68 for more information.
L2PT Enhancement	L2PT enhancement centralizes the L2PT termination configuration on VPLS L2 interfaces that are managed by a MVPLS L2 interface.	See chapter 68 for more information.
Down-When-Looped	Down-When-Looped monitors a physical loop (by transmitting periodical messages) and blocks accidental loops that can occur as a result of provisioning.	See chapter 17 for more information.
CPE Connectivity Test	This feature allows static routes to monitor the availability of the far-end using a periodic polling mechanism.	See chapters 71 and 27 for more information.
Ingress VLAN Translation support	This feature allows ingress VLAN translations by employing Ingress VLAN Rewrites and Ingress VLAN Swapping.	See chapters 67 and 68 for more information.
VCCV Trace	VCCV trace can trace the entire path of a PW with a single command issued at the T-PE or at an S-PE. This is equivalent to LSP-Trace.	See chapter 35 for more information.
Service Management Enhancements	These enhancements include changes to the display of certain operational and alarm flags. These appear on the General tab of all service configuration forms.	See the service chapters and chapter 2 for more information.
Ingress Multicast Path Management	Ingress Multicast Bandwidth policies are used to manage the ingress multicast path bandwidth of the multicast forwarding paths into the switching fabric.	See chapters 15, 17, 27, 43, 68, and 71 for more information.
TPSDA L2-CO extensions for Multi-Chassis Ring	This is an extension of dual homing support in TPSDA networks based on the L2-CO model. The extension addresses networks where multiple access nodes such as DSLAMs are connected in a single ring.	See 42 chapter for more information.
Support for the 7450 ESS 6-slot chassis	The 7450 ESS chassis configurations that are managed include the following shelf type: • 6-slot with 2 switch fabric card slots and 4 IOM slots The 7450 ESS-6v supports the 2 × 10-Gig MDA IOM, the 2 × 10-Gig MDA Oversubscribed IOM Card, the 2 × 10-Gig MDA IOM Card, B, and the 80g CPM / Switch Fabric 2.	See chapter 15 for more information.

(11 of 11)

3.5 5620 SAM Release 5.0 features

Table 3-5 lists the features and functions added in 5620 SAM Release 5.0.

Table 3-5 5620 SAM Release 5.0 features

Feature or function	Description	Reference for more information
Release 5.0 R6 features		
Multichassis synchronization	You can configure the synchronization of dynamic state information of subscriber management between two NEs in a redundant configuration. MC synchronization can be used to ensure that the following dynamic state information is synchronized: • basic and enhanced subscriber management • IGMP snooping in VPLS • IGMP on IES or VPRN group interfaces • SRRP on VPRN	See chapter 41 for more information.
Release 5.0 R5 features		
5620 SAM auto-client update	5620 SAM client configuration changes and software upgrades are automated. When a 5620 SAM client starts and detects an available configuration update or software upgrade on the 5620 SAM server to which it connects, the client automatically applies the update.	See the *5620 SAM | 5650 CP AM Installation and Upgrade Guide* for information about installing and upgrading the 5620 SAM client software. See chapter 5 for information about changing client configurations. See chapter 2 for information about client GUI startup options.
Telco T5C	The 5620 SAM does not support policy creation or application for Telco devices, Release 6.5 or later.	—
Feature support on the 7250 SAS and 7250 SAS-ES	• The 7250 SAS supports structured agnostic traffic over packet (SAToP) and CES over packet-switched networks (CESoPSN) for the transport of structured and unstructured TDM traffic over Ethernet or MPLS. The CES circuits can be configured as termination points on standard VLANs and TLS VLAN services. • Policies are not supported on Release 2.0 or later of the 7250 SAS and 7250 SAS-ES • TDM port and CES circuit threshold crossing alarms • Statistics for physical ports and interfaces • VLAN SAP enhancements Ability to specify the encapsulation type, tagged or untagged, on a VLAN access interface.	See chapter 17 for more information about 7250 SAS CES services. See chapter 65 for more information about VLAN service management.

(1 of 11)

Feature or function	Description	Reference for more information
Feature support on the 7250 SAS-ES	The 7250 SAS-ES is an enhanced version of the 7250 SAS. The 7250 SAS-ES supports all of the features available on the 7250 SAS plus several additional features not available on the 7250 SAS: • The 7250 SAS-ES incorporates two additional uplink ports that support additional features, including MPLS and VPLS. • A new ring group type, VPLS, in addition to the existing VLAN type. The 7250 SAS-ES can be added to a VPLS ring group. • Viewing of routing instances. Routing instances must be configured using CLI. • Viewing of L3 interfaces configured on the enhanced uplink ports. The L3 interfaces must be configured using CLI. • Configuration of MPLS paths and RSVP LSPs. The protocols for MPLS, LDP, and RSVP must be enabled using CLI. • Fast Reroute using guarding LSPs. There is no interoperability between Fast Reroute on the 7250 SAS-ES and other devices such as the 7750 SR. • Creation and management of VPLS	See chapter 17 for more information about 7250 SAS CES services. See chapter 65 for more information about VLAN service management.
APS support on channelized ASAP MDA	The APS support on channelized ASAP MDAs includes the following: • ASAP MDA channelization • deep channel support • APS IMA bundle groups	See chapter 37 for more information about how to configure APS. See chapter 17 for more information about how to configure multilink bundles.

Local policy enhancements	The following enhancements have been added to the 5620 SAM policy framework:
	• Global policies are created in draft mode and cannot be distributed until they are set to released mode.
	• You can compare two local policies to locate and highlight differences.
	• Read-only attributes are included in a policy audit
	• Local policies have two distribution modes:
	  • Sync with global
	  The local policy is locked in sync with the global policy at all times
	  • Local edit only
	  The policy can be edited locally only. Global changes are not synchronized with the local policy.
	• The Configuration Action parameter is set to Merge With Existing and is no longer configurable.
		See chapter 43 for more information.

Remote network monitoring policy	The 5620 SAM supports the mapping of remote network monitoring events to information alarms in the GUI.	See chapter 43 for more information.
Scheduling support using NE cron jobs	The 5620 SAM supports the creation of schedules and scheduled tasks that use the NE cron service and can be deployed to multiple NEs.	See chapter 74 for more information.
Generic NE alarm and interface support	5620 SAM generic NE management supports a variety of interface types and some standard system and interface SNMP traps. These enhancements allow the 5620 SAM to more directly manage generic NEs using script management and allows the use of a generic NE interface as the endpoint of a 5620 SAM physical link.	See chapter 15 for generic NE support information. See chapter 12 for generic NE commissioning information.

(2 of 11)

Feature or function	Description	Reference for more information
MD5 authentication for RSVP-TE sessions	The 5620 SAM supports the assignment of an MD5 key to an RSVP interface for increased session security.	See chapter 28 for more information.
GSMP support	You can configure GSMP to open an ANCP session within a VPLS or VPRN service on the 7450 ESS, and 7750 SR.	See chapters 68 and 71 for more information about using GSMP.
ANCP support	You can create ANCP policies to operate within a VPLS, VPRN, VLL or IES service.	See chapters 43, 64, 67, 68, 70, and 71 for more information.
ANCP loopback diagnostic	You can create an ANCP loopback diagnostic to send OAM messages.	See chapter 35 for more information.
802.3ah EFM OAM	You can configure an 802.3ah EFM OAM diagnostic on a physical port that supports Ethernet framing. The 802.3ah EFM OAM feature is not dependent on the Ethernet mode or the encapsulation type configured on the port being tested.	See chapter 17 for more information.
OAM ANCP test	You can create an OAM ANCP test to send OAM messages.	See chapter 35 for more information.
Ethernet OAM (802.3ah)	The 5620 SAM supports the configuration of EFM OAM on any physical port that supports Ethernet framing. The test network setup requires two physical ports that support EFM OAM. This function is not dependent on the Ethernet mode or encapsulation type on the ports under test.	See chapter 17 for more information.
Routed CO Dual Homing, using SRRP	SRRP allows two separate connections to an access node such as a DSLAM to operate in an active/standby configuration similar to the way in which VRRP interfaces operate.	See chapters 70 and 71 for more information.
Class-based forwarding	Packets belonging to a specific service can be preferentially forwarded based on the class-of-service (CoS). Packets of the same CoS and service are forwarded over a specific RSVP LSP or a static LSP, which is part of an SDP that the service is bound to.	See chapter 30 for more information.
Manual bypass tunnel	You can manually configure an LSP to be bypass-only on a Point-of-Local-Repair NE. This LSP is then used exclusively for bypass protection.	See chapter 29 for more information.

(3 of 11)

Feature or function	Description	Reference for more information
Release 5.0 R3 features		
Feature support on the 7710 SR, Release 5.0	The 7710 SR, Release 5.0 inherits all the features that are supported on the 5620 SAM for the 7750 SR, Release 4.0, which include the following: • **Service-related features** • Ipipe VLL • default SAP on a Dot1 Q port • L2PT for VPLS • BPDU translation for VPLS • MSTP for MVPLS • inter-AS connections for VPRN • OSPFv2 as IGP among CE and PE routers for VPRN • interface-triggered MAC flush for VPRN • VPRN direct route comparison of BGP and MP-BGP learned routes • ATM SAP terminations for VPRN and IES • data-MDT support for VPRN • Epipe SDP spoke termination on VPRN • **TPSDA features** • ARP reply agent • multipoint shared-queue policies • policy-based forwarding for VPLS • subscriber-host connectivity verification • routed CO and L3 group interfaces • DHCP proxy server • DHCPv6 • DHCPv6 prefix delegation • multicast CAC policies • MC LAG • L3 subscriber interfaces • RADIUS authentication of DHCP sessions for VPRN SAPs • IP multicast on residential SAPs • MVR on VPLS • MAC learning protection • efficient multicast replication through the use of egress multicast groups • residential subscriber management • residential split horizon groups • Web portal redirect • **System and system management** • non-stop routing for PIM and IGMP graceful restart • APS support on multiple devices • LACP enhancements • NTP • SSHv2 support • SNMP support for ICMP Ping and Traceroute • ILMI 3.1 and 4.0 support for ATM • MP-BGP • anycast RP for PIM-SM	—

(4 of 11)

Feature or function	Description	Reference for more information

Feature support on the 7710 SR, Release 5.0 (continued)	• **Routing**
	• IPv6 support
	  • BGP peering
	  • IS-IS adjacencies
	  • multicast routing
	  • static routes
	  • ICMP
	  • routing policies
	  • access ingress and egress policies
	  • CPM filter policies
	  • PPP
	  • IES SAPs
	• **MPLS**
	• ECMP support for LDP-based LSPs
	• **OAM**
	• VCCV ping for VLL
	• ATM OAM loopbacks
		—

Hardware support for the 7710 SR, Release 5.0	The 7710 SR, Release 5.0 includes support of the following daughter card types: • 2 × OC12/OC3 CMA • 4 × ATM OC12/OC3 • 2 × OC12/OC3 CMA when the daughter card slot is not configured for MDA carrier module support	See chapter 15 for more information.
Copying and moving SAPs between ports	You can copy and move SAPs between physical Ethernet ports, logical ports, or a combination of both.	See chapter 15 for more information.
Port scheduler	You can create port scheduler policies to define hierarchical bandwidth allocation and scheduling at the egress port level.	See chapter 43 for more information.
Release 5.0 R1 features		
Distributed server architecture	The 5620 SAM server can be installed in a cluster configuration that consists of a main server and one or more auxiliary servers. Auxiliary servers extend the network management processing engine by performing routine functions such as accounting and performance statistics collection, thus making more processing resources available to the main 5620 SAM server. Auxiliary-servers are supported for standalone and redundant configurations on Solaris platforms only.	See chapter 6 for information about auxiliary server cluster functions. See the *5620 SAM System Architecture Guide* for information about 5620 SAM distributed server architecture. See the *5620 SAM Planning Guide* and *5620 SAM | 5650 CP AM Installation and Upgrade Guide* for information about auxiliary server configuration.

(5 of 11)

Feature or function	Description	Reference for more information
Security management for 5620 SAM client GUI users and user groups	The security framework for 5620 SAM client GUI users and user groups allows you to define the access permissions on 5620 SAM server object types, or packages. You can create scope of command roles to suit specific functions in your operations by assigning specific access permissions to different functional areas of the 5620 SAM. You can create scope of command profiles to assign access permissions to a functional group of 5620 SAM Server objects. You can assign one or more scope of command roles to a scope of command profile.	See chapter 8 for more information about how to create scope of command profiles and roles.
Support for Sun AMD-based server installation	The 5620 SAM supports the installation of a server or database component on a Sun workstation built using the AMD x86-based processor architecture.	See the *5620 SAM Planning Guide* for information about 5620 SAM platform requirements.
Installer improvements	The 5620 SAM installer: • performs data-collection in one initial pass, when possible • displays a running progress indicator during time-intensive activities • preserves existing backup and configuration files • allows customized documentation installation • has executable files that are named using version information for ease of identification	See the *5620 SAM | 5650 CP AM Installation and Upgrade Guide* for information about installing 5620 SAM components.
New Oracle version	The 5620 SAM, Release 5.0, uses Oracle version 10r2 as the relational database management system.	See the *5620 SAM Planning Guide* and *5620 SAM | 5650 CP AM Installation and Upgrade Guide* for more information about 5620 SAM system requirements and planning guidelines.
Residential subscriber monitoring and active DHCP management	Residential subscriber management supports the periodic monitoring of DHCP events for subscriber hosts on SAPs, and provides host DHCP lease-state management.	See chapter 64 for information about residential subscriber host management.
Support for the 7450 ESS 6-slot chassis	The 7450 ESS chassis configurations that are managed include the following shelf type: • 6-slot with 2 switch fabric card slots and 4 IOM slots The 7450 ESS-6 supports the 2 × 10-Gig MDA IOM, the 2 × 10-Gig MDA Oversubscribed IOM Card, the 2 × 10-Gig MDA IOM Card, B, and the 80g CPM / Switch Fabric 2.	See chapter 15 for more information.
Support for new hardware	The 1 × 10-Gig Ethernet + 10 × 10/100/1000 Ethernet SFP is supported on the following IOM cards: • 2 × 10-Gig MDA IOM 2 on the 7750 SR, Release 5.0 or later • 2 × 10-Gig MDA IOM Card, B on the 7750 SR and 7450 ESS, Release 5.0 or later • 2 × 10-Gig MDA Oversubscribed IOM Card on the 7450 ESS, Release 5.0 or later The 1 × 10-Gig Ethernet + 10 × 10/100/1000 Ethernet SFP has 10 1-Gigabit SFP modules and one 10G-Base Ethernet XFP module.	See chapter 15 for more information about supported daughter cards.

(6 of 11)

Feature or function	Description	Reference for more information
Updated NE maintenance functions	The 5620 SAM provides convenient on-demand and policy-based functions for performing managed-device configuration backup and restore operations, software upgrades. The status of a maintenance operation is displayed as it occurs. Device configuration backups are stored in the 5620 SAM database and can be The software upgrade function includes scheduling, version confirmation and deferred software activation after an upgrade.	See chapter 21 for information about NE maintenance.
Alarm management enhancements	The 5620 SAM Alarm Window contains additional functions that include the following: • an Additional Text Policy configuration form to display the information about an alarmed object on the dynamic alarm list • a Manage filter form to create, select, and display specified network alarms • a Pause button to scroll lock the dynamic alarm list • a Count field to identify the number of alarms listed • the option to enable or disable the Monitoring Flag Panel • the option to open and view multiple alarm windows	See chapter 34 for more information about changes to alarm management.
Service mirroring enhancements	The 5620 SAM supports the configuration of ATM-SDU as an encapsulation type for a mirror service site.	See chapter 69 for information about service mirroring.
VLL switching and redundancy	VLL spoke switching allows you to create a VLL service by cross-connection two spoke SDPs. Spoke switching allows you to scale L2 services, such as VLLs and H-VPLS, over a multi-area network without the requirement for a full mesh T-LDP. The 5620 SAM supports spoke switching on all VLL types, however, all service instances must be the same type. VLL redundancy requires that you associate the SAP or SDP bindings to an endpoint. You can configure the endpoint association as active or standby so that you can create a redundant configuration. The associated NEs use signalling to determine the active SAP or SDP binding. The 5620 SAM supports VLL switching and redundancy for 7750 SR and 7450 ESS Release 5.0 devices.	See chapter 67 for information about VLL switching and redundancy.
NSR for OSPFv3	The 5620 SAM supports non-stop routing on a 7750 SR with two CPMs. If the active CPM fails, the standby CPM takes over and all OSPF states (for example, sessions and neighbors) remain intact.	—
Client GUI improvements	GUI improvements provide more flexibility on configuration forms and list forms, including: • new buttons Next Page, Previous Page, and Count • ability to copy and paste read-only fields • the addition of a Delete button to replace the two Remove buttons to ensure services are not inadvertently deleted • the ability to perform a SSH/Telnet session on a network element from the manage equipment form	See chapter 2 for information about GUI improvements.
5620 SAM server performance and network statistics collection	The 5620 SAM collects server performance and network statistics, which include: • memory usage and alarm counters for each 5620 SAM server • SNMP trap counters, accounting and SNMP polled statistics records counters, and network element resync counters, for each 5620 SAM server A default statistics log policy and configurable default collection interval for each statistics counter determine the frequency of server performance and network statistics collection from 5620 SAM servers.	See chapter 5 for information about 5620 SAM server performance and network statistics.

(7 of 11)

Feature or function	Description	Reference for more information
Topology map enhancements	Enhancements to the topology map provide more flexibility for managing and organizing network elements, including: • the ability to create a physical link by right-clicking on the topology map • the ability to select and move a group of objects using the Shift key or by drawing a rectangle around a group of objects • thicker lines to represent the path between linked objects in a group, making the whole path more visible on the topology map • the ability to apply the auto-layout option to a selected group of objects • topology map icons reduced in size for improved scalability • the addition of a plus sign symbol to replace the circle icon to identify a group link, and an arrow pointing in the direction of the path to identify a unidirectional link or link group • the relocation of the alarm status information from the top of the topology map icons to the right hand side of the topology map icons	See chapter 4 for information about topology map enhancements.
MSDP management support	The 5620 SAM supports MSDP on the 7750 SR and 7710 SR, Release 5.0 or later, to allow multiple PIM-SM domains to communicate with each other using their own RPs. MSDP also enables multiple RPs in a single PIM-SM domain to establish MSDP mesh-groups, and can be used between anycast RPs to synchronize information about the active sources being served by each anycast RP peer.	See chapter 28 for information about MSDP management support.
Policy enhancements	The following enhancements have been added to the 5620 SAM policy framework: • The 5620 SAM supports the partial distribution of global policies. Global policies, properties, or entries that are not supported by a network element are not distributed. • You can compare a local policy with a global policy to locate and highlight differences.	See chapter 43 for more information about policies.
Time of day policies	The 5620 SAM supports the creation of time of day policies that allow you to configure time-based QoS policies, ACL filters, and schedulers that are applied to aggregation schedulers and L2 and L3 access interfaces.	See chapter 43 for more information about policies.
Channelized ASAP MDA enhancements	The following features are supported on the channelized ASAP MDA: • SONET framing • DS1 and E1 channelization • DS3/E3 clear channel configuration • ATM cell mapping into a DS3 channel of an ATM interface (ATM direct mapping or PLCP mapping)	See chapters 15 and 17 for more information.
Network support for PPP-encapsulated DS3/E3 ports on channelized ASAP MDAs	Network mode is supported for DS3/E3 ports on channelized ASAP MDAs. You can configure DS3/E3 ports as network interfaces on the 7750 SR and 7710 SR, Release 5.0 or later.	See chapter 17 for more information.
Multilink bundle enhancements on channelized ASAP MDAs	You can create IMA bundles and multilink bundles on channelized ASAP MDAs. IMA version 1.0 specification is supported for IMA group bundles. Link fragmentation and interleaving is supported for multilink PPP bundles on channelized ASAP MDAs.	See chapter 15 for more information about IMA. See chapter 17 for more information about how to configure multilink bundles on channelized ASAP MDAs.

(8 of 11)

Feature or function	Description	Reference for more information
Script manager enhancements	You can create XML API scripts in the 5620 SAM script manager to execute more complex commands or tasks on the 5620 SAM. You can create Velocity-based CLI and XML API scripts.	See the *5620 SAM Scripts and Templates Developer Guide* for more information about how to create XML API scripts.
TCP authentication enhancements	The 5620 SAM supports the creation, modification, and distribution of TCP key chains and keys for increased security during BGP and LDP communication between NEs.	See chapter 20 for information about managing TCP enhanced authentication.
Support for multichassis LAG configurations	LAG configurations are supported over multiple devices to provide device-level redundancy in addition to link-level redundancy for link aggregation groups. A MC LAG configuration provides redundant L2 access connectivity that extends beyond link-level protection by allowing two devices to share a common LAG endpoint.	See chapter 37 for information about how to create multichassis LAGs.
Support for LDP-over-RSVP LSPs	The 5620 SAM supports the creation of LSPs using RSVP over LDP, which is also called tunnel-in-tunnel.	See chapter 29 for information about configuring LSPs using LDP over RSVP.
DHCP relay enhancements	Enhancements to the 5620 SAM DHCP relay function allow relay agents to append Option 82 information to DHCP packets.	See chapters 68, 70, and 71 for information about configuring DHCP relay in a 5620 SAM service.
DHCP for IPv6 support	You can configure DHCPv6 on IES L3 access interfaces on the 7710 SR and 7750 SR, Release 5.0 or later.	See chapter 70 for more information about configuring DHCPv6 on IES SAPs.
Channel framing enhancements	G.703 framing is supported on the 7750 SR, Release 5.0 or later. This allows you to configure unstructured E1 channels on deep-channel MDAs and channelized ASAP MDAs.	See chapter 17 for more information about configuring channels.
RADIUS enhancements	The 5620 SAM includes the following RADIUS enhancements: • Configuration of RADIUS authentication policies on the 7450 ESS, 7750 SR, and 7710 SR, Release 5.0 or later, for specific subscriber hosts. • Change of Authorization messages support RADIUS CoA messages are included to process unsolicited messages in subscriber authentication from the RADIUS server • RADIUS attribute support Standard and VSA attributes can be included in the authentication request messages	See chapter 18 for information about configuring RADIUS authentication policies.
RADIUS-based accounting policy	You can configure RADIUS-based accounting policies on the 7450 ESS, 7750 SR, and 7710 SR, Release 5.0 or later, for specific subscriber hosts. RADIUS-based accounting policies send accounting information on subscriber host sessions to RADIUS servers.	See chapter 43 for information about configuring RADIUS-based accounting policies.
Automatic service-tunnel management	The 5620 SAM supports the automatic creation of service tunnels between devices based on the network topology.	See chapter 30 for information about configuring auto-tunnel functions.

(9 of 11)

Feature or function	Description	Reference for more information
Operational-state reporting for VLL services	The management form for a VLL service displays indicators to provide information about end-to-end VLL connectivity.	See chapter 67 for information about operational state reporting for VLL services.
STM enhancements	The following enhancements have been added to the 5620 SAM STM system: • You can create ICMP ping and ICMP trace OAM tests for a group of routers or between VRFs in a VPRN group • You can create threshold-crossing events for non-NE-schedulable tests, and specify whether OAM tests are deployed and remain on an NE	See chapters 35 and 75 for information about configuring OAM tests and threshold crossing events.
IPv6 over MPLS	The 5620 SAM supports IPV6 label advertisement to enable IPv6 over MPLS.	See chapter 28 for more information about configuring an IPv6 label advertisement.
IGMP support for VPRN services	IGMP can be enabled and configured to operate within a VPRN service on the 7750 SR, and 7710 SR, Release 5.0 or later.	See chapter 71 for more information about IGMP support for VPRN services.
VPRN service topology map enhancement	The 5620 SAM supports an enhanced topology view to more accurately display a VPRN service. The import/export VRF targets of sites in the VPRN service are compared, and the most likely route of forwarded traffic is displayed.	See chapters 71 and 4 for more information about using the topology map for a VPRN service.
VPRN hub and spoke configuration	The 5620 SAM supports the simplified configuration of hub and spoke VPRNs. You can specify normal, hub and subscriber-split-horizon as the configuration type during VPRN creation.	See chapter 71 for more information about configuring a VPRN hub and spoke configuration.
Proxy neighbor discovery	The 5620 SAM supports proxy neighbor discovery on network interfaces and IES L3 access interfaces. Proxy neighbor discovery is a means by which one interface responds to a neighbor discovery query on behalf of another interface.	See chapters 27 and 70 for information about configuring proxy neighbor discovery.
Router advertisement prefix enhancements	You can configure the preferred lifetime and valid lifetime of a router advertisement prefix.	See chapters 27 and 70 for information about configuring router advertisement prefixes.
IP SAP egress dot1P Q in Q classification	Allows the specification of which dot1P bits to mark in a Q in Q encapsulated packet during egress on a SAP.	See the service creation procedural information in the appropriate service management chapter to configure encapsulation value on interfaces. See chapters 67, 68, 70, 71 and 69 for VLL, VPLS, IES, VPRN and Mirror Service QoS configuration information.

(10 of 11)

Feature or function	Description	Reference for more information
Remote authentication and authorization	The 5620 SAM, Release 5.0 or later, uses a JAAS security framework to provide authentication and authorization services. Depending on the samvsa flag setting in the SamJaasLogin.config file, two remote authentication and authorization scenarios are available for remote users that do not have a 5620 SAM client user account. • The remote server authenticates the user and the 5620 SAM provides the user group to which the user belongs. • The remote server authenticates the user and provides the user group to which the user belongs to the 5620 SAM.	See chapter 8 for information about configuring remote authentication and authorization for remote users that do not have a 5620 SAM client user account.
Routed CO for VPRNs	The 5620 SAM supports the aggregation of L3 SAPs on group interfaces for VPRN services. This feature allows the direct connection of customer access equipment, such as a DSLAM, to a router such as the 7750 SR, Release 5.0 or later. Routed CO function works with residential subscriber management in the 5620 SAM to support a variety of service-delivery models. A VPRN routed CO allows a service provider to resell wholesale carrier services while providing direct DSLAM connectivity. You can create a VPRN service for the retailer and also define subscriber access and configuration information for the retailer network.	See chapter 64 for more information about routed COs. See chapter 71 for information about configuring a routed CO in a VPRN.
Multiple OSPFv2 instances	The 5620 SAM supports the configuration of multiple instances of OSPFv2 on the same device for the 7750 SR, 7450 ESS, and 7710 SR, Releases 5.0 or later.	See chapter 28 for information about configuring multiple OSPFv2 instances.
Support removed for earlier 7450 ESS, 7750 SR, and 7710 SR devices	You cannot use the 5620 SAM Release 5.0 or later to manage Release 2.1 or earlier devices. The devices must be upgraded to Release 3.0 or later.	—

(11 of 11)

3.6 5620 SAM Release 4.0 features

Table 3-6 lists the features and functions added in 5620 SAM Release 4.0.

Table 3-6 5620 SAM Release 4.0 features

Feature or function	Description	Reference for more information
Release 4.0 R5 features		
Channelized ASAP MDA	The following MDA can be configured in the daughter card slot of the 2 × 10-Gig MDA IOM 2 card on the 7750 SR, Release 4.0 or later: • 4 × Any Service Channelized OC-3	See chapter 15 for more information about supported daughter cards.
IMA group bundles	You can create IMA group bundles on channelized ASAP MDAs to group E1 and DS1 ATM paths into a single logical ATM interface.	See chapters 15 and 17 for more information about how to configure IMA group bundles.

(1 of 9)

Feature or function	Description	Reference for more information
Support for the 7450 ESS 12-slot chassis	The 7450 ESS chassis configurations that are managed include the following shelf type: • 12-slot with 2 switch fabric card slots and 10 IOM slots The 7450 ESS-12 supports the 1 × 10-Gig MDA IOM; the 2 × 10-Gig MDA IOM; the 2 × 10-Gig MDA IOM Card, B; and the 400g CPM/Switch Fabric 2. In addition, the 7450 ESS-12 supports all the MDAs supported by the 7450 ESS-1 and the 7450 ESS-7.	See chapter 15 for more information.
Support for the 7710 SR-c4	The 5620 SAM supports network and element management of the 7710 SR-c4. The c4 is a compact, lower-cost, 7710 SR variant that retains the features, functions and interface-card support of the 7710 SR-c12. The 7710 SR-c4 supports up to 4 CMAs or 2 MDAs, and has a maximum system throughput of 9Gb/s.	See chapter 15 for general information about managed device support. See the 5620 SAM documentation suite for descriptions of 5620 SAM management of devices.
Multichassis APS groups	You can configure an APS group with working channels and protection channels on two independent devices. Multichassis APS configurations are supported on the 7750 SR, Release 4.0 or later.	See chapter 37 for more information about APS groups.
Mirror service templates	Mirror service management users can create mirror service templates. Only users with Mirror-Service Mgmt privileges can create, modify, delete or view any mirror service-related objects in the 5620 SAM.	See chapter 69 for more information about mirror service management. See chapter 8 for more information about user groups and permissions.
Dynamic ACL policies	You can use the 5620 SAM, 5620 SAM-O, and Velocity templates to dynamically manage dynamic ACL policies for 5750 SSC subscriber services.	See chapter 10 for more information about dynamic ACL policies for 5750 SSC subscriber services.
Release 4.0 R5 enhancements to previous functions		
Chassis mode configuration on the 7450 ESS-12	Chassis modes A and B can be configured on the 7450 ESS-12, Release 4.0 or later.	See chapters 15 and 17 for more information about chassis modes.
Residential subscriber management on the 7450 ESS-12	The 5620 SAM supports the management of residential subscribers and residential subscriber hosts on the 7450 ESS-12.	See chapter 64 for more information about residential subscriber management.
Release 4.0 R3 features		
New IOM card on the 7450 ESS-7, Release 4.0 or later	The 7450 ESS-7, Release 4.0 or later, supports the 2 × 10-Gig Oversubscribed MDA IOM card. The 2 × 10-Gig Oversubscribed MDA IOM card has two Ethernet MDA slots that share a single Flexible Fast Path complex. The two MDAs share network and access ingress QoS policies.	See chapter 15 for more information. See the specific device documentation for more information.

(2 of 9)

Feature or function	Description	Reference for more information
Additional integration configurations between 5620 SAM and 5750 SSC	To support the new extended service management, additional configuration procedures are required on the 5750 SSC and the 5620 SAM: • modelling the 73xx DSLAM in 5620 SAM • creating QoS and schedule policy templates and subscriber management profile templates • creating DSLAM ports and assigning circuits in 5750 SSC • creating subscriber user accounts to use triple play service component packages	See chapter 10 for more information.
MAC learning protection	You can create a list of protected MAC addresses in VPLS and MVPLS. You can also configure the behavior of SAPs and SHGs that receive packets containing protected source and unprotected destination MAC addresses.	See chapter 68 for more information.
Release 4.0 R1 features		
Residential subscriber management	The 5620 SAM supports the management of residential subscribers and residential subscriber hosts on the 7450 ESS-7, 7750 SR-7, and 7750 SR-12, Release 4.0 or later. Residential subscriber management provides functions for the efficient provisioning of access, QoS, and security features on IES and VPLS for static and dynamic subscriber hosts. Residential subscriber management supports a variety of triple play service delivery models in a routed or bridged configuration.	See chapter 64 for more information about residential subscriber management.
Routed CO for IES	The 5620 SAM supports the aggregation of L3 SAPs on group interfaces for IES. This feature allows the direct connection of customer access equipment, such as a DSLAM, to a router such as the 7750 SR, Release 4.0 or later. Routed CO works with residential subscriber management in the 5620 SAM to support a variety of service-delivery models.	See chapter 64 for more information about routed COs. See chapter 70 for information about configuring a routed CO in an IES.
SHCV	The 5620 SAM supports SHCV on VPLS, VPRN, and IES SAPs. SHCV is integrated with residential subscriber management to maintain connection-state information for static and dynamic subscriber hosts using periodic ARP requests.	See chapter 64 for more information about SHCV. See the appropriate service chapters for information about configuring SHCV.
IPv6 support	The 5620 SAM supports control-plane IPv6 addressing for network interfaces on the 7750 SR, Release 4.0 or later. The following entities support IPv6 configuration: • BGP peering • IS-IS adjacencies • multicast routing • static routes • ICMP • routing policies • access ingress and egress policies • CPM filter policies • PPP • Telnet • IES SAPs	See chapter 28 for more information about IPv6 support. See chapter 27 for information about routing policies. See chapter 43 for information about other policy types.
OSPFv3 support	The 5620 SAM supports OSPFv3 configuration on the 7750 SR, Release 4.0 or later, for NE routing instances and IES interfaces.	See chapter 28 for more information about configuring OSPFv3.

(3 of 9)

Feature or function	Description	Reference for more information
MP-BGP multicast extensions	The 5620 SAM supports the configuration of the IPv4 multicast family definition in a BGP instance. You can configure the redistribution of MP-BGP and BGP VPRN routes across autonomous systems. OSPF and IS-IS can be configured to import IGP routes into the multicast and unicast routing tables used by PIM for RPF lookups. You can select the routing tables that PIM uses for RPF lookups. PIM can use either the multicast routing table, multicast unicast routing table, or both to perform standard multicast and unicast RPF lookups.	See chapter 71 for more information about configuring the VPRN service. See chapter 28 for more information about configuring BGP, OSPF, IS-IS, and PIM.
Termination of routed bridge encapsulation ATM SAPs to L3 services	The 5620 SAM supports the termination of ATM SAPs on an L3-based service, such as IES or VPRN. You can configure these services to route encapsulated IPv4 traffic originating on an ATM router.	See chapter 70 for more information about configuring an IES service. See chapter 71 for more information about configuring a VPRN service.
Default dot1q SAPs on Ethernet ports	You can assign default status to a SAP on any Ethernet port for an Epipe VLL or a VPLS. Default SAPs can be used to deliver specialized customer services or perform management tasks.	See chapter 68 for more about creating a default SAP.
SAP and SDP forwarding in ACL IP and ACL MAC filter policies	ACL IP and ACL MAC filter policies can be configured to deliver traffic to a specified SAP or SDP.	See chapter 43 for more information about forwarding to specific SAPs and SDPs in ACL filter policies.
Efficient multicast replication through the use of egress multicast groups	Grouping SAPs on access ports enable a more efficient means for multicasting by reducing loopback on the egress forwarding plane.	See chapter 43 for more information about creating egress multicast groups.
Inter-autonomous system connections in VPRNs	You can configure BGP to connect VRFs of the same VPRN in multiple ASs.	See chapter 28 for more information about configuring BGP for inter-AS communication. See chapter 71 for more information about inter-AS connections in VPRNs.
LAG enhancements	The LAG object in the equipment view of the navigation tree can be expanded to display LAG groups. The LAG group objects can be expanded to view member ports and the active or standby mode of LAG subgroups. There can be up to eight LAG subgroups. Each subgroup can contain up to eight member ports. You can manually add ports to a subgroup or configure the 5620 SAM to group members based on which IOM or MDA the members belong to. You can also configure the criteria for selecting the active LAG subgroup.	See chapter 15 for more information about working with LAG objects. See chapter 17 for more information about how to create and configure LAG subgroups.

(4 of 9)

Feature or function	Description	Reference for more information
Configuration of TPSDA features on the 7750 SR	The following TPSDA features that users could configure only on the 7450 ESS, Release 3.0, can be configured on the 7750 SR, Release 4.0: • multicast VLAN registration (MVR) • residential split horizon groups (RSHGs) • anti-spoofing tools • interface-triggered MAC flush	See chapter 68 for more information about MVR on VPLS, RSHGs, and how to configure anti-spoofing and interface-triggered MAC flush parameters.
RADIUS authentication policies for the 7750 SR	You can distribute and apply RADIUS authentication policies to VPLS and IES services that terminate on the 7750 SR.	See chapter 18 for more information about creating and distributing RADIUS authentication policies to the 7750 SR.
MVPLS STP enhancements	MSTP is supported as an STP mode in an MVPLS.	See chapter 68 for more information about configuring MSTP in an MVPLS.
BPDU translation and L2PT termination	BPDU translation and L2PT termination are supported in a VPLS.	See chapter 68 for more information about configuring BPDU translation and L2PT termination in a VPLS.
ILMI management on ATM interfaces	ILMI links can be created and configured between ATM interfaces on the 7750 SR, Release 4.0 or later.	See chapter 17 for more information about creating and configuring ILMI links.
Ipipe VLL	The 5620 SAM supports the creation of an Ipipe with point-to-point Ethernet, ATM, frame relay, cHDLC, or PPP/IPCP encapsulation, or a combination of these encapsulation types, on a 7450 ESS or 7750 SR, Release 4.0 or later.	See chapter 67 for more information about configuring a VLL service.
VRRP configuration support	VRRP allows you to create a virtual router that provides backup packet forwarding if a router fails in a statically configured network. The virtual router transmits on the same IP address as the failed router through another router on the same LAN. You assign a priority to each backup router when more than one is used. VRRP policies can modify the conditions by which the backup router priority is set.	See chapter 36 for more information about creating and configuring virtual routers. See chapter 43 for more information about creating VRRP priority-control policies for virtual routers.
Test suite support for threshold crossing alarms	You can configure the STM test suites to support the generation of threshold-crossing alarms, to raise alarms when configured rising or falling values are reached based on jitter, latency, or reach issues.	See chapter 75 for more information.
Support for new VCCV, DNS, and ICMP OAM diagnostics	The 5620 SAM supports new OAM diagnostics: • VCCV for in-band VLL connectivity tests • ICMP ping and trace to detect and localize faults in IP networks • DNS ping to perform DNS name resolution	See chapter 35 for more information.
DHCP configuration for services	You can configure DHCP parameters, including Option 82 settings, from the applicable L2 or L3 interface in the context of a service.	See the appropriate service configuration chapter in the *5620 SAM User Guide*.

(5 of 9)

Feature or function	Description	Reference for more information
Generic network element management	The 5620 SAM supports limited management of licensed non-Alcatel-Lucent NEs. You can view reachability status and alarm information and use the 5620 SAM script manager to manage and run scripts on generic NEs. Discovery and polling of generic network elements are the same as for Alcatel-Lucent devices. Discovered generic NEs appear on the topology map and in the navigation tree. You can connect to devices using CLI. On the topology map, you can also create physical links between managed and unmanaged Alcatel-Lucent devices and generic NEs.	See chapter 12 for more information about creating generic NE profiles. See chapter 4 for more information about creating physical links.
New topology group	Newly discovered network elements appear in a topology group called Discovered NEs. You can drag and drop network elements from this topology group to any other group on the topology map or in the navigation tree.	See chapters 17 and 4 for more information.
L2 termination on an IES or VPRN using an SDP spoke	You can configure an IES or VPRN to terminate an Epipe service directly on an SDP spoke on the 7450 ESS and 7750 SR.	See chapter 70 for information about SDP spoke terminations on an IES. See chapter 71 for information about SDP spoke terminations on a VPRN.
ATM OAM loopback	You can configure a 7750 SR to verify the connectivity of an ATM encapsulated port by setting the test transmissions and responses from the endpoints on the virtual circuit. You can enable or disable ATM loopbacks on selected IES and VPRN SAPs on the configured router.	See chapter 17 for information about configuring ATM OAM loopbacks on routers.
SSH2 and host key management	SSH2 is a protocol that provides secure file transfer and CLI communication between the 5620 SAM and managed NEs. SSH2 enables the following: • secure CLI communication for device management and scripting • secure file transfers using SCP for backups, restores, and software upgrades, and for statistics collection SSH2 is supported on the 7450 ESS and 7750 SR, Release 4.0 or later, the 7250 SAS, and SSH2-capable generic NEs. You can manage the acceptance and rejection of SSH2 host keys in SSH2 connections using the 5620 SAM SSH2 known host key manager.	See chapter 13 for more information about configuring SSH2 on managed devices.
Configurable source IP addresses for IP applications	You can configure source IP addresses that override the default addresses in IP applications, such as SSH, Telnet, ICMP ping, and traceroute.	See chapter 71 for more information about configuring source IP addresses for IP applications. See chapter 18 for information about configuring source IPs in RADIUS and TACACS+ authentication.
OSPFv2 as an IGP in a VPRN	You can configure OSPFv2 as the IGP among PE and CE routers in a VPRN to distribute internal routes.	See chapter 71 for more information about configuring VPRN services.

(6 of 9)

Feature or function	Description	Reference for more information
Peer status indicators on VLL service tunnels	You can check the operational status of a peer device on a VLL.	See chapter 67 for more information about peer status indicators.
In-service software upgrade	You can upgrade the software on a multiple-CPM device without service interruption.	See chapter 21 for more information about in-service software upgrades.
Chassis modes and new card types	The 7750 SR supports the following cards: • 2 × 10-Gig MDA IOM 2 • 400g CPM/Switch Fabric 2 • 200g CPM/Switch Fabric 2 Chassis modes A and B can be configured on the 7450 ESS-7, Release 4.0 or later, and on the 7750 SR-7 and 7750 SR-12, Release 3.0 or later. Chassis mode C can be configured on the 7750 SR-7 and 7750 SR-12, Release 4.0 or later. The following features depend on the provisioned card type and the chassis mode that is configured on the device. Chassis mode B • enhanced subscriber management • per-service SDP binding statistics Chassis mode C • IPv6 configuration	See chapters 15 and 17 for more information about chassis modes and card types.
Script manager and result manager	The 5620 SAM script management tool allows you to securely create and manage scripts that are executed against managed devices, including generic NEs. Results of scripts can be compared with the results of other script executions. You can save and view the script results.	See the *5620 SAM Scripts and Templates Developer Guide* for more information about the script manager and result manager.
Web portal redirect	ACL IP and ACL MAC filters contain options for redirecting subscribers to a URL address. The 7750 SR, Release 4.0 or later opens a new connection to the web portal. The subscriber can use the web portal to create or modify a service profile. The web portal updates the ACL policy, directly or through another system such as the 5750 SSC, to remove the redirection policy. Web portal redirect is only supported on the 7750 SR-7 and 7750 SR-12.	See chapter 43 for more information.
Data MDT	An MDT is multicast tunnel through the P-network. MDTs transport customer multicast traffic encapsulated in GRE service tunnels that are part of the same multicast domain. A data MDT is a tunnel for high-bandwidth source traffic through the P-network to interested PE routers. Data MDTs do not broadcast customer multicast traffic to all PE routers in a multicast domain. Data MDTs are only supported for VPRN services.	See chapter 71 for more information.
Release 4.0 R1 enhancements to previous functions		
Connecting a client GUI to different 5620 SAM servers	During client GUI login, you can choose from different 5620 SAM servers. All clients and servers must be of the same release. To log in to a different server, shut down the client, start the client again, then choose another server.	See section 2.4 for more information.

(7 of 9)

Feature or function	Description	Reference for more information
No manual acknowledgement of a previous client GUI login	Users no longer have to manually click the OK button to acknowledge a previous client GUI login session.	—
Setting client inactivity timeouts based on all client sessions or by user group.	The 5620 SAM supports a method of setting an client inactivity check on a per user group basis. This allows administrators to fine-tune inactivity checks for those user groups, such as alarm monitoring, where no timeout check is needed.	See chapter 8 for more information about user group configuration
Support removed for earlier 7450 ESS and 7750 SR devices	You cannot use the 5620 SAM Release 4.0 or later to manage Release 2.0 or earlier devices. The devices must be upgraded to Release 2.1 or later.	—
Start time setup for managed device database backups	The 5620 SAM supports the configuration of scheduled device configuration backups.	See chapter 21 for more information.
User logging enabled by default	The 5620 SAM is configured by default to collect user account logging information.	—
Saving of multiple search filters	The 5620 SAM supports saving more than one search filter, from such configuration forms as the equipment window and the manage equipment forms that allow you to save search filters.	See chapter 2 for more information.
Reordering of IP or MAC ACL filters	The 5620 SAM supports the reordering of IDs for IP or MAC ACL filters, allowing you to reorder the execution of filter policies.	See chapter 43 for more information.
Using password2key utility on a client	The 5620 SAM supports the password2key utility on client installations.	See chapter 13 for the MD5 and SHA authentication, and DES privacy key configuration procedure
Redundancy information for 5620 SAM servers and databases contained on one form	Use the Administration→System Information form from the client GUI main menu to view redundancy information in the 5620 SAM management domain, including IP addresses, host names, status, and database instance names.	See chapter 6 for more information.
SPF and LSA parameters for OSPF configurable from 5620 SAM	The 5620 SAM supports SPF and LSA wait calculations using the OSPF interface properties form.	See chapter 190 for the parameter descriptions.
TACACS+ secret maximum character size increased	The 5620 SAM supports the configuration of a TACACS+ secret parameter of up to 40 characters.	—
Static FEC parameters configurable from 5620 SAM	The 5620 SAM supports static FEC parameter configurations using the LDP interface properties form.	See chapter 182 for the parameter descriptions.
Manage alert, trace, Listener, and audit database files using the 5620 SAM client GUI	The 5620 SAM supports the configuration of policies to control the file size of database alert, trace, Listener, and audit log files to help control disk space.	See chapter 7 for more information.
Database analysis function no longer performed from the client GUI	The database analysis tool is removed from the 5620 SAM client GUI. This function is automatically performed by Oracle.	—
Allow one additional admin account login when all client GUI sessions are in use	The 5620 SAM supports the configuration to allow one additional admin user account login, to ensure that one administrator can access a client GUI to manage client sessions, when all client sessions allowed by the license key are in use.	See chapter 8 for more information
Removal of support of SSH1	SSH1 is no longer supported on the 7450 ESS or 7750 SR, Release 4.0 or later, or the 7250 SAS. The devices use SSH2 by default.	See chapter 13 for more information.

(8 of 9)

Feature or function	Description	Reference for more information
ECMP support for LDP-based LSPs	The 5620 SAM supports ECMP to provide load balancing on LDP-based LSPs. All valid next-hop peers are installed on the forwarding plane of ingress and transit LSRs.	—
Non-stop routing for PIM and IGMP	The 5620 SAM supports non-stop routing on a 7750 SR with two CPMs. If the active CPM fails, the standby CPM takes over and all PIM states or IGMP states (for example, sessions and neighbors) remain intact.	—
Anycast RP for PIM	PIM uses a multicast domain to group receiver hosts on a router, which is called the RP. You can configure multiple active RPs for each group in a PIM-SM domain. Multiple RPs for each group provides the following benefits: • improved traffic flow • optimized forwarding of multicast packets • scalable register decapsulation • efficient convergence after the failure of the active RP	See chapter 28 for more information about configuring anycast RP for PIM.
Policy override	A policy override allows you to modify some or all settings associated with the following policies: • access ingress or access egress policy on an L2 or L3 access interface or SLA profile • scheduler policy on an L2 or L3 access interface or subscriber profile	See chapter 43 for more information.
Multipoint shared queues	Multipoint shared queues optimize the number of multipoint queues created for the following service components and subscriber profiles: • ingress VPLS, IES, or VPRN SAPs • ingress subscriber SLA profiles Shared queues minimize the number of ingress queues and benefit services with a large number of SAPs.	See chapter 43 for more information.
SNMP trap loss controls	The 5620 SAM supports the configuration of trap loss parameters to control how the resynchronization of network elements is handled when network events cause SNMP trap bursts.	See chapter 149 for the parameter descriptions.
Client GUI map management enhancements	Client GUI maps support the following functions: • device auto-layout • enhanced zooming	See chapter 4 for more information about map management.
Increase in the permitted size of a login security statement	The 5620 SAM supports a login security statement of up to 2000 characters.	See chapter 8 for more information about configuring a login security statement.
Configuring alarm forwarding to other network management systems	The 5620 SAM supports configuration of alarm forwarding to other network management systems using the nms-server.xml file.	See chapter 10 for more information.

(9 of 9)

Table 3-7 lists key changes and additions to the 5620 SAM documentation suite.

Table 3-7 Changes and additions to 5620 SAM Release 4.0 documentation

Change or addition	Description	Reference for more information
Release 4.0 R1		
Inventory generation using the 5620 SAM listing, properties, and management configuration forms	A new chapter in the *5620 SAM User Guide* describes how to use client GUI tools to generate inventories of information about 5620 SAM networks, including generating inventories based on individual managed devices, or for a network of managed devices. The inventory information includes: • generating CLEI and CLLI codes • card, shelf, and other physical objects part numbers and revision numbers	See chapter 19 for more information.
Reestablishing redundancy following a database failover	The 5620 SAM supports the reinstantiation of a previous primary database following a database failover, using the client GUI.	See chapter 6 for more information
Run a script to view the database version, status, or proxy status	The oracleproxy script is used to view the status of a 5620 SAM database, the database version, or current information about the Oracle proxy.	See the database troubleshooting chapter of the *5620 SAM Troubleshooting Guide*.
Additional VLAN configuration information	View more configuration information for VLANs on CLE devices, including the following: • description of management and standard VLANs • VLAN connections across a VPLS using service connectors • tagged and untagged traffic behavior, and the effect of VLAN port and ID configurations • password and user name settings to access CLE devices	See chapter 65 for more information about VLAN service management. See Procedure 13-4 for more information about mediation policies, user names, and passwords. See section 15.17 for more information about tagged and untagged traffic.
Description of installing a client delegate on a Solaris workstation	The 5620 SAM supports the installation of a client delegate. A client delegate allows multiple installations of client GUIs on one workstation. Users on other workstations, using X11 or native × software, can display clients. For each required client installation, install the client software in a separate directory.	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.
Replacement of SAS with STM	The acronym SAS (service assurance system) is replaced with STM (service test manager) to avoid confusion with the 7250 SAS device.	—
Explanation of Boolean filters in search and find forms	New information is provided about the Boolean EQUALS, NOT EQUAL, CONTAINS, and WILDCARD filters, which are used to return specific lists of network objects.	See chapter 2 for more information.
Simplified description of generating authentication and privacy keys for SNMPv3 users	The procedure to configure MD5 and SHA authentication and DES privacy keys is simpler to use, and is all contained in a single procedure for SNMPv3 user management.	See Procedure 13-1 in chapter 13 for more information.
Additions to the glossary	The glossaries that are contained in all 5620 SAM user documentation have been updated with a more comprehensive list of acronym expansions and definitions.	—

3.7 5620 SAM Release 3.0 features

Table 3-8 lists the features and functions added in 5620 SAM Release 3.0.

Table 3-8 5620 SAM Release 3.0 features

Feature or function	Description	Reference for more information
Release 3.0 R5 features		
Service test manager (STM)	The 5620 SAM STM allows the grouping of OAM tests into test suites for network monitoring and troubleshooting. Existing OAM tests can populate a test suite, or the 5620 SAM can generate tests for a test suite according to policy criteria. Test suites can be run as scheduled tasks to provide continual network and service performance feedback.	See chapter 75 for more information about STM.
Scheduling support	You can use the 5620 SAM to create schedules and scheduled tasks. Schedules can be used to set up and regularly run tasks that support scheduling.	See chapter 74 for more information about creating schedules and scheduling tasks.
7710 SR support	The 5620 SAM supports network and element management of 7710 SR devices, Release 3.0 or later. The 7710 SR is intended to be installed in telecommunications central office and CPE restricted access locations that provide weather protection and a temperature-controlled environment. The 7710 SR features and functions are similar to the 7750 SR, but the 7710 SR has more granular interfaces, a lower cost, and a 10 Gb/s maximum system throughput.	See chapter 15 for general information about managed device support. See the 5620 SAM documentation suite for descriptions of 5620 SAM management of devices.
Multicast OAM diagnostics	The multicast OAM diagnostics help identify problems in the transmission of IP multicast service traffic. The following multicast OAM diagnostics are supported. • Multicast FIB ping (mfib ping) identifies the SAPs that egress an IP multicast stream within a VPLS. The diagnostic can also be used to display the SAPs that are operationally up in the VPLS. • Multicast router information (mrinfo) identifies multicast information for the target router. The information includes details that are related to adjacent routers, supported protocols, traffic metrics, and time-to-live thresholds. Administrators can use this information to identify bidirectional adjacency relationships. • Multicast trace (mtrace) identifies the hop-by-hop route used by the multicast traffic to reach the target router. The diagnostic gathers the hop address, routing error conditions, and packet statistics at each hop. By default, the 5620 SAM attempts to trace the receiver to sender route for the traffic.	See chapter 35 for overview and configuration information.
WAN-PHY support	The 5620 SAM supports configuration of a 1-port 10-Gbyte Ethernet interface as a WAN-PHY interface, which encapsulates Ethernet frames over SONET.	See chapter 17 for more information about configuring Ethernet interfaces.
Size constraint policies	The 5620 SAM supports the creation of size constraint policies to regulate the number of historical records that accumulate in the 5620 SAM database.	See chapter 43 for more information about configuring size constraint policies.
Release 3.0 R3 features		
7250 Service Access Switch support	The 5620 SAM supports element and network management of the 7250 SAS in the provider network. The 7250 SAS provides Ethernet aggregation and TDM backhauling with circuit emulation across IP/MPLS networks, and distributes L2 VPN, Internet, and broadcast services from VPLS on 7450 ESSs across VLANs to subscribers.	See chapter 15 for equipment management information. See chapter 65 for VLAN information.

(1 of 7)

Feature or function	Description	Reference for more information
Performance statistics collection enhancements	A default statistics collection policy and configurable default polling interval for each statistics counter determine the frequency of performance statistics collection from network devices.	See the *5620 SAM Statistics Management Guide* for more information about the configuration of performance statistics. See chapter 13 for information about configuring NE mediation.
Physical topology map	Manage the physical layout and connectivity between the devices managed by the 5620 SAM using topology views, topology groups, and physical links.	See chapter 4 for information about using the physical topology map.
Composite service topology map	View composite services that are grouped according to their service tier structure, devices, and access interfaces.	See chapter 4 for information about using the composite service topology map.
Topology groups	The 5620 SAM supports the creation and management of topology groups, which are used to organize the network view.	See chapters 17 and 4 for information about creating and managing topology groups.
Physical links	The 5620 SAM supports the configuration and management of physical links. A physical link can be between two managed devices, or between a managed device and a non-managed device. The physical link properties form contains a new GUI button: Paste from Clipboard.	See chapters 17 and 4 for information about configuring and managing physical links. See chapter 2 for information about the Paste from Clipboard button.
Topology map enhancements	Topology map enhancements provide more flexibility including: • common map window • navigation tree • map view selector • map toggle button • search capability to find specific map objects • bookmarks • breadcrumbs	See chapter 4 for information about topology maps.
Equipment window enhancement	If a managed device is selected in the navigation tree when the equipment window is open, the equipment window form opens and displays the selected managed device information.	See chapter 16 for information about using the equipment window.
Client GUI enhancements	Enhancements to the client GUI include: • The server computer ID appears in the 5620 SAM main menu titlebar. • Up to seven navigation tree windows, with different roots, can be open at the same time.	See chapter 2 for information about the client GUI. See chapter 17 for information about opening multiple navigation tree windows.
Formats for saving listed information	You can save listed information in the following output formats: • HTML • comma-delimited CSV	See chapter 2 for more information about saving listed information.

(2 of 7)

Feature or function	Description	Reference for more information
CPE ping OAM tests using the service assurance tool	You can run CPE ping tests to test connections between SAPs and CPE.	See chapter 35 for more information about CPE ping OAM tests.
Q in Q encapsulation for LAGs	You can configure LAG endpoints to use Q in Q encapsulation for the 7450 ESS, Release 3.0 R3 or later, and the 7750 SR, Release 3.0 R3 or later.	See chapter 17 for more information about creating LAGs.
Database security enhancements	The 5620 SAM database security enhancements include: • providing secure communication between a 5620 SAM server and database • changing Oracle user passwords using a new password change tool • new Oracle default port value	See the *5620 SAM System Architecture Guide* for high-level information about secure server-database communication. See chapter 5 for information about configuring secure server-database communication. See the *5620 SAM Troubleshooting Guide* for information about changing an Oracle user password.
Release 3.0 R1 features		
Login security	When you log in to the 5620 SAM GUI from a PC or workstation, the 5620 SAM displays a dialog box with the date and time of the previous login using the same user account.	See chapter 2 for the basic GUI operation procedures.
Service creation process changes	The step-by-step configuration forms for services in the 5620 SAM have been replaced by simpler tabbed configuration forms that incorporate a navigation tree for service object management.	See the appropriate service chapter.
Composite service management	Through the 5620 SAM, services of the same or different types can be linked together by connectors to form a sophisticated service delivery mechanism.	See chapter 72 for information about configuring composite services.
VLL enhancements	The 5620 SAM supports the creation of VLL services with end-to-end Ethernet, ATM, or Frame Relay encapsulation, or a combination of these encapsulation types, is supported.	See chapter 67 for information about configuring a VLL service.
802.1X support for EAP authentication	Enable and configure 802.1X authentication policies and port configurations to validate subscribers on the 7750 SR. The 802.1X object no longer exists in the navigation tree. The device Properties form indicates whether 802.1X is enabled or disabled.	See chapter 17 for information about enabling 802.1X and configuring 802.1X for Ethernet ports. See chapter 43 for information about 802.1X policy management.
Spoke redundancy added to the 7750 SR	The 5620 SAM supports HVPLS spoke redundancy using MVPLS on the 7450 ESS and the 7750 SR.	See chapter 68 for information about configuring spoke redundancy.

(3 of 7)

Feature or function	Description	Reference for more information
Residential split horizon groups	RSHGs are SHGs that are configured with the Residential parameter. SAPs that are associated with an RSHG are lightweight SAPs. RSHGs are supported only on the 7450 ESS.	See chapter 68 for information about configuring RSHGs. See chapter 60 for information about lightweight SAPs.
Alarm management enhancements	Improvements and additions to 5620 SAM alarm management functions, including: • configuration form for setting alarm type policies altered to allow easier listing and navigation • new parameters to tag sets of alarms with the same name, for ease of grouping and listing • updates to the navigation tree to display alarm status and aggregated alarm status of all objects in the network tree • addition of alarm and connectivity status information to device icons on maps	See chapter 34 for more information about changes to alarm management.
Graceful Restart	For BGP, OSPF, and IS-IS, the router can function as a helper and assist other capable routers with a graceful restart operation.	See chapter 28 for more information about configuring GR Helper mode.
BGP Advertise for Inactive Routes	Enable and configure BGP advertise for inactive routes. This parameter advertises to peers as inactive the routes that are not selected as the active route in the routing table.	See chapter 28 for more information about configuring BGP advertise for inactive routes.
BGP/LDP TTL Security Enhancement	BGP and LDP sessions can be protected by providing an expected TTL to peers.	See chapter 28 for more information about BGP and LDP peer configuration.
Support for new hardware	The 5620 SAM supports the use of VSM-CCA daughter cards on the 7750 SR and 7450 ESS.	See the appropriate device documentation for more information. See chapter 15 for hardware support information.
Cross-connect aggregation groups use as an interface.	The 5620 SAM supports the creation and use of cross-connect aggregation groups for service configurations that may require paths that loop back onto themselves.	See chapter 17 for more information about configuring CCAG.
IES spoke into VPLS	The 5620 SAM supports the connection of an IES and a VPLS or VLL through an internal cross-connect on the 7450 ESS, Release 3.0, and the 7750 SR, Release 3.0.	See chapter 72 for information about joining services to form composite services.
Restructure of client GUI main menu and submenu layout and names	To simplify operation of the 5620 SAM client GUI in customer networks, the menu and submenu structure is reorganized and renamed. The changes include the following: • creation of new Administration and Tools main menu options to group together functions commonly performed by system administrators • grouping of create and manage tasks • organization of all maps and windows under the Application menu	All procedures in the 5620 SAM documentation suite are updated to reflect the new menu structure.

(4 of 7)

Feature or function	Description	Reference for more information
Client GUI improvements	GUI improvements provide more flexibility including: • a drop-down menu in the navigation tree to choose the different navigation tree views, including a ring group view • the ability to open multiple navigation trees at the same time • a contextual menu option in the navigation tree to open another navigation tree with the selected object as the root • a contextual menu option in the navigation tree to redefine a selected object as the root of the tree hierarchy • a button in the navigation tree to restore the default root of the tree • a Clipboard button on forms and in the navigation tree to copy the properties of selected objects to a clipboard from which you can copy and paste the properties, usually the object name and ID, to an external application • a toolbar in the service topology map to allow the user to manipulate the map view • Layer 3 interface port assignment and static route type displayed in network navigation tree • device version displayed as part of the device label in topology maps	See chapter 2 for information about choosing navigation tree views and copying object properties to the clipboard. See chapter 17 for information about grouping devices in a ring group and redefining the navigation tree root. See chapter 4 for information about the map toolbar.
IGMP snooping	IGMP snooping can be enabled for VPLS on the 7750 SR, Release 3.0 or later.	See chapter 68 for information about configuring IGMP snooping on a VPLS.
Interface triggered MAC flush	The 5620 SAM provides a LDP-based mechanism for recovering physical link failures in connections to VPLS on the 7450 ESS.	See chapter 68 for support and configuration information.
IGMP Snooping: Show all routers with “show querier” command	The 5620 SAM can display all current and previous queriers that are receiving IGMP membership reports.	See chapter 68 for more information.
PIM: hello interval for neighbor down for the 7750 SR	The 5620 SAM can change the neighbor down interval from the standard 3.5 multiplier.	See chapter 28 for configuration information.
PIM support for VPRN service	PIM can be enabled and configured to operate within a VPRN service.	See chapter 71 for more information.
OAM diagnostic test creation and management	Changes to the management and configuration of OAM diagnostics, to ease SLA management and provide easier access to tools: • creation of a test manager, to search for, list, create, edit, and run diagnostics • automatic enabling of all OAM diagnostics • grouping of tests based on network application layer	See chapter 35 for more information about the types, creation, and running of OAM diagnostics.

(5 of 7)

Feature or function	Description	Reference for more information
Service mirroring enhancements	The 5620 SAM supports service mirroring, introduced on 7450 ESS Release 3.0, and service mirroring enhancements, including: • the automatic creation of service tunnels when GRE is used as the transport type, and no other service tunnels exist between the source and destination sites • CCAGs as mirror sources • the default subscriber as the only subscriber to the service • a consistent encapsulation type among sites associated with a mirror	See chapter 30 for information about service tunnels. See chapter 69 for information about service mirroring.
RADIUS authentication of DHCP sessions	The 5620 SAM supports configuration and application of subscriber authentication policies for RADIUS authentication of DHCP sessions on the 7450 ESS, Release 3.0 or later, for VPLS and IES SAPs.	See chapter 18 for policy configuration information. See the following chapters for DHCP configuration information: • chapter 68 for VPLS • chapter 70 for IES
DHCP relay enhancements	DHCP relay can be enabled on the 7750 SR, Release 3.0 or later, for VPLS. The 5620 SAM supports the following DHCP relay enhancements on the 7450 ESS, Release 3.0 or later, and the 7750 SR, Release 3.0 or later: • specifying the maximum number of lease states allowed on IES, VPLS, and VPRN SAPs • automatic enabling of DHCP snooping on IES and VPRN SAPs when the number of lease states is specified • specifying the Relay Information Option, defined in RFC 3046, for IES, VPLS, and VPRN SAPs • configuring DHCP relay when using service-based templates	See the *5620 SAM Scripts and Templates Developer Guide* for information about service templates. See the following chapters for DHCP configuration information: • chapter 27 for Layer 3 interfaces • chapter 68 for VPLS • chapter 70 for IES • chapter 71 for VPRNs
Anti-spoof filter management	The 5620 SAM supports anti-spoof filter management on the 7450 ESS, Release 3.0 or later, and the 7750 SR, Release 3.0 or later, for IES, VPLS, and VPRN SAPs. Use anti-spoof filter management to configure: • anti-spoof filters on service configuration forms and when using service-based templates • ARP reply agents • population of static and dynamic hosts in the ARP cache • static subscriber hosts • MAC pinning	See the *5620 SAM Scripts and Templates Developer Guide* for information about service templates. See the following chapters for anti-spoof filter configuration information: • chapter 68 for VPLS • chapter 70 for IES • chapter 71 for VPRNs
Fault management using APS	The 5620 SAM supports 1+1 APS configurations on the 7750 SR, Release 3.0 or later. Use APS to protect SONET/SDH lines from linear bidirectional failures.	See chapter 37 for information about APS.
MVR on VPLS	The 5620 SAM supports MVR on VPLS for the 7450 ESS, Release 3.0 or later. At the port level, MVR allows a VPLS subscriber to subscribe or unsubscribe to a multicast stream on one or more network-wide multicast VPLS instances without requiring that the stream be part of the subscriber VPLS.	See chapters 27, 43, and 68 for more information about MVR on VPLS.

(6 of 7)

Feature or function	Description	Reference for more information
License key size increased	The 5620 SAM license key size has increased.	See chapter 5 for more information about modifying an existing license key. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about entering the license key during installation.

(7 of 7)

Table 3-9 lists key changes and additions to the 5620 SAM documentation suite.

Table 3-9 Changes and additions to 5620 SAM documentation

Document	Description	Reference for more information
Release 3.0 R3		
All user documentation is installed during client installation, and the documentation can be launched from the client GUI	When you install the 5620 SAM client software, the user documentation PDFs, XML reference, and XML schemas are installed on the PC or workstation. You can find the User_Documentation directory in the *Installation_directory*/nms/distribution folder or directory.	See chapter 2 for information about launching the documentation from the client GUI.
Statistics description information added to the *5620 SAM Statistics Management Guide*	For each supported statistics counter documented, the *5620 SAM Statistics Management Guide* provides a description of the counter, based on the MIB description of the counter.	See the *5620 SAM Statistics Management Guide*.
Alarm-clearing information added to the *5620 SAM Troubleshooting Guide*	For each alarm described, the *5620 SAM Troubleshooting Guide* specifies whether the alarm is self-clearing or must be manually cleared.	See the *5620 SAM Troubleshooting Guide*.
Release 3.0 R1		
Alarm management overview in the *5620 SAM User Guide*	Overview and example of the relationship between alarm status, alarm aggregation, and the differences between affecting, propagated, and related alarms.	See section 34.1 for illustrations and descriptions.
Restructure of the *5620 SAM Parameter Guide*	The *5620 SAM Parameter Guide* is restructured to match the new menu and submenu structure developed for the client GUI	See the *5620 SAM Parameter Guide*.
Service configuration procedures changes	The step-by-step service creation forms have been replaced by simpler tabbed configuration forms. All service procedures in the *5620 SAM User Guide* have been rewritten.	See the appropriate service chapter.
Reorganization of the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*	The *5620 SAM | 5650 CPAM Installation and Upgrade Guide* is: • organized by Solaris and Windows operating systems • describes end-to-end workflows for setting up standalone and redundant systems, and upgrades • uses the installation screens to illustrate the sequence of installation activities	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

(1 of 2)

Document	Description	Reference for more information
HQoS samples and description of the triple play service delivery architecture components	The *5620 SAM User Guide* describes: • sample HQoS configuration that uses tiered schedulers and queues incoming packets for processing based on the IP precedence marking of the packets • the major components of the triple play service delivery architecture, and the role of 5620 SAM is setting QoS and filters, and for creating multicast BTV streams	See chapter 60 for information about sample HQoS configuration and TPSDA.
Creation of example-based statistics documentation	The *5620 SAM Statistics Management Guide* describes: • performance, accounting, and on-demand statistics • sample real-world network configuration and the associated procedures required to collect statistics • mapping of statistics counter name to the associated MIB value	See the *5620 SAM Statistics Management Guide*.

(2 of 2)

3.8 5620 SAM Release 2.1 features

Table 3-10 lists the features and functions added in 5620 SAM Release 2.1.

Table 3-10 5620 SAM Release 2.1 features

Feature or function	Description	Reference for more information
Release 2.1 R2 or later features		
Service mirrors	Service mirroring is used to forward packets or portions of packets from a customer service to a mirrored destination port. Use service mirroring to: • troubleshoot service delivery issues • allow service providers to meet regulatory obligations regarding call records • reduce the complexity of an analyzer overlay network	See chapter 69 for more information about using service mirrors.
Database and server redundancy	Redundancy provides network visibility in case of the hardware or software failure of one or more 5620 SAM components, for example, a server. When the active component fails, the standby component is configured to automatically take control. Alternatively, perform manual failovers to test redundancy or prepare for network upgrades.	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information about installing redundancy components. See chapter 6 for more information about redundancy configuration and management.

(1 of 6)

Feature or function	Description	Reference for more information
Security management	Security enhancements to the 5620 SAM allow system administrators to manage client GUI user security more effectively. Use security management to: • enable user action logging • view or close active client GUI sessions • set scope of command for users and user groups • specify the maximum number of admin sessions • specify the expiry period for user accounts and passwords	See chapter 8 for more information about security configuration on the client GUI. See the *5620 SAM Troubleshooting Guide* for more information about user logs.
MAC move	The 5620 SAM supports MAC move on the 7750 SR. The MAC move feature can be configured at VPLS creation for SAPs and spoke SDPs.	See chapter 68 for information about MAC move configuration.
Service tunnel auto-creation	The 5620 SAM automatically creates service tunnels for VPLS and VLL services when GRE is used as the transport type, and no other service tunnels exist between the source and destination devices.	See chapter 30 for more information about service tunnels. See chapter 67 for more information about VLLs. See chapter 68 for more information about VPLS.
LSP cross-connect topology map	You can view a map that shows the LSP cross-connect topology.	See chapter 4 for information about using the LSP cross-connect topology map.
LSP path topology map enhancements	You can view the actual path and CSPF path topologies from the LSP path topology map.	See chapter 4 for information about using the LSP path topology map.
Release 2.1 R1 features		
Routing protocol enhancements	Multiple improvements have been made to routing policing configuration using the 5620 SAM, including: • proxy ARP • 31-bit mask IP address support • BGP fast fail over, BGP community sending disabling, AS override, outbound route filtering, and default originate • policy filtering for LDP label bindings and LDP tunnel damping • IS-IS IPv4 route summaries	See the appropriate routing protocol configuration information in chapter 28.
Interworking support with non-5620 SAM network management applications	The following network management software applications can be installed and configured to interwork with the 5620 SAM: • 5620 NM • 1354 BM You can use the interworking functions to: • navigate between network management GUIs • provide and view alarm feeds from the 5620 SAM to other network management applications	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information about installing non-5620 SAM network management applications. See chapter 10 for information about performing network management interworking functions.

(2 of 6)

Feature or function	Description	Reference for more information
License key information	The following information and functions are added to the license key infrastructure: • licensed quantity of MDA consumed and remaining • alarms raised when thresholds are exceeded • export license information to a text file • update license key dynamically to support increased licensed quantities of daughter cards (MDAs) without restarting the server	See chapter 2 for more information about viewing and exporting license information.
Client GUI improvements	GUI improvements provide a more flexible user interface: • provides a standard Java look and feel • provides the navigation tree and alarm windows as floating windows that can be resized, hidden, and have preferences stored, and that can be accessed from menus, tool bar icons, the taskbar, and shortcut keys • provides access to object properties by double-clicking on a leaf object in the navigation tree • provides title bars that display the object type, name, and ID in policy, subscriber, and service forms. When a form is minimized, a tooltip identifies it using the title-bar name. Additionally, titles of all opened forms are listed and can be selected from a Window menu. • provides Alcatel-Lucent-standard alarm colors • provides a configurable login message for client GUI users	See chapter 2 for more information about GUI basics.
Modularization of client GUI components	The functions of the 5620 SAM have been split among four components, which can be enabled by the license key: • 5620 SAM-E for device mediation, equipment management, security, CLI access to managed devices, backup and restore, equipment navigation, alarm policy management, real-time equipment statistics, and inventory and reporting • 5620 SAM-P for service provisioning, templates, network tunnel and path management, subscriber management, and policy management • 5620 SAM-A for service assurance functions, fault correlation using alarms, OAM tools, topology views, statistics policies and historical statistical data, and accounting policies and accounting data • 5620 SAM-O for the XML open interface	See chapter 2 for more information about the effects on not enabling all software components.
PIM management support	PIM, used in conjunction with IGMP, defines an IP routing protocol that delivers multicast traffic to receivers. 5620 SAM provides: • PIM configuration at the routing instance level • PIM configuration at the interface level • PIM availability for IES	See the PIM overview, configuration, and procedures in chapter 28. For information about how to apply PIM to an IES, see the PIM-specific procedures in chapter 70.
IGMP management support	IPv4 hosts and routers use IGMP to report their group memberships to neighboring multicast routers. 5620 SAM provides: • IGMP configuration at the routing instance level • IGMP configuration at the interface level • IGMP availability for IES	See the IGMP overview, configuration, and procedures in chapter 28. For information about how to apply IGMP to an IES, see the IGMP-specific procedures in chapter 70.

(3 of 6)

Feature or function	Description	Reference for more information
DHCP relay and snooping	DHCP relay interconnects DHCP clients with a DHCP server connected to another LAN segment or network. DHCP snooping allows 5620 SAM to build ACL filters. These features are supported in version 2.1 of the 7750 SR and in version 2.0 of the 7450 ESS.	See chapter 27 for DHCP configuration information for Layer 3 interfaces. See chapter 70 for the DHCP component of configuring an IES service. See chapter 71 for the DHCP component of configuring a VPRN service. See chapter 68 for the DHCP component of configuring VPLS.
Service templates	The 5620 SAM supports the configuration of VLL, VPLS, IES, and VPRN services using service-based templates. The templates allow a user with service management privileges to define common characteristics for a service.	See the *5620 SAM Scripts and Templates Developer Guide* for information about creating service templates. See the following chapters for information about using a pre-created template to create a service: • chapter 67 for VLL • chapter 68 for VPLS • chapter 70 for IES • chapter 71 for VPRN
Telco device, VLAN, and services	The 5620 SAM supports element and network management of Telco devices in the provider network. Telco Ethernet devices provide Ethernet and service-aware Ethernet aggregation across IP/MPLS networks. Telco devices are used in ring groups to distribute L2 VPN, Internet, and broadcast services from VPLS or VLL services on 7450 ESSs across VLANs to subscribers.	See chapter 15 for general support information. See chapter 43 for Telco device policy management information See chapter 65 for VLAN information.
Support for 7750 SR high availability	High availability on the router is used to ensure active and standby redundancy in the managed network elements. You can view the status of router redundancy and the reason for a fail over from the active to the standby from the properties form of the router.	—

(4 of 6)

Feature or function	Description	Reference for more information
Support for ATM traffic routing	The 5620 SAM supports: • the creation of SONET/SDH channels with ATM encapsulation • ATM interface management to create PVCs within IES or VPRN services • ATM QoS policy creation and management • ATM OAM	See chapter 17 for information about how to create SONET/SDH channels. See chapter 70 for IES service creation information and chapter 71 for VPRN service creation information. See chapter 43 for information about ATM QoS policy creation and management. See chapter 35 for information about ATM OAM.
802.1X support for EAP authentication	Enable and configure 802.1X authentication policies and port configurations to validate subscribers on the 7450 ESS.	See chapter 15 for general support information. See chapter 17 for information about configuring 802.1X parameters for Ethernet ports. See chapter 43 for information about 802.1X policy management.
Forwarding subclass support	Associates one or more forwarding subclasses with each forwarding class. This provides a greater degree of SAP ingress packet classification.	See chapter 43 for support and configuration information.
Shared network queues	Supports shared queues for SAPs using a default shared queue policy	See chapter 43 for more information.
Policy management enhancements	Policy management improvements include: • doubling the number of managed policies to 131 072 • controlling local and global policy interaction • limiting local policy influence to initial discovery • synchronizing local and global policies • auditing policies	See chapter 43 for more information.
IP interface trust override	Provides the ability to explicitly override default trust states for IES, VPRN, and network IP interfaces	See chapter 70 for IES configuration information. See chapter 71 for VPRN configuration information. See chapter 27 for information about configuring a Layer 3 interface.
IGMP snooping	IGMP snooping can be enabled for VPLS on the 7450 ESS.	See chapter 68 for information about configuring IGMP snooping on a VPLS.

(5 of 6)

Feature or function	Description	Reference for more information
Spoke redundancy	The 5620 SAM supports HVPLS spoke redundancy using MVPLS on the 7450 ESS.	See chapter 68 for information about configuring spoke redundancy.
Split horizon groups	Split horizon groups control traffic flowing through SAPs or spoke SDPs for a VPLS.	See chapter 68 for information about configuring split horizon groups.
RSTP support	Supports RSTP (802.1D-2004) for VPLS instances on the 7750 SR and the 7450 ESS and remains compatible with older STP variants	See chapter 68 for RSTP configuration during VPLS creation.
Support for new hardware	Additional card support for the 7450 ESS includes: • 20 × 10/100/1000 Ethernet Tx • 20 × 10/100/1000 Ethernet SFP Additional card support for the 7750 SR includes: • 4 × OC3 Deep Channel • 16 × ATM OC3 SFP • 4 × DS3/E3 Deep Channel • 4 × ATM OC12/OC3 SFP • 1 × 10-Gig Ethernet XFP Card support for the Telco devices includes: • 24 × Fast Ethernet 10/100 TX • 24 × Fast Ethernet 10/100 FX • 48 × Fast Ethernet 10/100 TX • 4 × Gig Ethernet (2 TX, 2 FX) • 24 × Gig Ethernet (20 TX, 4 Dual TX/FX) • 24 × Gig Ethernet (20 FX, 4 Dual TX/FX)	See the appropriate hardware documentation and port information, such as line length and hardware specifications. See chapter 15 for information about hardware modelling support.
IP SAP ingress dot1P Q in Q classification	Allows the specification of which dot1P bits in a Q in Q encapsulated packet are used to evaluate dot1P QoS classification. Support for this feature is dependent on the software release of the NE. See the 7750 SR and 7450 ESS documentation for more information.	See chapters 67, 68, 70, and 71 for VLL, VPLS, IES, and VPRN QoS configuration information.
Single fiber router connection	Supports the enabling of packet gathering and redirection from a single fiber on a SONET interface for redistribution to other interfaces. Support for this feature is dependent on the software release of the 7750 SR. See the 7750 SR documentation for more information.	See chapter 17 for configuration information.
Upgrading to a new 5620 SAM release	Multiple upgrade scenarios are possible. Use the ClientServerInstaller and DBconfig installers to perform upgrades. Contact your Alcatel-Lucent support representative for more information.	See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information about upgrades.

(6 of 6)

Table 3-11 lists key changes and additions to the 5620 SAM documentation suite in Release 2.1.

Table 3-11 Changes and additions to 5620 SAM documentation in Release 2.1

Document	Description	Reference for more information
Release 2.1 R1		
5620 SAM Parameter Guide parameter descriptions	Allows planners, system administrators, and operators to find and view information for parameters that are configurable from the 5620 SAM client GUI, including: • default value • range • description • dependencies on other parameter values • equivalent XML property name	See chapters 1 to 193
Parameter links between the *5620 SAM User Guide* and the *5620 SAM Parameter Guide*	You can click on a parameter name in the *5620 SAM User Guide* to launch and view the description of the parameter in the *5620 SAM Parameter Guide*.	—
Addition of the *5620 SAM Planning Guide*	Allows planners and administrators to plan deployments of the 5620 SAM database, server, and clients, including: • supported operating system configurations • hardware platform requirements • redundancy architecture • network bandwidth requirements • scaling guidelines • PC and workstation configurations, including disk layout recommendations	See the Support Documentation Service SDS site on http://www.alcatel.com
Addition of the *5620 SAM Maintenance Guide*	Allows planners and NOC staff responsible for developing maintenance procedures to plan maintenance activities, including: • guidelines for developing base measures • daily, weekly, monthly, and as required procedure baselines	See the Support Documentation Service SDS site on http://www.alcatel.com See the User_Documentation directory on the product DVD-ROM
Modification of the *5620 SAM Troubleshooting Guide* to include network troubleshooting	Allows planners and NOC staff responsible for troubleshooting activities to understand the use of 5620 SAM in planning and managing network and service troubleshooting, including: • theory of network troubleshooting • troubleshooting using alarms from the 5620 SAM client GUI • troubleshooting services using OAM tools from the 5620 SAM client GUI	
Release 2.1 R2 or later		
Addition of multicast sample configuration to the *5620 SAM User Guide*	Allows planners to see a sample configuration of multicast for broadcast TV, including: • required PIM and IGMP configurations • service setup and configuration	See chapter 28 for more information.
Addition to 5620 SAM user and user group security management	Allows 5620 SAM system administrators to understand in more detail the user privileges granted by each user group type, and an example configuration of users.	See chapter 8 for more information.

3.9 5620 SAM Release 2.0 features

Table 3-12 lists the features and functions added in 5620 SAM Release 2.0.

Table 3-12 5620 SAM Release 2.0 features

Feature or function	Description	Reference for more information
VPRN service	The 5620 SAM supports the creation of VPRN services using the 7750 SR as a PE and provider core (P) router. VPRNs, which are also called IP VPNs or BGP/MPLS VPNs, are defined in RFC 2547bis, which describes a method of forwarding data and distributing routing information across an IP/MPLS provider core network. A VPRN service consists of CE devices connected to PE routers. PE routers connected to P routers transport data across the IP/MPLS provider core network in service tunnels. The 5620 SAM supports the creation of GRE or MPLS LSP service tunnels.	See chapter 71 for overview and configuration information.
Router security management, including user domain control and using TACACS+ or RADIUS authentication	Security support for accessing the managed routers, such as the 7750 SR, in the following ways: • Create and manage users, management access filters, profiles, and passwords for access to the managed routers. • Configure RADIUS or TACACS+ authentication to allow controlled access to the managed routers using 5620 SAM user accounts. RADIUS and TACACS+ are access server AAA protocols. Each protocol provides a standardized method of exchanging information between a RADIUS or TACACS+ client, located on the managed router, and a RADIUS or TACACS+ server, located externally from the managed router and the 5620 SAM.	See chapter 18 for overview and configuration information.
LSP, VPRN, and MAC OAM diagnostics	The LSP ping and traceroute diagnostics provide a mechanism to detect data plane failures in MPLS LSPs. The diagnostics are modeled after the ICMP echo request/reply used to detect and isolate faults in IP networks. The following MAC OAM diagnostics are supported. • MAC ping determines whether an egress SAP that binds a specific MAC address within a VPLS exists. • MAC trace OAM displays the hop-by-hop route of MAC addresses used to reach the target MAC address at the far end. • MAC populate OAM populates a service FIB with an OAM-tagged MAC entry.	See chapter 35 for overview and configuration information.
Support for new hardware	7450 ESS chassis configurations that are managed include the following shelf types: • 1-slot with 1 I/O slot that supports 2 daughter cards • 7-slots with 6 slots that support 12 daughter cards. Additional card and port support, including: • 12-port DS3 to the T1/E1 and DS0 level and E3 to the E3 level on the 7750 SR • 1-port OC12/STM4 to the DS0 level on the 7750 SR • Gigabit Ethernet with 10 and 20 ports on the 7450 ESS • 10 × Gigabit Ethernet with 1 port LAN/WAN physical card on the 7450 ESS	See the appropriate hardware documentation for card and port information, such as line length and hardware specifications. See chapter 15 for information about hardware modelling support by the 5620 SAM.

(1 of 4)

Feature or function	Description	Reference for more information
XML northbound OSS interfaces	An OSS application uses the 5620 SAM Open Interfaces XML interface to configure or access network management information contained in the 5620 SAM database. The XML interface can then receive information from or manipulate the managed object model. All transactions with the 5620 SAM database are processed by the 5620 SAM server. The 5620 SAM-O XML interface allows OSSs to: • access all 5620 SAM FCAPS functions for read, or read and write methods • ensure backward compatibility • access functions using HTTP or HTTPS and simple SOAP encoding • securely transport requests and receive responses	See the *5620 SAM-O OSS Interface Developer Guide*.
IS-IS protocol support	IS-IS is a link-state interior gateway protocol that uses the shortest path first algorithm to make routing decisions. IS-IS entities consist of: • networks, which are autonomous system routing domains • intermediate systems, which are routers such as the 7750 SR • end systems, which are network devices that send and receive PDUs The IS-IS information displayed and configured from the GUI includes: • a backbone area and the devices in the backbone area • a list of areas with the devices that are participating in the area • the open the area devices to display the interface IP addresses with the configured level (1, 2, or 1 and 2) of each interface	See the IS-IS overview, configuration, and procedural information in chapter 28.
Protocol support enhancements for BGP and LDP	From the GUI, you can enable and configure LDP parameters. From the network tab routing instance, there are two trees for LDP: Interfaces and Targeted LDP Peers. LDP is used to distribute labels. Devices can establish LSPs across a network by mapping network-layer routing information directly to the data link layer-switched paths. After LDP distributes the labels to an LSR, the LSR assigns the label to a FEC, and then informs each LSR in the path of the label and how the label is to switch data. T-LDP is supported on 7750 SRs and 7450 ESSs, DU-LDP is only supported on the 7750 SR. You can use the 5620 SAM to enable BGP on the device and to: • set the AS values for the routing instance • create confederations to group-managed routers • create BGP peer groups • create neighbors within the BGP peer groups	See the BGP and LDP overview, workflow, and procedures in chapter 28.

(2 of 4)

Feature or function	Description	Reference for more information
Daughter card and channelization support on the 7750 SR	The 5620 SAM supports: • Configuring unchannelized 1-port OC192, and 2- and 4-port OC48 daughter cards and card objects. • Configuring channelized 1-port OC12 and the 12-port DS3 daughter cards. You cannot create DS3 children objects using the 5620 SAM. Ports and channels can only be used in access mode. • Configuring BCP-Null, BCP Dot1q, Frame Relay, and IPCP encapsulation on access ports and channels on the daughter cards listed above. • Configuring PPP encapsulation on network ports and channels on the daughter cards listed above. • Configuring channelized 1x OC12 daughter cards and card objects to the DS0 level using the STS1 sub-channels that are available. • Configuring channelized 12xDS3/E3 daughter cards and card objects to the DS0 level using TDM channels.	See the equipment window overview and procedural information in chapter 15.
MPLS administrative group policy support	The 5620 SAM supports configuring MPLS administrative group policies, and assigning the groups to MPLS interfaces, LSPs, and LSP paths.	See the MPLS administrative group, MPLS interface, LSP, and LSP path procedural information in chapter 27.
Slope and network policy support	The 5620 SAM supports configuring slope and network policies which can be applied to router objects during service configuration or modification.	See the policy overview and procedural information in chapter 43.
Q in Q support	The 5620 SAM supports enabling Q in Q encapsulation on applicable ports, and configuring Q in Q encapsulation values on interfaces.	See the port and channel procedural information in chapter 17 to enable Q in Q. See the service creation procedural information in the appropriate service management chapter to configure encapsulation value on interfaces.
CSPF, Make before Break, and inheritance support on LSPs and LSP paths	The 5620 SAM supports configuring CSPF and Make before Break parameters on LSPs and LSP paths, and the inheritance of key LSP parameters, including CSPF and Make Before Break, by LSP paths.	See the LSP and LSP path procedural information in chapter 27.
MPLS topology maps, including LSP map	From the GUI, you can view additional maps that show the MPLS and LSP topology.	See the map management information in chapter 4.
Product renaming	The 5620 SRM is renamed to the 5620 Service Aware Manager. Most instances of 5620 SRM on the GUI are updated.	—

(3 of 4)

Feature or function	Description	Reference for more information
HVPLS	A hierarchical VPLS is created by enhancing the VPLS core mesh with access spoke circuits that are interconnected to another VPLS, a VLL, or a site. An HVPLS can: • reduce the complexity of mesh configuration • decrease the amount of signaling of routes between devices When traffic arrives at an access spoke circuit, it acts similarly to a bridge port. Flooded traffic received on the access spoke is replicated to all other spokes, meshes, or SAPs but is not transmitted on the port where it is received.	See the VPLS overview and procedures documentation for information about creating HVPLS spokes in chapter 68.
Grouping	You can use the grouping function to: • represent devices that are located in the same area, for example, in the same city • indicate network topology, for example, devices that operate in the same spanning tree or SONET/SDH ring	See the navigation tree configuration Procedure 17-4 for more information about creating groups.

(4 of 4)

4 — 5620 SAM map management

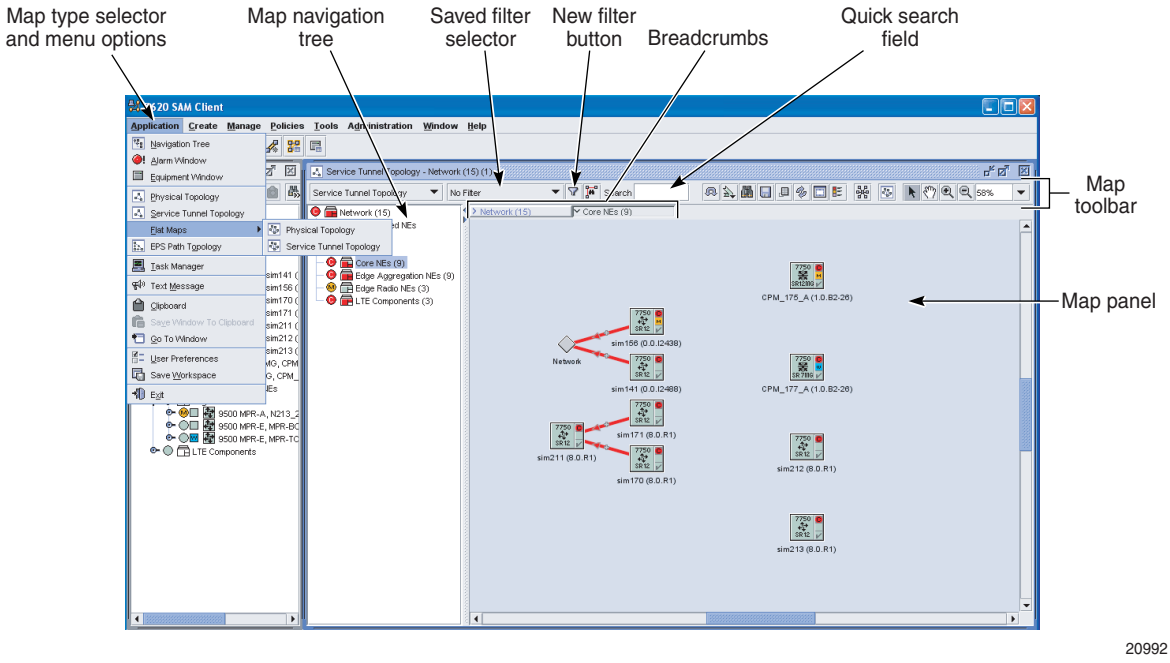
4.1 5620 SAM map management overview

The following 5620 SAM network topology maps are available:

- physical
- service tunnel
- service
- composite service
- LSP path
- LSP cross-connect

Each map displays network objects and information, and provides contextual menus to open forms that display additional information. In the context of a 5620 SAM map, a link object, such as a physical link or service tunnel, is called an edge. An object other than a link between objects, such as an NE or a topology group, is called a vertex. Figure 4-1 shows the main map elements.

Figure 4-1 Map elements



Map window

The map window includes the following:

- a title bar
- a map panel that displays the network objects
- a navigation tree that lists the topology groups
- a toolbar, which consists of a view selector, saved filter selector, quick-search field, and buttons that perform various functions

The title bar of the map window displays the following information:

- map type, for example, Physical Topology
- path from the network root to the currently displayed topology group; each step in the path is called a breadcrumb
- map number, for example, the first or the tenth map opened

Map panel

The map panel is associated logically with the map navigation tree. As the user navigates through the topology groups in the map navigation tree, the contents displayed on the map panel change. The topology group that is selected in the map navigation tree is the group that is displayed on the map panel.

When you double-click on a topology group object, the contents of the group on the map panel are displayed and the group is selected and opened in the map navigation tree. When you double-click on other map objects, such as routers or links, their property form opens. Right-click on any map object to display a contextual menu.

When map objects are linked between different topology groups, the line representing the connection terminates on a map object called a connector. The connector indicates that the endpoint of the link resides in another topology group. The label of the connector icon is the name of the topology group to which the link points. Connector objects do not have contextual menus.

When a physical link is created between a port or LAG managed by the 5620 SAM and an unmanaged object, the unmanaged object is called a remote endpoint. The remote endpoint label is configured by the user when the physical link is created.

You can configure a background image to display in the map panel for a topology group, for example, a map image of North America. You can position device icons and topology group icons in the map of the network to reflect their relative geographic locations.

Selecting map objects

Click on the Select Tool button to select an object on the map. You can select multiple objects by pressing the Shift key and clicking on each object you want to select, or by drawing a selection rectangle around all of the objects you want to select on the topology map. You can also press CTRL-A to select all items on a map.

You can select one or more objects and view them exclusively in a map by right-clicking on the selection and choosing Show Only Selected. The map is then filtered to display only the selected objects and the links between them. Links to other objects are not shown. You can revert to the previous view by right-clicking in the map and choosing Cancel Show Only.

When multiple objects are selected, you can shift the map focus to the next object using the F3 key, and shift the map focus to the previous object by pressing CTRL-F3.

You can also select all of the NEs that are attached to an NE by selecting one or more NE and right-clicking and choosing Select Attached.

You can deselect a selected NE by pressing the CTRL key and clicking on the NE.

Moving map objects

The 5620 SAM allows you to move map objects in the following ways:

- in the map panel; for example, to add a router to a topology group by dragging and dropping the router object to the topology group object in the map panel
- from the map panel to the map navigation tree; for example, to add a router to a topology group by dragging and dropping the router object from the map panel to the topology group object on the map navigation tree
- after discovery by using either the Auto-layout button or by moving the tiled icons to a new map panel location
- between two maps
- in the map navigation tree; for example, to make a topology group the immediate descendant of another topology group by dragging and dropping one topology group object to another topology group object in the map navigation tree

When a topology group is created, users with Topology Mgmt privileges can populate the group from the topology map by dragging and dropping map objects into the group in the map panel or in the map navigation tree, or from the map panel to the map navigation tree.

Note — You cannot move map objects to or from groups that are not within your span of control.

By default, users can move map objects and change the layout of the objects on the map, however the changes are not saved to the database when the map is closed. The ability to save changes to the layout of topology maps is controlled by scope of command roles and access permissions. Permissions are set by using 5620 SAM security configuration forms. See chapter 8 for more information about setting access privileges.

The Reload button icon indicates when you move a map object and change the layout of the objects. The Reload button icon changes to indicate whether moving a map object and changing the layout of the objects is saved to the database. See "Map toolbar" in this section for more information about the Reload button.

Note — When you move a map object in the map panel, the X,Y coordinates for the map object change. If you have update and execute scope of command access permission, this change affects all users that display the map view and the topology group.

Connectors can only be moved in the map panel. Connectors cannot be moved to another topology group.

Finding map objects quickly

The Search field beside the toolbar buttons is used to quickly locate a map object. When you enter a text string in the Search field and press ↵, the 5620 SAM searches each object name in the map for the string. If a match is found, the map focus shifts to the object. If multiple matches are found, you can shift the map focus to the next object using the F3 key, and shift the map focus to the previous object by pressing CTRL-F3.

Links and link groups

The topology maps display single links and multiple links that connect two map objects. Links are used to represent the physical connectivity between two NEs or logical connectivity, such as service tunnels. The map uses an arrow to display the direction of a unidirectional link. Multiple links between 2 objects are grouped, by default, as one link with no defined direction. Bidirectional links are displayed with no defined direction. A link group is displayed with a plus sign located on the link object.

When you double-click on a single link, the properties form for the link opens. When you double-click on the link group object for multiple links, a list form opens displaying all of the links that belong to the link group. For the physical, service tunnel, and LSP maps, a list form opens regardless of whether there is one link or multiple links in the link group.

A bidirectional link group is displayed with a plus sign icon located in the middle of the link object. A unidirectional link or link group is displayed using an arrow icon on the object pointing in the direction of the path.

The color of a single link object is determined by the status of each link endpoint. The color of a link group object is determined by the most serious alarm that is raised for a link in the link group.

Breadcrumbs

Breadcrumbs are buttons that are displayed along the top of the map panel. Breadcrumbs indicate, from left to right, the hierarchy of the topology groups to the group currently displayed in the map panel. The default top of the hierarchy, the breadcrumb at far left, is the entire network. Click on a breadcrumb to open the map for the corresponding group.

Map navigation tree

The following network topology maps display a map navigation tree:

- physical map
- service tunnel map

You can use the map navigation tree:

- for non-linear navigation to any topology group on the map
- to display the topology group hierarchy starting from the entire network

The map navigation tree displays:

- topology groups, including group names
- status of the topology groups

The circle icon to the left of the topology group icon represents the aggregated alarm status for the group. It represents the most serious alarm against descendant device.

The topology group icon is divided into three sections. The top right square represents the most severe state of all descendant devices. The bottom right square represents the most severe state of all descendant links. The bottom section of the topology group icon represents the most severe state of the devices and edges that are immediately descendant of the group. See chapter 34 for more information about viewing alarm status information in a map navigation tree. To troubleshoot alarms using topology maps, see *5620 SAM Troubleshooting Guide*.

When you click on a map object in the map navigation tree, the contents of the object are displayed in the map panel, and the map object is selected.

When you double-click on an object in the map navigation tree or press the + key when the object is selected, the object opens and the child objects are displayed. Double-click on the object again or press the - key to close the object. A turner to the left of the map object indicates that the object contains child objects. For example, a topology group that contains one or more child topology groups has a turner to the left of the topology group in the navigation tree.

Note — Keyboard-based navigation tree operations may not function as expected when you open the client GUI using a third-party access tool, for example, a Citrix server.

Contextual menus for objects in the map navigation tree

To open a contextual menu for an object, right-click on a map object in the map navigation tree. The following describes the contextual menu options for each object in the map navigation tree hierarchy.

- The contextual menu options for the default Discovered NEs topology group include:
  - List

    The List option opens the Discovered NEs form with a list of newly discovered NEs.

- The contextual menu options for a topology group include:
  - Equipment

    The Equipment option opens a Group (Create) form to create a descendant topology group for the selected group in the navigation tree.
  - Delete

    The Delete option deletes the topology group from the network after the objects in the group have been removed from the group. This option is not available for the network (root) topology group.
  - Make Root In New Tree

    The Make Root In New Tree option opens an equipment navigation tree window with the selected topology group as the root of the tree.
  - Make Flat Map for Group

    The Make Flat Map for Group option opens a flat map of the topology group.
  - Properties

    The Properties option opens the Group (Edit) form. The form displays read-only information and configurable parameters. You can use the Copy button to create topology groups in the network using the same parameter information.

The composite service topology map also has a map navigation tree. The following describes the contextual menu options for each object in the map navigation tree hierarchy of the composite service topology map:

- The contextual menu option for a composite service includes:
  - Properties

    The Properties option opens the Composite Service (Edit) form. The form displays read-only information and configurable parameters.
- The contextual menu options for a service tier include:
  - Properties

    The Properties option opens the *Service* (Edit) form. The form displays read-only information and configurable parameters for the selected service.
  - Remove

    The Remove option deletes the service from the network.

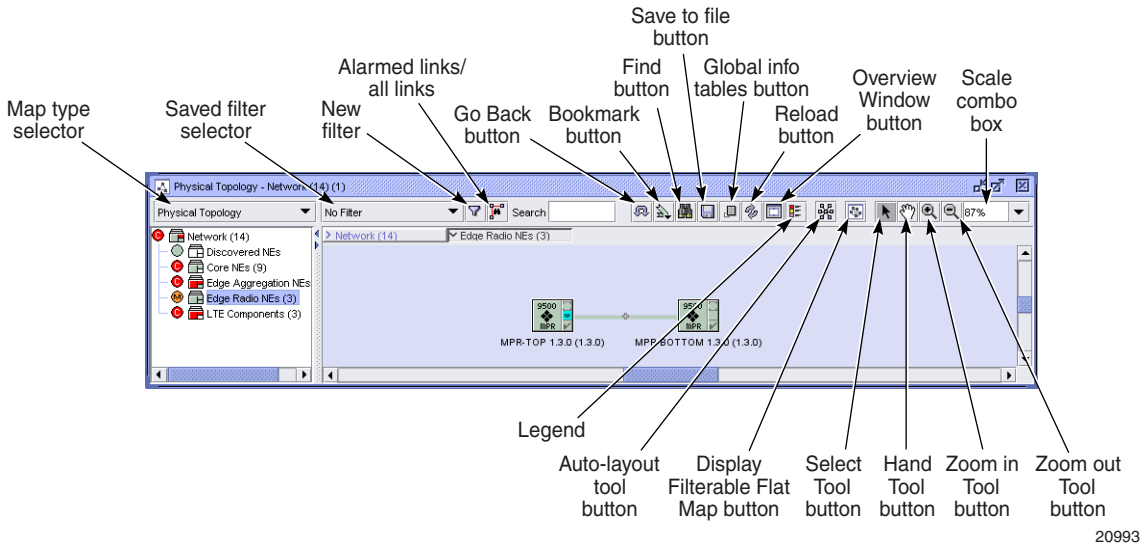
Warning — Deleting a service is not the same as removing a service from a composite service. Deleting a service removes the service from the 5620 SAM database. To avoid a service outage, be certain of the action that you are taking.

See Procedure 72-2 for more information about removing a service from a composite service.

Map toolbar

The map toolbar allows you to manage a 5620 SAM map view. The toolbar is above the map panel in the map window. Figure 4-2 shows the map toolbar elements.

Figure 4-2 Map toolbar elements



Map type selector

The map type selector is a drop-down menu that lists the map view options that you can choose to specify the view. The map type selector offers the following views:

- Physical Topology
- Service Tunnel Topology

Links shown button

Click on the Links shown button to specify whether the topology map displays all links or only links with associated alarms. The Links shown button options are:

- All links shown
- Only alarmed links shown

Go Back button

Click on the Go Back button to navigate between previously viewed topology groups. For example, if you are viewing Router Group 1 then view Router Group 2, click on the Go Back button to return to Router Group 1. The Go Back button only functions in one map type; both previously viewed topology groups must be the same map type.

Bookmark button

Bookmarks are used to create shortcuts to frequently visited locations on a map. Click on the Bookmark button and choose to add a bookmark or manage existing bookmarks.

Find button

Click on the Find button to search for network objects on a map. You can choose to search for specific vertices or edges. A list form opens that allows you to configure specific criteria to filter the results of your search. See chapter 2 for information about performing searches.

When the network object is found, the map navigation tree displays the topology group that contains the object. If necessary, the 5620 SAM scrolls to the part of the map where the object is located.

Save To File button

Click on the Save To File button to save the map view or the full map. You can choose the location to save the map image and the file type. See Procedure 4-12 for more information about using the Save To File button. Figure 4-3 shows the Save To File button.

Figure 4-3 Save To File button

Global Info Tables button

Click on the Global Info Tables button to create information table configurations, apply information table configurations globally, or turn the global information table option off. See Procedures 4-13 and 4-14 for more information about using the Global Info Tables button. Figure 4-4 shows the Global Info Tables button.

Figure 4-4 Global Info Tables button

Caution — Applying an information table configuration to many objects on the map may take a long time.

Reload button

Click on the Reload button to load the topology map from the 5620 SAM database. The topology map is updated to display the latest configurations. The Reload button icon changes to indicate whether moving a map object and changing the layout of the object is saved to the database. Figure 4-5 shows a Reload button icon when changes do not affect the database.

Figure 4-5 Reload Button indicating no database changes

Figure 4-6 shows the Reload button icon when changes are made to the map view and saved to the database.

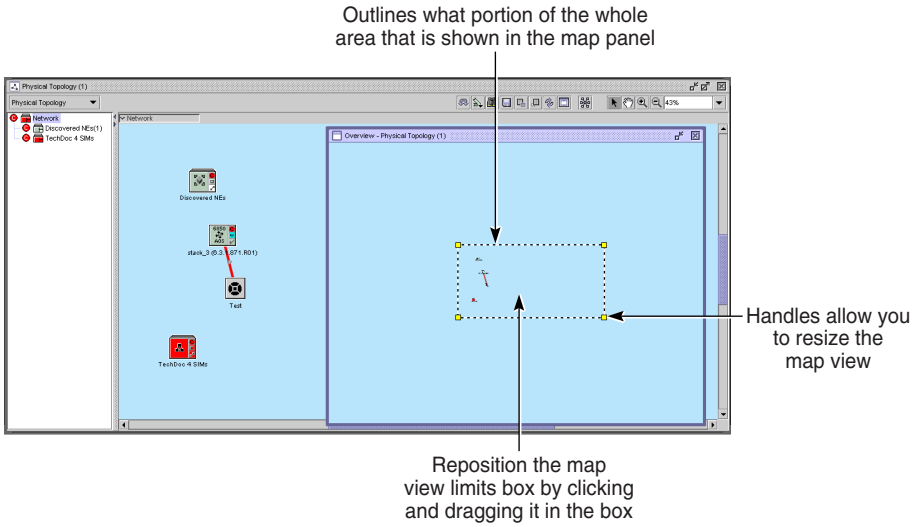
Figure 4-6 Reload Button indicating database changes

Caution — When you reload a map from the database, the database is unavailable during the loading period.

Overview Window button

Click on the Overview Window button to open the Overview window. Use the Overview window to pan the entire map, or a specific group or service, and the area that you want to view. Figure 4-7 shows the Overview window.

Figure 4-7 Overview window



Legend button

Clicking on the Legend button opens a contextual menu that displays a list of map legend types, if multiple legends are available, or opens the Legend form. Choosing a legend type from the contextual menu opens the Legend form with the appropriate legend tab displayed. The following legend types are available, depending on the map type:

- icons—always shown; displays the icons used to identify objects
- colors—displays the color scheme used for identifying map objects
- highlight sessions—displays the highlight sessions for the current map, and allows clearing of one or more sessions
- other legend types that are specific to a type of map

Figure 4-8 shows the Legend button.

Figure 4-8 Legend button

Rearrange by Service Tiers button

The Rearrange by Service Tiers button is available only for composite service topology maps. Figure 4-22 shows the composite service map. Figure 4-9 shows the Rearrange by Service Tiers button.

Figure 4-9 Rearrange by Service Tiers button

Click on the Rearrange by Service Tiers button to organize the composite service tier icons in the map panel by service tier. The service tier icons are displayed in the following order from the top of the panel:

- tier 1 icons (typically IES and VPRN services)
- tier 2 icons (typically VPLS and MVPLS)
- tier 3 icons (typically satellite HVPLS and VLL services)
- tier 4 icons (typically VLAN services)

  .

  .

  .
- tier n icons (user-assigned)

Caution — The current composite service map is redrawn when you click on the Rearrange by Service Tiers button, and the prior layout of the composite service map cannot be recalled.

Auto-Layout button

Click on the Auto-layout button to lay out the map icons. Figure 4-10 shows the Auto-Layout button.

Figure 4-10 Auto-Layout button

The layout options are:

- Circular — emphasizes ring and star topologies in networks. Objects are grouped according to the network structure and arranged in circles or radial tree structures.
- Smart Organic—emphasizes inherent data groupings and symmetries. This information helps with understanding the interconnections of complex structures.

The Auto-Layout tool is useful when:

- many newly discovered NEs are tiled together on the map and difficult to view
- a large number of network device icons are spread out across the map and cannot be easily viewed without zooming out

After you click on the Auto-Layout button, icons with links between them are placed closer together in the center of the map. Icons without links are placed on the periphery of the linked icons.

Note — You can also apply the auto-layout option to a contiguous group by right-clicking on one of the selected objects. See Procedure 4-23 for information about using the auto-layout function.

Caution — After you click on the Auto-Layout Tool button and confirm the action, any existing map layout is overwritten and cannot be recovered. If you are satisfied with the layout of the icons on the map, do not use the Auto-Layout Tool button.

Display Filterable Flat Map button

Click on the Display Filterable Flat Map button to quickly display a flat map of the current topology map view. You can also view a flat map on the 5620 SAM by choosing Application→Flat Maps from the 5620 SAM main menu. Figure 4-11 shows the Display Filterable Flat Map button.

Figure 4-11 Display Filterable Flat Map button

Select Tool button

Click on the Select Tool button to select and move an object on the map or to view object information. You can select and move multiple objects by pressing the Shift key and clicking on each object you want to select, or by drawing a selection rectangle around all the objects you want to select on the topology map.

Hand Tool button

Click on the Hand Tool button to switch to a pan mode. Click on the background to move the contents of the map in any direction. When you are in the pan mode and you scroll over an object, you can select and move an object on the map or view object information. You can select and move multiple objects by pressing the Shift key and clicking on the object you need to select.

Note — You can temporarily activate the panning function by pressing and holding the space bar, and then clicking in the map panel.

Zooming in and out using a mouse or toolbar buttons

The ability to zoom in and out on a map allows you to view hundreds of map objects at once to see the scope of the network, or view the information for one NE. Click on the Zoom in Tool and Zoom out Tool buttons and click on the map to resize the objects in a map or use the mouse wheel to zoom in and zoom out of topology maps. Click on the map and roll the mouse wheel forward to zoom in or roll the mouse wheel backward to zoom out. Each roll of the mouse wheel brings the map objects closer or further.

When a map is at a low zoom level, the icons are displayed at a reduced size, link lines are thinner and labels are hidden. Labels are displayed when you click on the reduced icon. When a map is viewed at a high zoom level, the icons are displayed at normal size, link lines are thicker and labels are displayed.

Note — Object icons are displayed at a reduced size in a flat map.

Scale combo box

Use the scale combo box to increase or decrease the map zoom. You can choose a zoom percentage value from 25% to 300%, or fit all objects in the window from the drop-down menu. The scale combo box displays the current scale of the map.

New Filter button

A filter allows you to apply one or more object filters to a map view, to narrow the range of objects that are displayed. Filters can be saved for future searches on similar objects. When a filter is applied, the name of the filter is displayed on the saved filter selector.

When a filter is applied, only the objects that the filter returns are displayed, with the following exceptions:

- if one link endpoint is displayed, the other endpoint is also displayed, even if the filter excludes it
- if a filter does not include a link filter, only the links between the returned NEs are displayed.

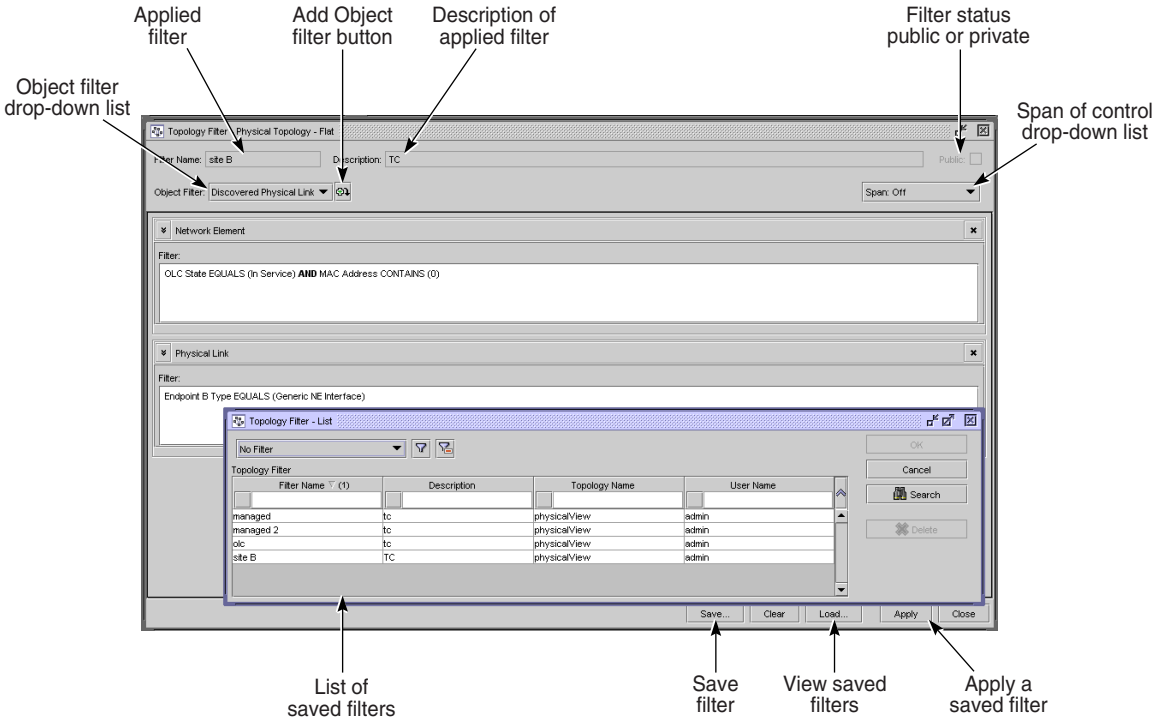
Filters can be saved as private or public. You can apply a span of control to public filters to filter out objects that are not in the current user span of control. Public filters can only be changed by the user who created them. Private filters appear only for the user who creates them.

Click on the Filter button to create and save filters that specify the objects displayed in a map. Figure 4-12 shows the Filter button.

Figure 4-12 Filter button

You can create a filter based on a combination of search criteria. Figure 4-13 shows the navigation buttons that you can use to create, apply, and save a map filter. See Procedure 4-19 for more information about creating a topology map filter. See chapter 2 for more information about configuring filters.

Figure 4-13 Filtered map form



Zooming in and out

The ability to zoom in and out on a map allows you to view hundreds of map objects at once to see the scope of the network, or view the information for one NE. See Procedure 4-24 for information about zooming functions.

When a map is viewed at a low zoom level, the icons are displayed at a reduced size, link lines are thinner and labels are hidden. Labels are displayed when you click on the reduced icon. When a map is viewed a a high zoom level, icons are displayed at normal size, link lines are thicker and labels are displayed.

Bookmarks

You can bookmark frequently visited areas of the map for easier navigation when you return to those locations. Bookmarks are associated with a map view. To use the bookmark, you must be in the same view where you created the bookmark or a view that shares the same group, for example, a topology group that belongs to both the physical topology map and the service tunnel map. Otherwise, the bookmark menu option is disabled.

You can access the bookmark drop-down menu using the Bookmark button on the map toolbar. Figure 4-2 shows the Bookmark button. The bookmark menu is divided into two sections and separated by a horizontal line. The top section of the drop-down menu contains the bookmark management functions, and the bottom section contains the user-created dynamic list of bookmarks.

The list of bookmarks is updated when you add, remove, group, or rearrange the bookmarks. The menu items can be bookmarks or folders, which can expand to display more bookmarks or folders.

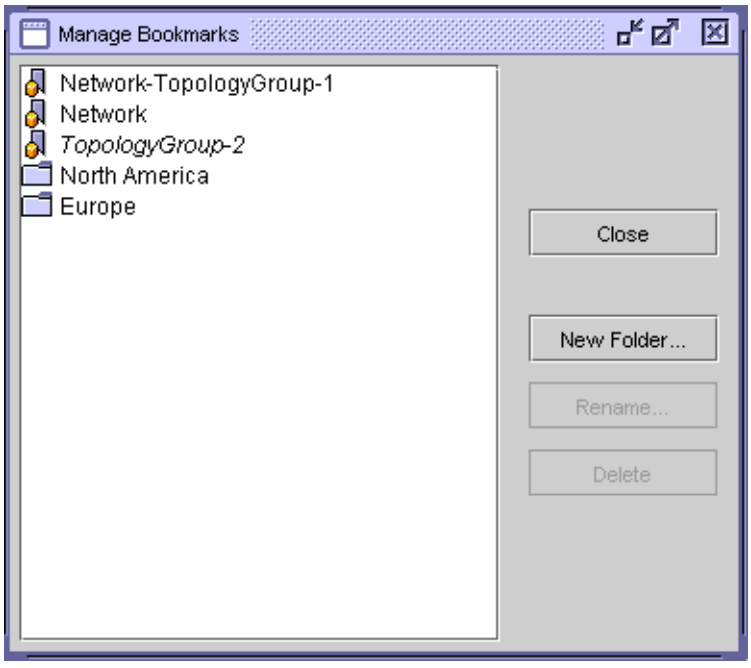
Note — A large number of bookmarks is difficult to manage. Bookmarks should be organized in folders for better usability and easier management. Alcatel-Lucent recommends that you create a maximum of 1000 bookmarks.

When a bookmark is selected, the map panel displays the bookmarked topology group. The map navigation tree expands to display the topology group.

When a valid bookmarked topology group is moved to another group, the bookmark for the group is updated to correspond to the new location of the group. If the bookmark location is not valid, for example, a topology group was deleted since the bookmark was created, an invalid bookmark message is displayed. The map panel remains unchanged.

Click on the Add Bookmark menu option to add the topology group currently viewed in the map panel as a bookmark. Click on the Manage Bookmarks menu option to open the Manage Bookmarks form. Figure 4-14 shows the Manage Bookmarks form.

Figure 4-14 Manage Bookmarks form



The Manage Bookmarks form has a list panel on the left in which the bookmarks and folders are listed in a tree structure. You can drag and drop bookmarks and folders in and out of other folders in the list panel. Select a bookmark or folder for editing. Click on an empty area to deselect the tree object. Double-click on a top-level folder to open the folder and display its contents. A turner to the left of the descendant folder object in the list panel indicates that the folder contains descendant objects, such as bookmarks or other folders.

The names of invalid bookmarks, and bookmarks and folders that are not from the current view, are displayed in italics.

The following buttons with which you can perform different actions are displayed to the right of the list panel:

- Close—used to close the Manage Bookmarks form. All changes in the form are saved when you click on the Close button.
- New Folder—used to create a folder in the list panel. The Folder Properties dialog box appears.
  - If a folder is selected in the list panel, the new folder that is an immediate descendant object of the selected folder.
  - If no folder is selected in the list panel, the new folder is created as a top-level folder.
- Rename—used to rename a folder or bookmark. The Rename dialog box appears. The Name field contains the name of the selected folder or bookmark. This button is enabled only when a folder or bookmark is selected in the list panel.
- Delete—used to delete a selected folder or bookmark from the list panel. This button is enabled only when a folder or bookmark is selected.

Information tables

You can configure information tables that are displayed beside map objects. An information table contains specific values, such as an NE chassis type, software descriptor, and system address. Information tables are displayed beside each map object to which the configuration applies. You can drag and drop information tables on topology maps, but the new table location is not saved with the map.

Note — You cannot apply an information table configuration to link groups or topology groups.

Multiple information tables can be applied to map objects, but only one is displayed at a time. Tab indicators appear on the information table to indicate that multiple information tables apply to the map object. You can cycle through the applied information tables by clicking on the information table and pressing the Tab key.

You can specify that information tables are to be displayed only during a mouse-over operation, which is when the mouse pointer passes over an object. You can also specify whether an information table contains a header. Header display is enabled by default, and cannot be disabled for mouse-over tables. See Procedure 4-13 for more information. Mouse-over supports cycling between tables using the Tab key.

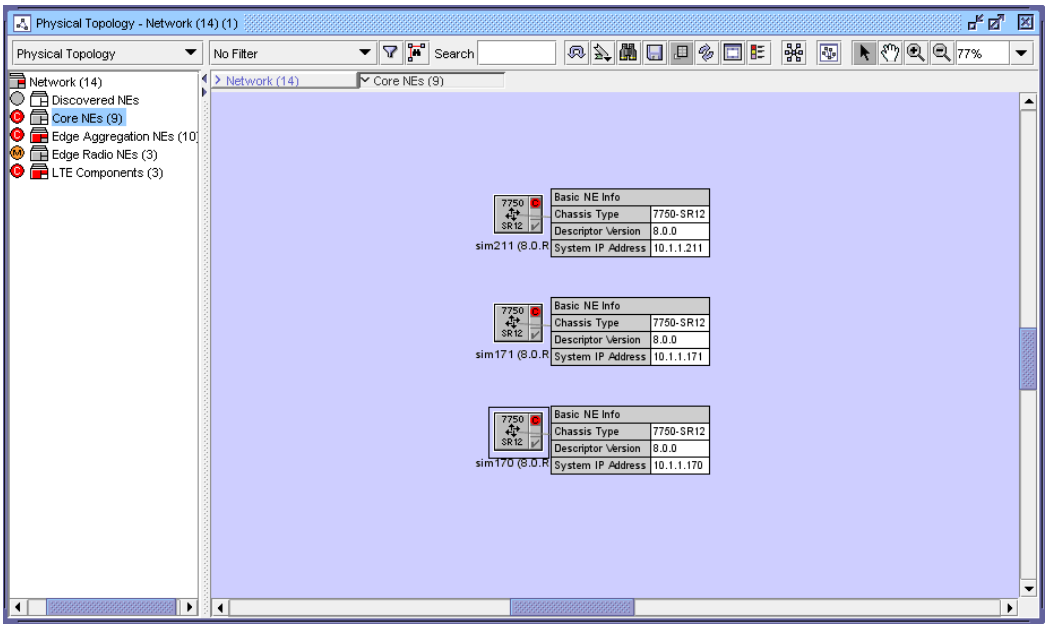
The following types of information tables can be applied to map objects:

- global—available for all map types
- selected—available for all map types
- highlight—available for maps that support the highlight function
- others that are specific to a map type

Global Info Tables

When one or more information table configurations are available for a map type, you can apply an information table configuration to all map objects using the Global Info Tables button. You can also use this button to turn the global information table configuration off. See Procedure 4-14 for more information about how to use the Global Info Tables feature. Figure 4-15 shows a map view with an information table configuration applied to all map objects.

Figure 4-15 Applied global information table configuration



Selected Info Tables

You can apply an information table configuration to one map object or a selected group of map objects by right-clicking on the object or selected group. You can also use this contextual menu to turn the selected information table configuration off. See Procedure 4-15 for information about how to use the Selected Info Tables feature.

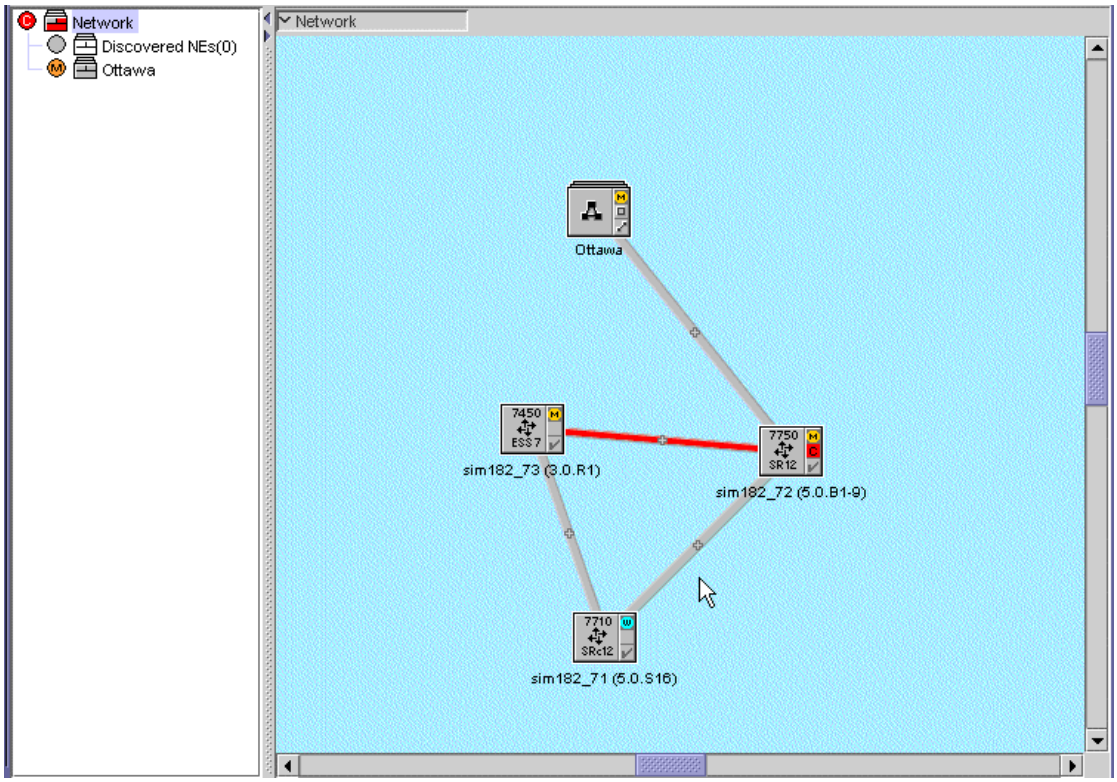
Map Highlight Info Tables

On a map that supports the highlight function, you can apply an information table configuration to a map highlight by right-clicking on an existing highlight session from the Highlight Sessions tab of the Legend-*topology* form. You can also use this contextual menu to turn the highlight information table configuration off. See Procedure 4-16 for more information about how to use the Map Highlight Info Tables feature.

Physical topology map

The physical topology map is available by choosing Application→Physical Topology from the 5620 SAM main menu. The physical topology map is used to view and manage Layer 1 objects, including the logical grouping of devices. Figure 4-16 shows the physical topology map.

Figure 4-16 Physical topology map



The physical topology map is open in the working panel by default when the 5620 SAM client GUI starts.

The following apply to link objects in the physical topology map:

- The following colors indicate link status:
  - Red—the link has failed
  - Light Gray—the link is in service
  - Green—the link is new
  - Blue—the link is in standby or backup mode
  - Dark gray—the link is unknown
  - Purple—the physical link is being diagnosed
- If endpoint B of a physical link is on an unmanaged device, the status of the physical link is the same as the status of endpoint A, which is on a 5620 SAM-managed device.
- A LAG link is represented as a single physical link. However, if you right-click on a LAG link, the form that opens provides information and configuration options for the entire LAG link. For example, the Endpoint Info tab on the Discovered Physical Link form shows the link endpoints as LAG endpoints rather than physical ports, and allows the operator to open the LAG properties form.

Menu options for physical topology map background

To open a contextual menu for the map background, right-click on the map background.

- The contextual menu options for the map background include:
  - Equipment

    The Equipment option displays a fly-out menu. You can choose the Create Group option to create a descendant topology group for the selected group in the navigation tree or a choose the Create Physical Link option to create links between map objects.
  - Delete

    The Delete option applies only to a topology group view, and deletes the topology group.
  - Make Root In New Tree

    The Make Root In New Tree option opens an equipment navigation tree window with the selected topology group as the root of the tree.
  - Properties

    The Properties option opens the Group (Edit) form. The form displays read-only information and configurable parameters. You can use the Copy button to create topology groups in the network using the same parameter information.
  - Reference

    The Reference option displays a fly-out menu. You can choose from the Set All, Clear All, or the Cleanup All options.

    The Reference option essentially takes a snapshot of the physically topology at a specific time. Any deviation from this checkpoint can then be subsequently shown.

    The Set All option checkpoints all currently discovered links that exist. Any object that was previously checkpointed and is operationally down is left untouched. Any object that goes operationally down in the future is not removed, but is simply marked as operationally down.

    The Clear All option clears all object checkpoints. Any object that is operationally down (shown as a red link) is removed from the database. Any non-checkpointed object that becomes operationally down in the future is removed from the system.

    The Cleanup All option keep the current checkpoint set for objects that are operationally up, but removes checkpoints from objects that are operationally down objects. This is basically the same as the Clear All option, but only affects operationally down objects.
  - Highlight MTU Mismatch

    The Highlight MTU Mismatch option is used to highlight MTU mismatches between physical ports. When the configured MTU on two or more endpoints do not match, an alarm is raised to notify the operator of a possible configuration error.

    This is supported on both point-to-point and broadcast physical links. MTU mismatches can also be discovered by conducting an RCA audit. See Procedure 77-6 for more information.
  - Duplicate Links

    The Duplicate Links option displays a fly-out menu. You can choose either the Highlight Duplicate Links or Delete Duplicate Links option.

    It is possible for both a manual link and a discovered physical link to exist on the same two endpoints. When this happens, a duplicate link alarm is raised. This alarm only occurs on point-to-point links and when both endpoints are ports or LAGS. You can identify such duplicate links by choosing the Highlight Duplicate Links option. You can remove these duplicate links by choosing the Delete Duplicate Links option. This action prompts you with a warning and then delete all of the manually created physical links. This alarm is not raised on existing manual links (for example, those in place after a database upgrade).

- Highlight Nearest Non-TPMR Links

  The Highlight Nearest Non-TPMR Links option is used to highlight the nearest Non-Two Port MAC Relay links between nodes. See "LLDP" in chapter 27 for more information.
- Highlight Nearest Customer Links

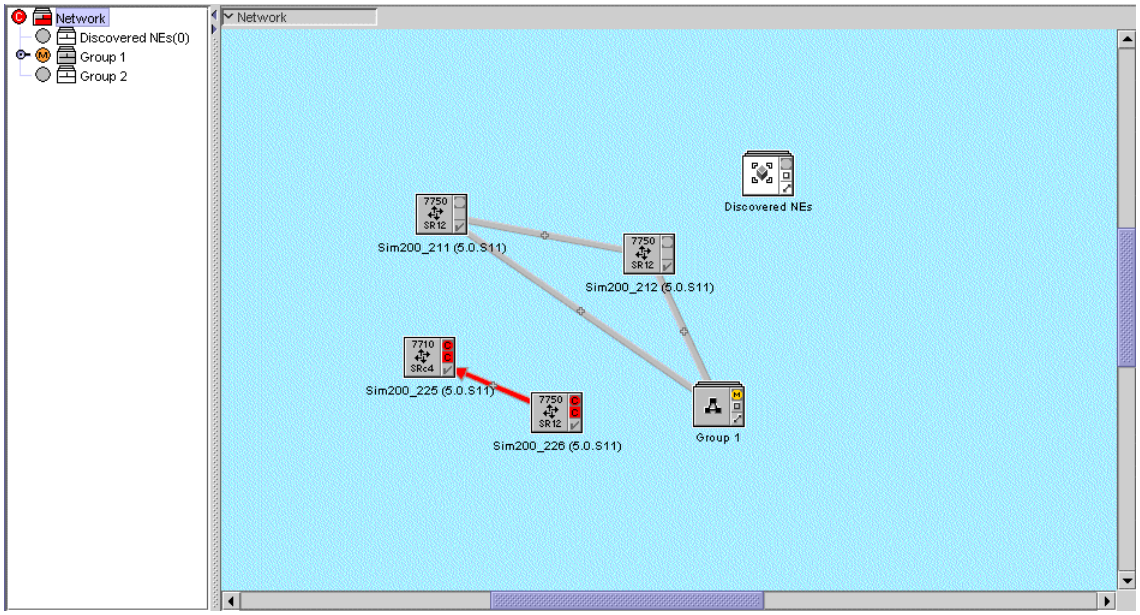
  The Highlight Nearest Customer Links option is used to highlight the nearest customer links between nodes. See "LLDP" in chapter 27 for more information.
- Discovery Manager

  The Discovery Manager option opens the Discovery Manager (Edit) form. You can create NE discovery rules and discover NEs. See chapter 13 for information about discovering NEs and creating discovery rules.

Service tunnel topology map

A service tunnel topology map is available on the 5620 SAM by choosing Application→Service Tunnel Topology from the 5620 SAM main menu. The Service Tunnel Topology map is displayed, as shown in Figure 4-17.

Figure 4-17 Service tunnel topology map



Icons in the service path topology map represent devices. The color of the device icon represents the status of the device. Red indicates that the device is down. Green indicates that the device is up. Yellow indicates that the device is being synchronized.

Link groups between devices represent service tunnels. When a link group is red, at least one tunnel in the link group is down. For link groups between managed devices, right click on the link group icon to list and edit tunnels in the link group. For link groups between managed and unmanaged devices, right-click on the link group icon to open contextual menus and submenus which allow you to open additional information forms for the service tunnel, including the properties form.

EPS path topology maps

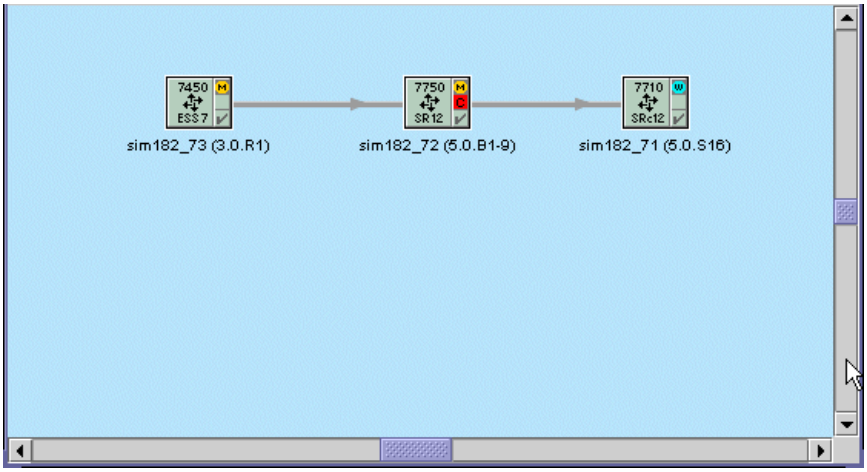
An EPS path topology map is available on the 5620 SAM by choosing Application→EPS Path Topology from the 5620 SAM main menu. See the *5620 SAM LTE User Guide* for information about EPS paths.

LSP path topology map

An LSP path topology map is available from the MPLS Path form and the LSP Path form. See Procedure 4-5 to view the map from the MPLS Path form. See Procedure 4-6 to view the map from the LSP Path form.

The LSP path topology map is used to view a specific provisioned, actual, or CSPF LSP path in the context of its source, and transient and destination hops. Figure 4-18 shows an LSP path topology map.

Figure 4-18 LSP path topology map



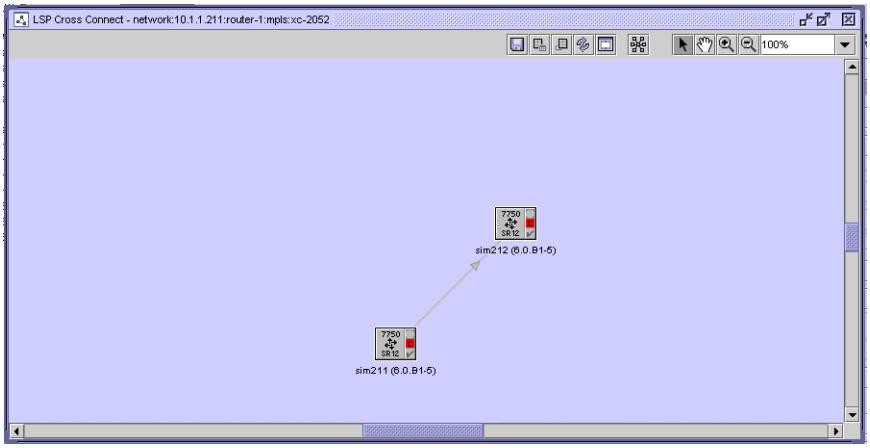
When you view the LSP path topology map, hops are linked by straight lines, where each line represents a sub-path between two hops of the LSP path. The direction of each path is indicated by an arrow. Green lines indicate provisioned paths, and gray lines indicate actual paths.

LSP cross-connect topology map

An LSP cross-connect topology map is available from the LSP Path form. To view the map from the LSP Path form, see Procedure 4-8.

The LSP cross-connect topology map is used to view a specific LSP cross-connect in the context of its source, and transient and destination hops. Figure 4-19 shows the LSP cross-connect topology map.

Figure 4-19 LSP cross-connect map



Flat maps

Flat maps provide a complete network view without topology groups. A flat topology map can display up to 1000 objects. You can narrow the range of objects that are displayed by creating and saving filters and filter definition trees.

A flat map is available on the 5620 SAM by choosing Application→Flat Maps from the 5620 SAM main menu. The following flat map types are available:

- Physical Topology
- Service Tunnel Topology

A flat map is used to view a large number of network objects and link groups. You can double-click on a NE in the flat map to display the object properties. For example, when you double-click on an NE, a property form opens, from which you can view or configure the NE parameters.

Object icons in a flat map are displayed at a reduced size, link lines are thinner, and object information is not displayed. Flat maps support the following, as do other 5620 SAM topology maps:

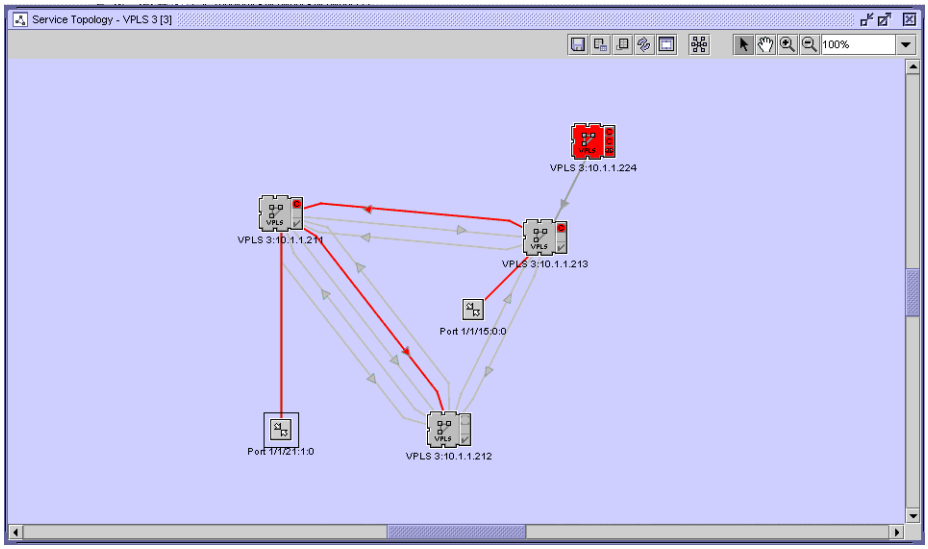
- mouse-based navigation
- zooming
- NE and link status colors
- searching
- filtering

Service topology maps

A service topology map is available from the Manage Services form. To view the map from the Manage Services form, choose Manage→Service→Services from the 5620 SAM main menu and list services by clicking on the Search button. Select one or more services in the list and click on the Topology View button.

Figure 4-20 shows the service topology map.

Figure 4-20 Service topology map



The large icons represent managed devices. The small icons represent unmanaged devices. The label of the managed device icon indicates the service name and the IP address of the device.

The symbol and color in the top-right corner of the managed device icon represents the aggregated alarm status, the most severe alarm on any of the services on the device. The symbol immediately below the aggregated alarm status symbol on the icon and the color of the icon together indicate the alarm status for the service site. A red icon indicates that the service on the device is down. A green icon indicates that the service on the device is up.

The port icons represent managed access interfaces. A service site can support up to 20 SAPs. When the number of SAPs on a service site exceeds 20, all of the SAPs on that site are grouped into a SAP group, represented by a SAP group icon on the map. When the number of SAPs drops below 20, the SAP group icon is replaced with the icons for all the individual SAPs on the map. To view the list of SAPs in a SAP group, right-click on the SAP group icon and choose List L2 Access Interface or List L3 Access Interface, depending on the service type, from the contextual menu. The corresponding Site form for the service opens with the L2 Access Interface or L3 Access Interface tab is displayed.

A line between two map objects represents a link or group of links. Links between device icons represent service circuits. Links between device icons and port icons represent the binding of an access port or interface to a service. The symbol and color in the bottom right corner of the managed device icon represents the connectivity alarm status. During a resynchronization of the managed device, the icon represents the resynchronization status, and is shown in yellow. The status is inherited from the link endpoints. A plus sign icon located in the centre of the link indicates a bidirectional group link. An arrow icon located on the link indicates a unidirectional link and identifies the direction of the path.

Right-clicking on a managed NE, port, or link opens a contextual menu. Contextual menus allow you to open additional information forms, such as the properties form for an object.

You can view multiple services on a map at the same time if the services are selected from the Manage Services form during map creation.

Service segmentation

A service segmentation view is also available to aid in conceptualizing complex services. Segments are logical grouping of interconnected sites, services, and bindings. The segmentation view is available for VPLS and VLL services.

A service segment is considered to be a portion of a single service that extends to multiple sites connected within that segment. It is based on the service type through one of the possible connection topologies (for example, mesh, PBB tunnels, a switching VLL, rings, and so on), without having to pass through any connectors such as spokes, CCAGs, or SCPs (SAP-to-SAP).

General examples of segments in Layer 2 service topologies include:

- A simple pair or single spoke/mesh SDP binding comprises one segment
- A mesh of a multi-node VPLS service comprises one segment
- A multi-node mesh with a spoke SDP to a single node comprises two segments
- Each mesh of VSIs forms a segment (applicable to H-VPLS)

Just a few examples of the many possible service-specific segmentation configurations include scenarios such as the following:

- H-VPLS (Inter-Metro with redundant spoke SDPs):
  - One application of H-VPLS is the connection of two or more geographically-dispersed VPLS domains belonging to the same customer. Two spoke SDP connections are used to connect each VPLS between the two metros, either in a redundant PW spokes topology or under STP protocol. The redundant spokes comprise one segment, while each VPLS will also comprise one or more segments, depending on their specific configurations.
- VLL Switching:
  - For a VLL service at a switching router, a terminating PE device has at least one VLL SAP, while a switching PE device has a VLL instance which cross-connects two spoke bindings. All VLL instances of such a service must have the same service ID, and if the VLL has one or more switching sites, it must have at least two terminating sites. In this scenario, the primary and redundant spoke SDPs on the same network endpoint are considered to be in the same segment.
- PBB:
  - In a PBB configuration, the B-VPLS is considered a service tunnel, from the I-VPLS or I-Epipe perspective. Therefore, the sites connected via a B-VPLS (that is, having the same ISID) are considered to be in one segment.
  - I-Sites bound to the same PBB tunnel (B-VPLS) and having the same ISID exist in the same segment.
  - Epipe sites bound to same PBB tunnel (B-VPLS) exist in the same segment

Whenever you modify a service, note that the following actions can trigger segment creation, modification, or deletion in a segmented service view:

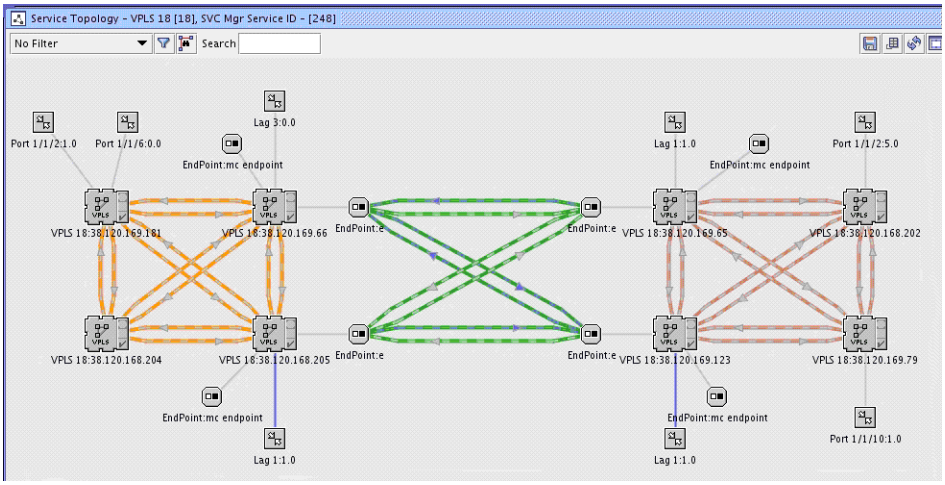
- Adding or removing service sites
- Creating or deleting spoke and/or mesh bindings (either through the 5620 SAM GUI or CLI)
- Creation or deletion of VLAN Uplinks by 5620 SAM

You can access the segmented view of a service by right-clicking on an empty portion of the background in the service's topology view. A contextual menu allows you to activate or de-activate the segmented view for the service.

In a segmented view, the outlined links of all spoke bindings, mesh bindings, or VLAN Uplinks are colored in the same distinct way for the segment they belong to. However, there are currently only 19 different colors available for use in showing service segments. If all the colors for a specific service are used, a warning message is logged to indicate this.

Figure 4-21 shows an example of how the 5620 SAM displays the segmented view of an H-VPLS Metro-to-Metro service.

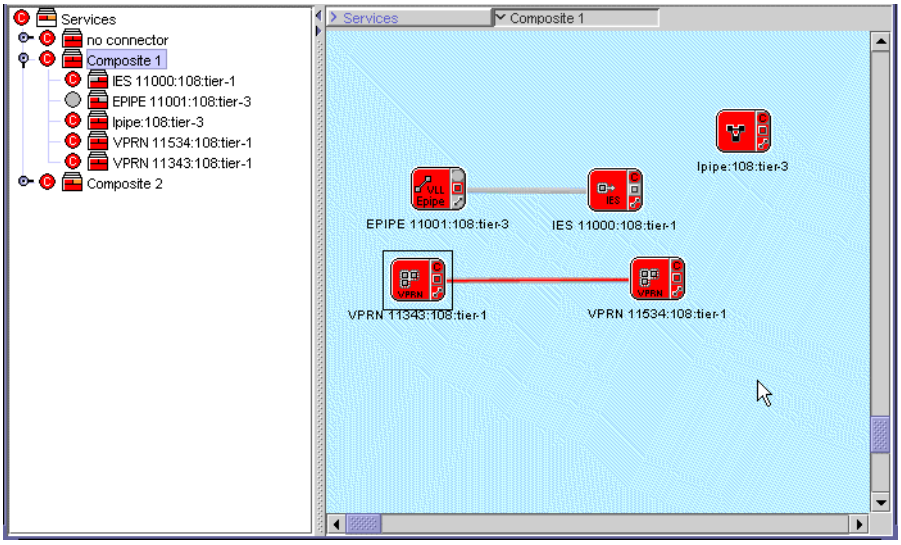
Figure 4-21 Service segmentation example



Composite service topology maps

You can use the 5620 SAM to view composite service topology and flat topology maps. Figure 4-22 shows a sample composite service topology map. When you open a flat topology view map, the navigation tree is not part of the map.

Figure 4-22 Composite service topology map



In a composite service topology map, you can use the navigation tree at the left side to display the composite service and service tier hierarchy starting from the services object. The map navigation tree displays the following:

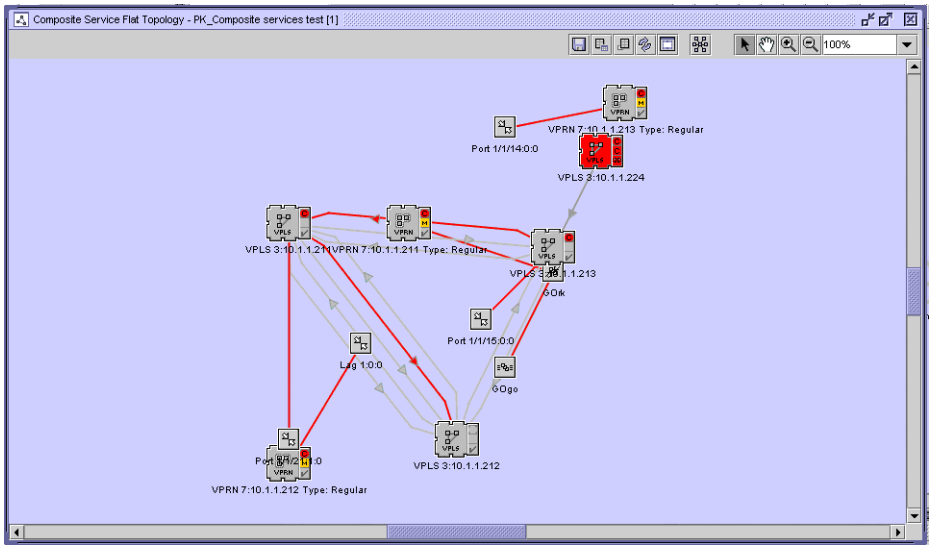
- composite services and service tiers, including service name and tier number
- status of the composite services and their tiers

The map toolbar for the composite service topology map includes the Rearrange by Service Tiers button. See "Rearrange by Service Tiers button" in this section for more information.

Double-click on a composite service object in the map panel to display the service objects that belong to the composite service. Double-click on the service objects to display the service sites and access interfaces. The links or groups of links between the service sites and access interfaces are also displayed.

In the composite service topology map, all service objects in the composite service are displayed simultaneously. The service sites, access interfaces, and the links or groups of links between them are also displayed. The navigation tree is thus not required in this view. Figure 4-23 shows a sample composite service flat topology map.

Figure 4-23 Composite service flat topology map



You can right-click on an object icon or link group icon to turn up, shut down, or display the properties form for the item.

Modifying a service from the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the component tree view in the service configuration forms.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

Services that can be modified from their topology views include VPLS, VPRN, VLL, IES, and composite services. See the appropriate service management chapter for procedures that describe how to modify services from the topology view.

Managing OAM diagnostics from the topology view

A 5620 SAM operator can configure and execute OAM diagnostic tests from the service topology view. A right-click contextual menu of test types and test operations allows a GUI user to perform many test-management tasks. The OAM diagnostic functions on the map are enabled and disabled using a selector in the map window.

5620 SAM OAM diagnostic test management using the topology map is supported for the following service types:

- VPLS
- Epipe
- VPRN

You can use a contextual menu option to open a test-creation form for selected map objects such as NEs, SAPs, SDPs, MEPs, and MIPs. The form is automatically populated with the information for the selected objects. After you apply the test configuration, you can use the map to execute the test and view the results. A test result summary is viewable using statically displayed or mouse-over global info tables that are shown beside the object that initiates the test. By default, the info table for a tested object displays the five most recent test results; you can enable or disable the display of individual or all results.

The general OAM contextual menu options that are available include the following:

- Create OAM Tests—lists the tests that are appropriate for the service type and selected objects; choosing a test type opens the pre-populated test-creation form
- Select OAM Tests—opens a filterable list form from which you can choose previously created tests associated with one or two objects

Note — The tests that are listed using the Select OAM Tests option do not include generated tests, or manually added first-run or last-run tests in a test suite.

See Procedure 4-4 for information about enabling basic OAM-related map functions.

Working with Ethernet CFM objects

You can configure and manage Ethernet CFM objects such as MEGs, MEPs, and MIPs using the Ethernet CFM contextual menu option. MEPs and MIPs are represented iconically. For example, a SAP or SDP binding object can have a graphical connector to MEPs and MIPs, and a site object can be connected to a B-VPLS MEP.

A service topology map displays only one MEG at a time. The MEG is selectable using a drop-down list in the map window when the OAM function on the map is enabled. The CFM objects associated with the currently selected MEG are displayed.

For a MEP, the following attributes are displayed:

- the MEP level, as a number inside the icon
- the MEP direction, as the up or down direction in which the icon points
- the MEP administrative state, as the icon color

For a MIP, only the level is displayed.

The displayed Ethernet CFM contextual menu options for MEPs and MIPs depend on the Ethernet CFM configuration, for example, the MD level and whether MEPs and MIPs are already present in the MEG.

When an operator right-clicks on the map background, the available Ethernet CFM option is global MEG creation, which opens a configuration form populated with the selected sites or all service sites, if none are selected.

When the selected object is a SAP, you can create, view, and delete MEPs, however MEP creation in this context is limited to B-VPLS sites. You can enable, disable, and view MIPs. Enabling a MIP creates a MIP only when the configuration supports this function.

When the selected object is an SDP binding, you can enable, disable, and view the associated MEPs.

Note — When you enable a MIP on a SAP or SDP binding, the 5620 SAM creates a MEG site if one does not exist, and uses explicit MHF creation.

4.2 5620 SAM map management workflow

1 Determine the map you want to use.

- view maps that show services
- view maps that show topology

2 View the relationship between objects drawn on the map by choosing one of the following map types:

- service, to show which NEs are used by the services
- topology, to show the relationship between NEs in a routing domain

3 Create topology groups and populate the groups with devices to organize the network, as required, or create map filters to narrow the range of objects displayed.

4 Create physical links between managed and unmanaged devices to configure Layer 1 management, as required.

4.3 5620 SAM map management procedures

Use the following procedures to perform map management tasks.

Procedure 4-1 To open a map from the 5620 SAM main menu

1 Choose Application from the 5620 SAM main menu.

2 Choose a type of map to view from the menu options:

- Physical Topology to view Layer 1 network connectivity
- Service Tunnel Topology to view service tunnels
- Flat Maps→Physical Topology
- Flat Maps→Service Tunnel Topology

The appropriate map opens and displays the network objects.

See Procedure 4-11 for information about using the map elements. See Procedure 4-21 to list or view object information from a map. See section 4.1 for information about the map views.

Procedure 4-2 To open a service topology map

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Create an appropriate filter and click on the Search button. A list of services is displayed.

3 Select one or more services in the list and click on the Topology View button. A dialog box appears.

4 Click on the Yes button to continue. The Service Topology map opens.

See Procedure 4-11 for information about the map elements. See Procedure 4-21 to list or view object information from a map. See section 4.1 for information about the map views.

Procedure 4-3 To open a composite service topology map

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Create an appropriate filter and click on the Search button. A list of composite services is displayed.

3 Select one or more composite services in the list and perform one of the following steps:

a Click on the Topology View button. The Composite Service Topology map opens.

b Click on the Topology View Flat button. The Composite Service Flat Topology map opens.

4 See Procedure 4-11 for information about the map elements. See Procedure 4-21 to list or view object information from a map. See section 4.1 for information about the map views.

Procedure 4-4 To use OAM diagnostic functions on a service topology map

Perform this procedure to enable the OAM diagnostic functions on a service topology map and use the basic OAM controls in the map window. See the other procedures in this chapter for information about using specific elements such as the toolbar buttons and info tables.

1 Create a service topology map by selecting the service in the Manage Services form and clicking on the Topology View button.

2 Select the OAM check box at the bottom left of the map window.

3 To manage one or more objects, select the objects and right-click on the set of objects to choose an option from the contextual menu.

4 To select a MEG to display, choose the MEG using the drop-down list of available MEGs at the bottom of the map window.

5 To view the properties of the selected MEG, click on the MEG Properties button at the bottom of the window. The Global Maintenance Entity Group (Edit) form opens with the General tab displayed. The service displayed on the map is listed on the Service tab.

6 To resynchronize the MIPs in the selected MEG, click on the Resync MIPs button at the bottom of the window.

7 Use the other procedures in this chapter to refine the map contents or display object properties, as required.

8 Use the right-click contextual menu options to configure and manage OAM objects, as required. See "Managing OAM diagnostics from the topology view" in section 4.1 for a functional description of the available contextual menu options for OAM diagnostics.

Procedure 4-5 To open an MPLS provisioned path map from the MPLS Path form

1 Choose Manage→MPLS→MPLS Paths from the 5620 SAM main menu. The Manage MPLS Paths form opens.

2 Create an appropriate filter and click on the Search button. A list of MPLS paths is displayed.

3 Select an MPLS path in the list and click on the Properties button. The MPLS Path configuration form for the MPLS path opens.

4 Click on the Provisioned Path tab button. The hops of the MPLS path appear in a list.

5 Select a hop in the list and click on the Topology View button. The MPLS provisioned path map opens showing the hops between the devices.

See Procedure 4-11 for information about the map elements. See Procedure 4-21 to list or view object information from a map. See section 4.1 for information about the map views.

Procedure 4-6 To open a dynamic LSP path map from the LSP Path form

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Create an appropriate filter and click on the Search button. A list of dynamic LSPs is displayed.

3 Select a dynamic LSP in the list and click on the Properties button. The Dynamic LSP (Edit) form opens.

4 Click on the LSP-Path Bindings tab button. The LSP paths appear in a list.

5 Select an LSP path in the list and click on the Properties button. The LSP-Path Binding (Edit) form opens.

6 Perform one of the following:

a View the topology for provisioned paths:

i Click on the Provisioned Path tab button. The hops of the LSP path appear in a list.

ii Select a hop in the list and click on the Topology View button. The LSP path map opens showing the hops between the devices.

b View the topology for actual paths:

i Click on the Actual Path tab button. The hops of the actual path appear in a list.

ii Select a hop in the list and click on the Topology View button. The LSP path map opens showing the actual path hops between the devices.

c View the topology for CSPF paths:

i Click on the CSPF Path tab button. The hops of the CSPF path appear in a list.

ii Select a hop in the list and click on the Topology View button. The LSP path map opens showing the CSPF path hops between the devices.

See Procedure 4-11 for information about the map elements. See Procedure 4-21 to list or view object information from a map. See section 4.1 for information about the map views.

Procedure 4-7 To open a flat map

1 Perform one of the following.

a Open a flat physical topology map.

i Choose Application→Flat Maps→Physical Topology from the 5620 SAM main menu. The Topology Filter - Physical Topology - Flat filter form opens.

ii Go to step 2.

b Open a service tunnel topology map.

i Choose Application→Flat Maps→Service Tunnel Topology from the 5620 SAM main menu. The Topology Filter - Service Tunnel Topology - Flat filter form opens.

ii Go to step 2.

See Procedure 4-11 for information about the map elements. See Procedure 4-21 to list or view object information from a map. See section 4.1 for information about the map views.

2 Perform one of the following:

a Perform Procedure 4-19 to create a filter definition.

b Perform Procedure 4-20 to load and apply a saved filter.

3 View the map.

4 Close the map.

Procedure 4-8 To open a dynamic LSP cross-connect topology map

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Create an appropriate filter and click on the Search button. A list of dynamic LSPs is displayed.

3 Choose an LSP in the list and click on the Properties button. The Dynamic LSP (Edit) form opens.

4 Click on the Cross Connects tab. The cross-connects of the LSP path appear in a list.

5 Choose a cross-connect in the list and click on the Topology View button. The LSP path map opens and displays the cross-connects between the devices.

See Procedure 4-11 for information about the map elements. See Procedure 4-21 to list or view object information from a map. See section 4.1 for information about the map views.

Procedure 4-9 To configure and view topology map icon labels

By default, topology map icons include a descriptive label. For example, the label on a managed device icon on the Service Topology map includes the service name and the IP address of the device.

1 Choose Application→User Preferences. The User Preferences form opens with the General tab displayed.

2 Click on the Topology tab. A list of topology map icons is displayed.

3 Select a topology map icon.

4 Configure Text Field #1 and Text Field #2 to identify the information to display in each map icon label.

5 Click on the OK button. The User Preferences form closes.

Procedure 4-10 To preserve the topology map layout

Perform this procedure to configure the 5620 SAM client software to preserve the topology map layout in one client session for use during the subsequent session. This procedure applies to 5620 SAM single-user clients and to client delegate servers.

Note 1 — To save the topology map layout, you must be a system administrator using an account with an assigned admin scope of command role.

Note 2 — Performing this procedure on a client delegate server affects all clients that use the client delegate server.

Note 3 — You can use the 5620 SAM auto-client update function to reconfigure the client software for multiple 5620 SAM single-user clients. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about using auto-client update to perform a client software upgrade. See chapter 5 for information about using auto-client update to perform a client software configuration change.

Changes to the client configuration file on the 5620 SAM main server override the local client configuration. You can exclude a 5620 SAM client from a global configuration change by specifying a startup option when you open the client GUI, as described in chapter 2.

1 Choose Application→Exit from the 5620 SAM main menu. A dialog box appears.

2 Click on the Yes button. The GUI application closes.

3 Log in to the single-user client or client delegate server station.

Note — On a client delegate server station, you must log in as the samadmin user.

4 Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config on Solaris and C:\5620sam\client\nms\config on Windows.

5 Open the nms-client.xml file using a plain-text editor.

6 Locate the following line in the file:

```
<mapserver mapLayoutAdminLock="false">
```

7 Edit the line to read as follows:

```
<mapserver mapLayoutAdminLock="true">
```

8 Save the nms-client.xml file.

9 Close the nms-client.xml file. Subsequent client GUI sessions that open on the single-user client or client delegate server station save the topology map layout in the database.

Procedure 4-11 To view and understand map elements

1 Open a map, as described in Procedures 4-1 to 4-8.

2 View the map elements, which can include the following:

- device icons, which each display one of the following background colors to represent connectivity status and SNMP reachability
  - red—down or unreachable
  - yellow—resynchronizing or discovering
  - green—normal

  The icon in the top-right corner of a device icon represents the most serious alarm raised against the device.

  The icon in the middle right hand side of a device icon represents the alarm status for the device.

The icon in the bottom right corner of a device icon represents the connectivity to the device. During resynchronization, the icon represents the resynchronization status; for example, yellow.

- topology group icons, which have the following characteristics:
  - The background color white indicates that the topology group does not contain any descendant objects.
  - The color and icon in the upper left corner of the topology group icon indicate the most severe alarm on any of the devices in the group.
  - The color of the upper middle section of a topology group icon indicates the aggregated connectivity status of the devices in the group.
  - The color of the upper right corner of the topology group icon indicates the aggregated link status of the links in the group.

- composite service icons, which have the following characteristics:
  - The color and icon in the upper left corner of the composite service icon indicate the most severe alarm on any of the devices in the composite service.
  - The color of the upper middle section of the composite service icon indicates the aggregated connectivity status of the devices in the composite service.
  - The color of the upper right corner of the composite service icon indicates the aggregated link status of the links in the composite service.

- service tier icons in composite service maps, which have the following characteristics:
  - The color and icon in the upper left corner of the composite service icon indicate the most severe alarm on any of the devices in the service.
  - The color of the upper middle section of the composite service icon indicates the aggregated connectivity status of the devices in the service.
  - The color of the upper right corner of the composite service icon indicates the aggregated link status of the links in the service.

Procedure 4-12 To save a map to a file

You can use the Save to File button to save a portion of a map or the entire map to a file. You can save the file in JPEG, BMP or PNG format.

1 Open a map.

2 Click on the Save To File button. The save options are displayed in the drop-down menu.

3 Choose a type of view from the drop-down menu:

- Choose Save Map View to save the current view.
- Choose Save Full Map to save the entire map view.

The Save form opens.

4 Save the results.

i To choose a directory for the file, use the Save In parameter.

ii To create a filename, use the File Name parameter.

iii Choose BMP, JPEG, or PNG from the File of Type drop-down menu.

iv Click on the Save button. The map view is saved to the specified file.

Procedure 4-13 To create an information table configuration

You can create an information table configuration for all map objects, selected map objects, or map highlights. See Procedure 4-14 to apply a configuration to all map objects. See Procedure 4-15 to apply a configuration to selected map objects. See Procedure 4-16 to apply a configuration to highlighted map objects.

1 Open a map.

2 Click on the Global Info Tables button. A drop-down menu opens with the information table configurations displayed.

3 Select the Configure menu item. The *topology_view* Info Table Configurations form opens.

4 Click on the Create button. The *topology_view* - Info Table Configuration form opens.

5 Configure the Configuration Name parameter.

6 For each map object type, click on the associated check box to select the attribute for display in the information table.

Note — If an applicable attribute is not selected for a specific object type, an information table is not displayed when you apply an information table configuration to objects of that type.

7 Click on the OK button. The *topology_view* - Info Table Configuration form closes, and the new configuration is listed on the *topology_view* - Info Table Configurations form.

8 Close the *topology_view* - Info Table Configurations form.

Procedure 4-14 To enable or disable a global information table

The Global Info Tables button allows you to view an information table for all map objects. An information table configuration must be created before it can be applied. See Procedure 4-13 for information about creating an information table configuration.

1 Open a map.

2 Click on the Global Info Tables button. A drop-down menu opens with the information table configurations displayed.

3 Perform one of the following:

- **a** Select a radio button to apply an existing global information table configuration. The map is refreshed with the corresponding information table displayed beside the map objects.
- **b** Click on the Off button. The global information table feature is disabled.

Procedure 4-15 To enable or disable a selected information table

The Selected Info Tables menu option allows you to view an information table for a map object, or a group of map objects. An information table configuration must be created before it can be applied to a map object or a group of map objects. See Procedure 4-13 for information about creating an information table configuration.

1 Open a map.

2 Right-click on a map object or a selection of map objects. A drop down menu opens.

3 Choose Selected Info Tables. A drop down menu opens with a list of information table configurations and an Off option.

4 Perform one of the following:

- **a** Choose an information table configuration. The map view is refreshed with the configured information table displayed beside the map objects.
- **b** Choose the Off option. The selected information tables for the selected map objects are no longer displayed.

Procedure 4-16 To re-enable or disable map highlights

1 Open the required map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Perform one of the following:

a Re-enable a disabled highlight. Perform the following steps.

i Select the check box in the Active column for the highlight.

ii Click on the Apply button. The map view is refreshed with the highlight displayed.

b Disable the highlight. Perform the following steps.

i Deselect the check box in the Active column for the highlight.

ii Click on the Apply button. The map view is refreshed. The highlight and the associated information tables are no longer displayed.

4 Click on the Close button. The Legend - *topology* form closes.

Procedure 4-17 To enable or disable a highlight information table

You must create an information table configuration before you can apply it to a map highlight. See Procedure 4-13 for information about creating information table configurations.

1 Open the required map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Select one or more highlight sessions in the list.

4 Right-click on the selected highlight sessions and choose Highlighted Info Sessions from the contextual menu. A drop-down menu opens with a list of information table configurations and an Off option.

5 Perform one of the following.

a Choose an info table configuration. The map view is refreshed with the chosen information table displayed beside the highlighted map objects.

b Choose the Off option. The map view is refreshed and no longer displays information tables for the highlighted map objects.

Note — When a highlight is disabled or deleted, the map no longer displays the information tables for the highlight.

6 Click on the Close button. The Legend - *topology* form closes.

Procedure 4-18 To delete a map highlight

1 Open a map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Click on a map highlight to select it.

4 Right-click on the selected highlight and choose Delete. A dialog box appears.

5 Click on the Yes button. The highlight is deleted.

6 Click on the Close button. The Legend - *topology* form closes.

Procedure 4-19 To create a map filter

Perform this procedure to configure a filter to restrict the objects in a map view. You can save the filter for searches on similar objects.

1 Open a map.

2 Click on the New Filter button. The Topology Filter - *topology_view* form opens.

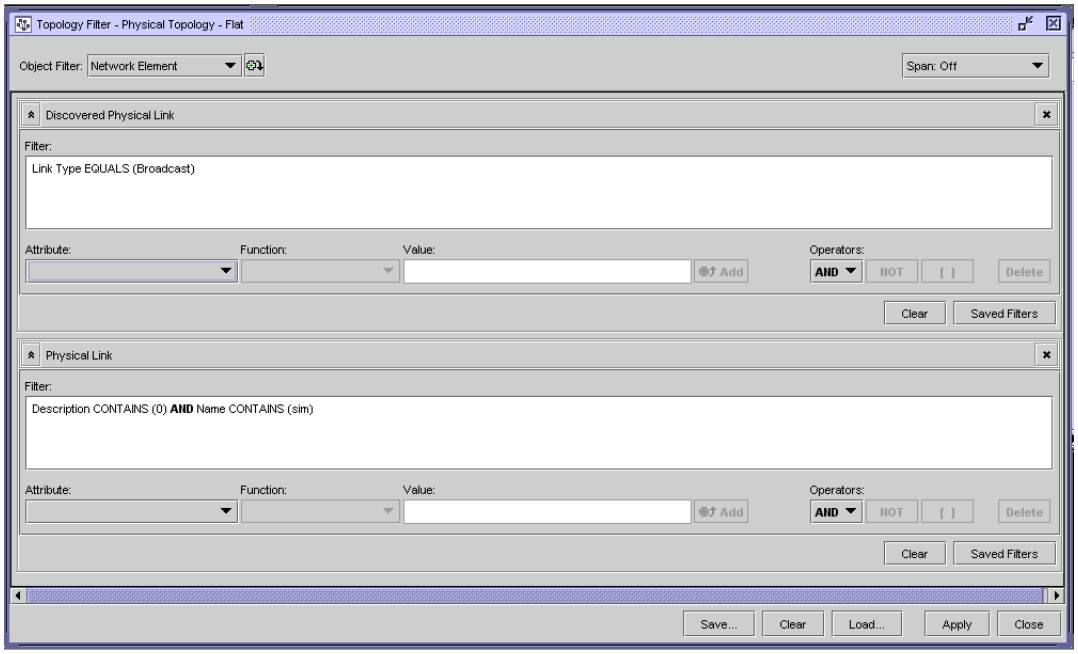
3 Choose an object filter from the Object Filter drop-down menu. Table 4-1 lists the filter options for each map type.

Table 4-1 Map filter options

Type of map	Filter options
Physical topology	Discovered Physical Link Network Element Optical Link Physical Link
Service tunnel topology	Network Element Tunnel

4 Click on the Add Object Filter button. The selected object filter is displayed in the filter panel as shown in Figure 4-24.

Figure 4-24 Map filter



5 Choose one or more of the object filters to create the filter. See chapter 2 for information about creating filters.

6 Configure the Span parameter.

7 Perform one of the following:

a Click on the Apply button to apply the filter and not save the filter. The map view is refreshed to display only the map objects defined in the filter. The filter selector displays Filter Applied.

b Perform the following steps to save the filter.

i Click on the Save button. The Save Filter form opens.

ii Configure the parameters:

- Filter Name
- Description
- Public

8 Click on the Save button. The Save Filter form closes.

9 Close the Topology Filter - *topology_view* form.

Procedure 4-20 To load and apply a saved filter to a topology map

See Procedure 4-19 for information about creating a filter definition tree.

1 Open a map.

2 Click on the saved filter selector and choose a filter from the drop-down list.

The 5620 SAM applies the filter and the map view is refreshed to display only the map objects specified in the filter. The filter name is displayed in the saved filter selector.

Procedure 4-21 To view object information from a map

1 Open a map.

2 Right-click on one of the following objects:

- device icon
- plus sign icon in the centre of a link or link group
- port of a generic or unmanaged NE that indicates the endpoint of a link, path, tunnel, or service
- topology group icon

The appropriate contextual menu appears.

3 Choose a contextual menu option. The following are examples of the options available, depending on the type of object selected.

- Choose Equipment Window to view the object in the Equipment Window.
- Choose Properties to open the properties form for the object.
- Choose Scripts to open the properties form for an NE with the Scripts tab displayed.

Procedure 4-22 To manage the topology map window

The topology map panel and navigation tree panel are separated by a vertical split bar that you can use to control the panels. You can change the size, and hide, or show the map panel or the navigation tree panel.

1 To change the size of the map panel and the navigation tree panel, drag the vertical split bar to the left or right to control the amount of space used for the map panel and the navigation tree.

2 To hide the navigation tree panel, click on the vertical split bar left-facing arrow icon. The tree panel is hidden.

3 To show the map navigation tree panel, click on the vertical split bar right-facing arrow icon. The tree panel opens.

4 To hide the map panel, click on the vertical split bar right-facing arrow icon. The map panel is hidden.

5 To show the map panel, click on the vertical split bar left-facing arrow icon. The map panel opens.

Procedure 4-23 To auto-layout icons on a map

Caution — After you click on the Auto-Layout button and confirm the action, the existing map layout is overwritten and cannot be recovered. If you are satisfied with the layout of the icons on the map, do not use the Auto-layout button.

1 Open a map.

2 Perform one of the following:

a Auto-layout all of the icons on the map.

i Click on the Auto-Layout Tool button and choose one of the following options:

- Circular
- Smart Organic

A dialog box appears.

ii Click on the Yes button.

b Auto-layout a contiguous group of icons on the map.

i Select multiple objects.

ii Right-click on an object in the group and choose Layout Selected→Circular or Layout Selected→Smart Organic from the contextual menu.

The map layout changes so that icons with links between them are closer together, and icons without links between them are on the periphery.

Procedure 4-24 To zoom in and zoom out on a map

1 Open a map.

2 Perform one of the following:

- **a** Use the mouse wheel to zoom in and zoom out. Perform the following steps.
  - **i** Click on the map.
  - **ii** To zoom in, roll the mouse wheel forward.
  - **iii** To zoom out, roll the mouse wheel backward.
- **b** Use the Zoom In Tool and Zoom Out Tool. Perform the following steps.
  - **i** Click on the Zoom in Tool or Zoom out Tool button.
  - **ii** Move the mouse pointer into the map panel. The pointer changes to a magnifying glass containing a + or - sign.
  - **iii** Click on the area of the map you want to expand or contract. The map expands or contracts. Continue clicking until the desired zoom level is reached.
  - **iv** Use the opposite button and an equal number of clicks to return the map to its default setting.
  - **v** To return to the pointer icon, click on the Select Tool button in the toolbar.

3 Use the Scale combo box to specify a zoom level, and press ↵.

Procedure 4-25 To display only selected map objects

1 Open a map.

2 Select the objects.

3 Right-click on the selected objects and choose Show only Selected from the contextual menu. The map refreshes to display only the selected objects, and the word Hidden is displayed in the map panel to indicate that some objects are currently hidden.

4 To restore the original map view, right-click in the map panel and choose Cancel Show Only from the contextual menu.

Procedure 4-26 To display only highlighted map objects

1 Open a map.

2 Click on the Legend button in the toolbar and choose Highlight Sessions from the drop-down menu. The Legend form opens with the Highlight Sessions tab displayed.

3 Select one or more highlight sessions in the list.

4 Right-click on the selected highlight sessions and choose Show Only Highlighted from the contextual menu. The map refreshes to display only the highlighted objects, and the word Hidden is displayed in the map panel to indicate that the non-highlighted objects are currently hidden.

5 To restore the original map view, right-click in the map panel and choose Cancel Show Only from the contextual menu. The map refreshes to display the original view.

Note — You can also restore the original map view by right-clicking on the selected highlight sessions in the Legend form and choosing Cancel Show Only from the contextual menu.

Procedure 4-27 To search for a specific network object

1 Open a map.

2 Perform one of the following:

a To search for a network object by typing the name, or part of the name of the network object:

i Click on the Find button in the map toolbar.

ii Choose Find Vertex or Find Link. The Find *object* form opens.

iii Configure the filter criteria and click on the Search button. A list of objects is displayed.

Note — The search function is case sensitive.

iv Select an object in the list.

b To search for a network object by pasting the name of the network object from the clipboard:

i Click on the network object that you want to locate from the equipment view of the navigation tree or from a generated or displayed list.

ii Click on the Copy to Clipboard icon to copy the network object name to the clipboard.

iii Click on the Find button.

iv Choose Find Vertex or Find Link. The Find Object form opens.

v Click on the Paste button. The network object that you copied to the clipboard is displayed in the Find object with label containing text field.

Note — Only the first item listed on the clipboard is pasted in the Find object with label containing text field of the Find Object form.

c Use the Quick-search field on the map window. Perform the following steps.

i Type part or all of the object name in the Quick-search field beside the toolbar icons.

ii Press ↵. The map shifts to display the first object that matches the search criterion.

iii Press F3 to shift the map focus to the next matching object, if the search finds multiple matches.

iv Press CTRL-F3 to shift the map focus to the previous matching object, if the search finds multiple matches.

v Go to step 5.

3 Click on the OK button.

a If a match is found, the map panel displays the topology group that contains the object and the map navigation tree expands to display the group. If necessary, the map panel scrolls to the portion of the map where the object is displayed.

b If multiple matches are found, the Find Object form opens with a drop-down list of all of the search results. Go to step 4.

4 Select a network object and click on the OK button. The map panel displays the topology group that contains the object and the map navigation tree expands to display the group. If necessary, the map panel scrolls to the portion of the map where the object is displayed.

5 Manage the object, as required.

Procedure 4-28 To create a bookmark

See section 4.1 for more information about the bookmark function.

1 Open a map.

2 Locate the topology group that you want to bookmark.

Note — Bookmarks are associated with a map view. To use the bookmark after it is created, you must be in the same view where you created the bookmark or a view that shares the same group, for example, a topology group that belongs to both the physical topology map and the service tunnel map.

3 Click on the Bookmarks button and choose Add Bookmark. A bookmark for the currently displayed topology group is created.

Procedure 4-29 To manage bookmarks

See section 4.1 for more information about the bookmark function.

1 Open a map, as described in Procedures 4-1 to 4-8.

Note — Bookmarks are associated with a map view. To use the bookmark after it is created, you must be in the same view where you created the bookmark or a view that shares the same group, for example, a topology group that belongs to both the physical topology map and the service tunnel map.

Bookmarks that were not created in the map view currently displayed, or that are invalid, are disabled and cannot be selected. In the Manage Bookmarks form, these bookmarks appear in italics.

2 Click on the Bookmarks button and choose Manage Bookmarks. The Manage Bookmarks form opens.

3 Perform one of the following:

a Create a top-level folder to manage the bookmarks.

i Click on the New Folder button. The Folder Properties form opens.

ii Enter the name of the new folder in the Name field and click on the OK button. A new top-level folder is added to the list panel.

b Create a folder in an existing folder.

i Select an existing folder in the list panel and click on the New Folder button. The Folder Properties form opens.

ii Enter the name of the new folder in the Name field and click on the OK button. A new folder is added to the list panel inside the existing folder.

c Organize your bookmarks and folders. Drag and drop bookmarks and folders in and out of other folders in the list panel.

d Rename a bookmark or folder.

i Select an existing bookmark or folder in the list panel and click on the Rename button. The Rename form opens with the existing name in the Name field.

ii Change the text in the Name field and click on the OK button. The name of the bookmark or folder is modified.

e Delete a bookmark or folder.

i Select a bookmark or folder that you want to delete in the list panel.

ii Click on the Delete button. The selected bookmark or folder is removed from the list panel and the bookmark drop-down menu on the map toolbar.

4 Click on the Close button to close the Manage Bookmarks form and save the changes.

Procedure 4-30 To change the map background image

To view the map background image examples provided by the 5620 SAM, navigate to the background directory in the 5620 SAM client Installation directory, for example, /nms/images/map/background.

When adding your own map image to the directory, ensure that the file type is GIF and that the size is a maximum of 2000 × 2000 pixels.

The default background image is defaultBackgroundImage.gif.

1 Open a map, as described in Procedures 4-1 to 4-8.

2 In the map navigation tree, right-click on the topology group for which you want to change the map background image and choose Properties from the contextual menu. The Group - Network (Edit) form opens.

3 Modify the Background Image parameter to specify a new map image file, for example, n_america.gif.

4 Click on the OK button. A dialog box appears.

5 Click on the Yes button to proceed. The background image for the topology group changes to the selected image.

Procedure 4-31 To create a topology group

Note — A topology group can contain a maximum of 500 NEs.

1 Open the Group (Create) form using one of the following methods.

   a Choose Create→Equipment→Group from the 5620 SAM main menu.

   b Right-click on the Network icon in the equipment view of the navigation tree and choose Equipment→Create Group from the contextual menu.

2 Configure the parameters:

- Group Name
- Description
- Background Image

3 Click on the Apply button.

4 Click on the Spans tab button.

5 Click on the Add button. The Select Span(s) - Equipment Group form opens with a list of available spans.

6 Select one or more spans to apply to the topology group.

7 Click on the OK button. The Select Span(s) - Equipment Group form closes and a dialog box appears.

8 Click on the OK button to confirm the action.

After the topology group is created, an object for the topology group is displayed in the equipment navigation tree, and on the appropriate topology maps.

Procedure 4-32 To populate a topology group

Note — A topology group can contain a maximum of 500 NEs.

1 Choose Application→Physical Topology, Service Tunnel Topology, or LSP Topology from the 5620 SAM main menu. The appropriate map window opens.

2 Populate topology groups, as required,

a Click on a map object in the map panel, for example, a router or router group, and drag the object onto the topology group object to which you want the map object to belong in the:

- map panel
- map navigation tree

The map object becomes a descendant object of the topology group.

b Click on a topology group object in the map navigation tree and drag the object onto another group object in the map navigation tree to which you want the group object to belong. The topology group object becomes a descendant object of another group object.

Procedure 4-33 To modify a topology group and create topology groups with the same parameter settings

1 Right-click on the topology group object on the map for which you want to modify the parameters and choose Properties from the contextual menu. The Group (Edit) form opens.

2 Modify the parameters as required.

3 Click on the Apply button. A dialog box appears.

4 Click on the Yes button to save the changes.

5 If required, click on the Copy button to create more topology groups based on the same parameter information. A Group (Create) form opens with the existing parameter information.

6 Edit the parameter information as required.

7 Click on the OK button. The Group (Create) form closes.

8 Close the Group (Edit) form.

Any changes to the properties of a topology group appear immediately on the equipment navigation tree and the appropriate topology maps.

Procedure 4-34 To delete a topology group

When you delete a topology group object, the topology group cannot contain any devices or descendant topology groups.

1 Choose Application→Physical Topology, Service Tunnel Topology, LSP Topology from the 5620 SAM main menu. The appropriate map window opens.

2 Drag and drop all devices and descendant topology groups from the topology group that you want to delete to another topology group or the root group, for example, the network.

3 Right-click on the topology group object that you want to delete on the map and choose Properties from the contextual menu. The Group (Edit) form opens.

4 Click on the Delete button. A dialog box appears.

5 Click on the OK button to proceed. The topology group is deleted.

Procedure 4-35 To modify a service or composite service using the topology view

You can use the service or composite service topology view to add, modify, or navigate to service components. The service configuration form can also be accessed directly at any time from this view by right-clicking any component. This allows quick access to conduct more detailed component configuration.

1 Perform one of the following.

   a Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

   b Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure a search filter, if required, and click on the Search button. A list of services or composite services is displayed.

3 Perform one of the following.

   a Select a service and click on the Topology View button. The Service Topology map opens.

   b Select a composite service and click on the Flat Topology View map opens.

4 Right-click on the map background, or on one or more selected service sites, to display a contextual menu of configuration options. When you choose an option, a configuration form opens.

5 See the appropriate service management chapter for information about modifying a specific service type.

Procedure 4-36 To create a physical link

The MDA type for both physical link endpoints must be the same. Only one physical link can be configured on a port.

Users with Device Mgmt privileges can create, modify, and delete physical links.

1 Open the Physical Link (Create) form using one of the following methods.

a Choose Create→Equipment→Physical Link from the 5620 SAM main menu.

b Right-click on the topology map background in the equipment view of the navigation tree and choose Equipment→Physical Link from the contextual menu.

2 Configure the parameters:

- Name
- Description
- Endpoint A Type
- Endpoint B Type
- Notes

3 Configure the parameters in the Endpoint A panel by performing one of the following.

a If you set the Endpoint A Type parameter in step 2 to Port, go to step 4.

b If you set the Endpoint A Type parameter in step 2 to Network Element, go to step 5.

4 Configure the parameters in the Endpoint A - Port panel by performing one of the following steps.

a Use the Select Endpoint A - Port - Physical Link form to search for a port.

i Click on the Select button in the Endpoint A – Port panel to choose a managed endpoint for the physical link. The Select Endpoint A - Port - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of ports.

iii Select a port and click on the OK button. The Select Endpoint A - Port - Physical Link form closes and the port parameter information is displayed in the Endpoint A - Port panel of the Physical Link (Create) form.

b Choose a port from the equipment navigation tree.

i Select a port object and click on the Copy to Clipboard button. The port information is copied to the clipboard.

Alternatively, you can choose a port object from the equipment window and click on the Copy to Clipboard button. See chapter 16 for information about using the equipment window.

ii Click on the Paste from Clipboard button in the Endpoint A - Port panel of the Physical Link (Create) form. The port parameter information is displayed in the Endpoint A - Port panel.

5 Configure the parameters in the Endpoint A - Network Element panel by performing one of the following steps.

a Use the Select Endpoint A - Network Element - Physical Link form to search for a port.

i Click on the Select button in the Endpoint A panel to choose a managed endpoint for the physical link. The Select Endpoint A - Network Element - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of NEs.

iii Select an NE and click on the OK button. The Select Endpoint A - Network Element - Physical Link form closes and the NE parameter information is displayed in the Endpoint A - Network Element panel of the Physical Link (Create) form.

b Choose an NE from the equipment navigation tree:

i Select an NE and click on the Copy to Clipboard button. The NE information is copied to the clipboard.

Alternatively, you can choose a NE from the equipment window and click on the Copy to Clipboard button. See chapter 16 for information about using the equipment window.

ii Click on the Paste from Clipboard button in the Endpoint A - Network Element panel of the Physical Link (Create) form. The NE parameter information is displayed in the Endpoint A - Network Element panel.

6 Configure the parameters in the Endpoint B panel by performing one of the following.

a If you set the Endpoint B Type parameter in step 2 to Port, go to step 7.

b If you set the Endpoint B Type parameter in step 2 to Network Element, go to step 8.

c If you set the Endpoint B Type parameter in step 2 to Unmanaged NE, go to step 10.

7 Configure the parameters in the Endpoint B - Port panel by performing one of the following.

a Use the Select Endpoint B - Port - Physical Link form to search for a port.

i Click on the Select button in the Endpoint B panel to choose a managed endpoint for the physical link. The Select Endpoint B - Port - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of ports.

iii Select a port and click on the OK button. The Select Endpoint B - Port - Physical Link form closes and the port parameter information is displayed in the Endpoint B - Port panel of the Physical Link (Create) form.

b Choose a port from the equipment navigation tree.

i Select a port object and click on the Copy to Clipboard button. The port information is copied to the clipboard.

Alternatively, you can choose a port object from the equipment window and click on the Copy to Clipboard button. See chapter 16 for information about using the equipment window.

ii Click on the Paste from Clipboard button in the Endpoint B - Port panel of the Physical Link (Create) form. The port parameter information is displayed in the Endpoint B - Port panel.

8 Configure the parameters in the Endpoint B - Network Element panel by performing one of the following.

a Use the Select Endpoint B - Network Element - Physical Link form to search for a port.

i Click on the Select button to choose a managed endpoint for the physical link. The Select Endpoint B - Network Element - Physical Link form opens.

ii Use the configurable filter and click on the Search button to generate a list of NEs.

iii Select an NE and click on the OK button. The Select Endpoint B - Network Element - Physical Link form closes and the NE parameter information is displayed in the Endpoint B - Network Element panel of the Physical Link (Create) form.

b Choose an NE from the equipment navigation tree:

i Select an NE and click on the Copy to Clipboard button. The NE information is copied to the clipboard.

Alternatively, you can choose an NE from the equipment window and click on the Copy to Clipboard button. See chapter 16 for information about using the equipment window.

ii Click on the Paste from Clipboard button in the Endpoint B - Network Element panel of the Physical Link (Create) form. The NE parameter information is displayed in the Endpoint B - Network Element panel.

9 If the Endpoint B is an unmanaged NE that the 5620 SAM recognizes as an unmanaged mobile NE such as an eNodeB, go to step 12.

10 Configure the parameters in the Endpoint B - Unmanaged NE panel:

- Unmanaged - Name
- Unmanaged - Management Address
- Unmanaged - Description

Note — If the 5620 SAM is to manage endpoint B, configure the Unmanaged - Name parameter with the management IP address of the unmanaged NE.

When the 5620 SAM discovers the NE, the unmanaged endpoint of the physical link is updated with the newly managed NE on the topology map.

11 Go to step 15.

12 Click on the Select button in the Endpoint B - Unmanaged NE (LTE) panel to choose an unmanaged mobile NE such as an eNodeB. The Select Unmanaged NE - Physical Link form opens.

13 Use the configurable filter and click on the Search button to generate a list of unmanaged mobile NEs for example, eNodeBs.

14 Select an unmanaged mobile NE and click on the OK button. The Select Unmanaged NE - Physical Link form closes and the NE information is displayed in the Endpoint B - Unmanaged NE (LTE) panel of the Physical Link (Create) form.

15 Click on the OK button to close the form. The physical link is created between the two endpoints and can be viewed from the physical topology map.

Procedure 4-37 To modify a physical link and create physical links with the same parameter settings

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Physical Link from the object drop-down list.

3 Configure the filter criteria and click on the Search button.

4 Select a physical link in the list and click on the Properties button. The Physical Link (Edit) form opens.

5 Modify the parameters as required.

6 Click on the Apply button to save the changes.

7 If required, click on the Copy button to create more physical links based on the same parameter information. A Physical Link (Create) form opens with the existing parameter information.

8 Edit the parameter information as required.

9 Click on the OK button. The Physical Link (Create) form closes.

10 Close the Physical Link (Edit) form.

After a physical link is created, you can view the link on the physical topology map.

Procedure 4-38 To delete a physical link

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Physical Link from the object drop-down list.

3 Configure the filter criteria and click on the Search button.

4 Select a physical link in the list and click on the Delete button. A dialog box appears.

5 Click on the Yes button to proceed. The physical link is deleted.

Note — When a NE is unmanaged or removed, all the physical links that terminate on the ports or on the NE itself are deleted.

Procedure 4-39 To configure bandwidth availability on physical links

Use this procedure to configure bandwidth parameters on links being used by service CAC.

Note — This capability is only available if service CAC has been configured. See chapter 5 for information about enabling and disabling service CAC.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Perform one of the following.

   a Choose Discovered Physical Link from the object drop-down menu.

   b Choose Physical Link from the object drop-down menu.

3 Configure the filter criteria and click on the Search button.

4 Select a physical link in the list and click on the Properties button. The Physical Link (Edit) form opens.

5 Click on the Bandwidth tab button.

6 Select the Endpoint A or the Endpoint B tab.

7 Configure the following endpoint bandwidth parameters:

- Bandwidth (Mbps)
- Used Bandwidth (Mbps)
- Utilization Threshold (%)

8 Configure the following effective bandwidth parameters:

- Name
- Bandwidth (Mbps)
- Booking Factor (%)
- Utilization Threshold (%)
- Used Bandwidth (Mbps)

9 To view a summary of bandwidth usage for all tunnels and services currently using the physical link, click on the Bandwidth Usage tab button.

10 Click on the OK button. The Physical Link (Edit) form closes.

11 Close the Manage Equipment form.

Procedure 4-40 To view and modify discovered physical link properties

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Discovered Physical Link from the object drop-down list.

3 Configure the filter criteria and click on the Search button.

4 Select the required discovered physical link in the list and click on the Properties button. The Discovered Physical Link (Edit) form opens with the General tab page displayed.

5 Configure the following parameters, if required:

- Name
- Description

6 Select the appropriate tab to view the information you require.

7 Click on the OK button. The Discovered Physical Link (Edit) form closes.

8 Close the Manage Equipment form.

5620 SAM system management

5 — 5620 SAM component configuration

5.1 5620 SAM component configuration overview

A 5620 SAM system may occasionally require a configuration change. The procedures in this chapter describe how to perform operations such as the following on the components in a 5620 SAM system:

- changing a component IP address or hostname
- adding a 5620 SAM database, server, or client
- updating a license key to accommodate new software modules or equipment
- changing the configuration of all 5620 SAM GUI clients
- implementing secure communication in a 5620 SAM cluster

Note 1 — You can also change the configuration of a 5620 SAM component such as a database, server, or client using the 5620 SAM installation software, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

Note 2 — This chapter does not describe how to configure SSL on a 5620 SAM component. See chapter 9 for information about configuring 5620 SAM SSL.

You can use the 5620 SAM auto-client update function to reconfigure multiple 5620 SAM clients. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about using auto-client update to perform a client update. See Procedure 5-7 for information about performing global auto-client updates.

5.2 Software configuration procedures

The following procedures describe how to view and change the general 5620 SAM software configuration.

Procedure 5-1 To view the 5620 SAM software release, license key, and system information

Perform this procedure to display information about the installed 5620 SAM software release, license capacity, and system configuration.

1 Perform one of the following.

a View the software release information; perform the following steps.

i Choose Help→About 5620 SAM from the 5620 SAM main menu. The About the 5620 SAM Client Application form opens.

ii Review the software release information. The build information specifies the release of the 5620 SAM software installed, for example, Release 8.0 R1, where 8.0 is the major release identifier, and R1 is the minor release identifier.

b View the 5620 SAM license information; perform the following steps.

i Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens with the General tab displayed.

ii Review the software license information, which includes the following:

- customer name and the active license key value
- host name and IP address of the main server
- number of supported operator positions
- status of the primary and standby servers
- supported 5620 SAM modules and packages
- redundancy configuration information for redundant Solaris installations

iii Click on the Devices and Quantities Licensed tab button.

iv Review the software license information, which includes the following:

- device information that includes the following:
  - quantity licensed
  - quantity consumed
  - quantity remaining
- card and daughter card information that includes the following:
  - quantity licensed
  - quantity consumed
  - quantity remaining

Note — A highlighted entry is alarmed. You can double-click on an alarmed entry to view the alarm details.

c View the 5620 SAM main server and database redundancy information, if applicable; perform the following steps.

i Choose Administration→System Information. The System Information form opens.

ii Review the redundancy information, which includes:

- whether redundancy is enabled in the 5620 SAM management domain
- the IP addresses, host names, and statuses of the 5620 SAM main servers
- the IP addresses, host names, database names, and instance names of the 5620 SAM databases

iii Click on the Auxiliary Servers tab button to view the 5620 SAM auxiliary server IP addresses, host names, port numbers, server roles, and status information.

iv Click on the Faults tab button to view redundancy and system alarm information, if required.

2 Close the open forms.

Procedure 5-2 To export license information to a file

You can export the license information as text to a file storage location. This text file can be sent to Alcatel-Lucent to provide information about your system.

1 Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens.

2 Click on the Export License information to file button. A Save as form opens.

3 Use the form to specify a name, location, and format for the file that contains the exported license information.

Note — License key files can be saved in either HTML or Text format.

4 Click on the Save button. The license key file is saved to the specified location.

5 Close the 5620 SAM License (Edit) form.

Procedure 5-3 To verify that the required 5620 SAM software modules are installed

The 5620 SAM functions are provided by the following modules that are specified as enabled or disabled in the 5620 SAM license key:

- 5620 SAM-E for device mediation, equipment management, security, CLI access to managed devices, backup and restore, equipment navigation, alarm policy management, real-time equipment statistics, and inventory and reporting
- 5620 SAM-P for service provisioning, templates, and network tunnel, path, customer, subscriber, and policy management
- 5620 SAM-A for service assurance functions, fault correlation using alarms, OAM tools, topology views, statistics policies and historical statistical data, and accounting policies and data

- 5620 SAM-O for the XML open interface
- Mobile Services Package for LTE functions

Note — The 5620 SAM-E module is enabled By default. You cannot install and run other modules without installing the 5620 SAM-E.

If a module or package is not installed, you cannot use the client GUI to perform the functions associated with the module or package.

1 Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens with the General tab displayed.

2 View the options in the 5620 SAM Modules and Packages Licensed panel. If a module or package is not selected, it is not enabled in the license key.

3 Verify that the required software modules are installed.

If you cannot perform a function using the client GUI and you have sufficient user privileges on a managed device, you can use a CLI on the device to perform the function.

4 View the other license key information, as required.

5 Close the 5620 SAM License (Edit) form.

Procedure 5-4 To change the license key in a standalone 5620 SAM system

Perform this procedure to update the 5620 SAM license information for a standalone 5620 SAM system.

A 5620 SAM license key is generated based on multiple parameters such as the platform type, the software release, and the required number of GUI clients and managed MDAs. When a license key parameter changes, a new license key is required.

Note 1 — The Solaris command lines in this procedure use the # symbol to represent the CLI prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

Note 2 — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

1 Log in to the main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<license
```

This section of the file contains the 5620 SAM license information that is configured in the following steps.

6 Replace the existing license key value between the quotation marks in the following line with the updated license key value in the following format:

key="*XXXXX-XXXXX*"

7 Ensure that the customer name provided with the new license key exactly matches the existing customer name. If required, update the customer name between the quotation marks in the following line with the new customer name:

customerName="*customer_name*"

where *customer_name* is the case-sensitive customer name value received with the updated license key

8 Save and close the nms-server.xml file.

9 Open a console window.

10 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin on a Solaris station or C:\5620sam\server\nms\bin on a Windows station.

11 Perform one of the following.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash read_config ↵
```

b If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat read_config ↵
```

The main server reads the nms-server.xml file and the additional functionality defined in the updated license key is enabled.

12 Perform one of the following to display the updated license information.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash nms_status ↵
```

b If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat nms_status ↵
```

The main server displays status information.

13 Review the information in the 5620 SAM License Information section of the command output to ensure that it is correct.

14 If one or more license parameters are incorrect, contact Alcatel-Lucent technical support for assistance.

Procedure 5-5 To change the license key in a redundant 5620 SAM system

Perform this procedure to update the 5620 SAM license information for a redundant 5620 SAM system.

A 5620 SAM license key is generated based on multiple parameters such as the platform type, the software release, and the required number of GUI clients and managed MDAs. When a license key parameter changes, a new license key is required.

In a redundant 5620 SAM system, the primary and standby main server license key parameters must be identical, except for the primary and standby main server station host IDs.

Caution — The primary and standby main server license keys must be synchronized to ensure proper 5620 SAM operation in the event of a main server activity switch. The main servers compare license key values when they establish communication or when one main server is performing a read_config operation using the nmsserver.bash script. If a difference in the keys is detected, the 5620 SAM raises an alarm that clears when the license keys are again synchronized.

Note 1 — The Solaris command lines in this procedure use the # symbol to represent the CLI prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

Note 2 — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

Change license key on primary main server

1 Log in to the primary main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<license
```

This section of the file contains the 5620 SAM license information that is configured in the following steps.

6 Replace the existing license key value between the quotation marks in the following line with the updated license key value in the following format:

```
key="XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXX
XX-XXXXX-XXXXX-XXXXX"
```

7 Ensure that the customer name provided with the new license key exactly matches the existing customer name. If required, update the customer name between the quotation marks in the following line with the new customer name:

```
customerName="customer_name"
```

where *customer_name* is the case-sensitive customer name value received with the updated license key

8 Save and close the nms-server.xml file.

9 Open a console window.

10 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

11 If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file, the license information is updated, and the additional functionality defined in the updated license key is enabled.

12 Enter the following at the prompt to verify the updated license information:

```
# ./nmsserver.bash nms_status ↵
```

The main server displays status information.

13 Review the 5620 SAM License Information section of the command output to ensure that the license parameters are correct.

Note — The license information that is displayed is associated with the local main server.

14 Keep the console window open. It is used later in the procedure.

Change license key on standby main server

15 Log in to the standby main server station as the samadmin user.

16 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

17 Create a backup copy of the nms-server.xml file.

18 Open the nms-server.xml file using a plain-text editor.

19 Locate the following XML tag:

```
<license
```

This section of the file contains the 5620 SAM license information that is configured in the following steps.

20 Replace the existing license key value between the quotation marks in the following line with the updated license key value in the following format:

```
key="XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXX
XX-XXXXX-XXXXX-XXXXX"
```

21 Ensure that the customer name provided with the new license key exactly matches the existing customer name. If required, update the customer name between the quotation marks in the following line with the new customer name:

```
customerName="customer_name"
```

where *customer_name* is the case-sensitive customer name value received with the updated license key

22 Save and close the nms-server.xml file.

23 Open a console window.

24 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

25 Enter the following at the prompt:

```
# ./nmsserver.bash force_restart ↵
```

The main server restarts using the updated license information, and the additional functionality defined in the updated license key is enabled.

26 Enter the following at the prompt to verify the updated license information:

```
# ./nmsserver.bash nms_status ↵
```

The main server displays status information.

27 Review the 5620 SAM License Information section of the command output to ensure that the license parameters are correct.

Note — The license information that is displayed is associated with the local main server.

28 Compare the standby main server license information to the active main server information displayed in step 13 to ensure that it is the same.

29 If the active and standby license parameters do not match, contact Alcatel-Lucent technical support for assistance.

Procedure 5-6 To enable 5670 RAM support

Perform this procedure to enable the 5670 RAM function on a 5620 SAM system.

1 Log in to the appropriate main server station as a user with local administrator privileges.

Note 1 — In a redundant deployment, you must log in to the primary main server station.

Note 2 — If the main server is installed on Solaris, you must log in as the samadmin user.

2 Navigate to the server configuration directory, which is typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following section:

```
<ram5670
        ramEnabled="false" />
```

6 Change "false" to "true".

7 Save and close the nms-server.xml file.

8 Perform one of the following.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash read_config ↵
```

b If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat read_config ↵
```

The main server reads the nms-server.xml file and the new support settings are put into effect.

9 Log off the server.

10 If it is a redundant system, log in to the standby main server station as the samadmin user. Otherwise, go to step 13.

11 Navigate to the server configuration directory, which is typically /opt/5620sam/server/nms/config, then perform steps 3 to 7.

12 Restart the standby main server:

```
cd /opt/5620sam/server/nms/bin/nmsserver.bash force_restart ↵
```

13 Restart each auxiliary server in the 5620 SAM system.

5.3 System configuration procedures

The following procedures describe how to configure system parameters that define the connections between 5620 SAM components.

Procedure 5-7 To change the global 5620 SAM client configuration using the auto-client update utility

Perform this procedure to modify the base configuration of each 5620 SAM GUI client that connects to a specific 5620 SAM main server.

Note 1 — You can exclude a specific 5620 SAM client from a global configuration change by using a command-line option when you open the client GUI, as described in chapter 2.

Note 2 — Do not use this procedure to configure SSL for 5620 SAM clients. Use the appropriate SSL configuration procedures in chapter 9 to configure SSL.

Note 3 — The Solaris command lines in this procedure use the # symbol to represent the CLI prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

Note 4 — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

1 Log in to the 5620 SAM main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

2 If required, modify the appropriate server configuration file. For example, update the nms-server.xml file with a new user documentation location in the event that the location is changed.

3 Perform one of the following to update a client configuration file on the main server with the server configuration change. For example, update the nms-client.xml file with a new user documentation location.

   a If the main server is installed on Solaris, modify the appropriate configuration file in the *install_dir*/nms/config/clientDeploy directory

   where *install_dir* is the server installation location, typically /opt/5620sam/server

   b If the main server is installed on Windows, modify the appropriate configuration file in the *install_dir*\nms\config\clientDeploy directory

   where *install_dir* is the server installation location, typically C:\5620sam\server

4 Open a console window.

5 Perform one of the following to enable an update notification for clients that connect to the server and to prepare the client configuration files for download.

   a If the main server is installed on Solaris, enter the following at the prompt:

   # *install_dir*/bin/nmsdeploytool.bash deploy ↵

   where *install_dir* is the server installation location, typically /opt/5620sam/server

   b If the main server is installed on Windows, enter the following at the prompt:

   _install_dir_\bin\nmsdeploytool.bat deploy ↵

   where *install_dir* is the server installation location, typically C:\5620sam\server

6 Perform one of the following on each 5620 SAM single-user GUI client station and client delegate server station.

Note — When you perform this step on a client delegate server, you affect each GUI client that connects through the client delegate server.

   a Update the client configuration by restarting the client GUI. The client automatically backs up the current configuration and applies the configuration change.

Note — On a client delegate server station, you must start the client software as the root user or the configuration update fails.

   A Solaris client stores the backup of the current configuration in the *install_dir*/nms/configBackup directory

   where *install_dir* is the client installation location, typically /opt/5620sam/client

A Windows client stores the backup of the current configuration in the *install_dir*\nms\configBackup directory

where *install_dir* is the client installation location, typically C:\5620sam\client

b Preserve the current client configuration when the client GUI starts by specifying a startup option that disables the auto-client update function. See chapter 2 for information about 5620 SAM client startup options.

Note — Specifying a client startup option affects only the current GUI session. To ensure that the client configuration is not updated automatically during a subsequent session, you must open the session using the startup option that disables the auto-client update.

Procedure 5-8 To configure a client GUI login form to display multiple server options

Perform this procedure to enable the users of a specific 5620 SAM client GUI to choose the 5620 SAM main server to which they connect.

Note 1 — You cannot configure a client delegate server to display multiple server options on the client login form. If you require client connections to multiple 5620 SAM servers through a client delegate server, you must install one 5620 SAM client delegate software instance for each 5620 SAM server.

Note 2 — The 5620 SAM auto-client update function overrides the nms-client.xml configuration changes that are specified in this procedure. If the nms-client.xml file on a main server changes, it overwrites the local client copy the next time the client connects to the server, unless a client startup option is used to prevent it. For information about using client startup options, see chapter 2.

Alcatel-Lucent recommends that you use the 5620 SAM auto-client update function described in chapter 5 to modify the 5620 SAM client configuration.

1 Click on Application→Exit to close the 5620 SAM client GUI, if it is open. The client GUI closes.

2 Navigate to the client installation configuration directory, typically C:\5620sam\client\nms\config on Windows or /opt/5620sam/client/nms/config on Solaris.

3 Open the nms-client.xml file using a text editor.

4 Find the lines starting with <j2ee> and <systemMode>. By default, the IP address and port information of the standalone or redundant servers, as configured during installation, are displayed.

5 For each standalone server or server redundant pair you want displayed on the client GUI login form, perform the following:

i Copy the entire <j2ee> and <systemMode> sections of the file.

ii Paste the <j2ee> and <systemMode> sections after the previous section.

iii Modify the ejbServer IP address to the IP address or hostname of the server you want displayed during client GUI login.

iv Modify the nameOne (for standalone) or nameOne and nameTwo (for redundant) parameters to indicate the domain name and hostname of the server, for easier identification by operators. This name does not have to be the hostname of the server domain. In some cases, the name may be the same for the active and standby server in a redundant server domain. The name is not automatically derived from a host lookup.

Note — Common hostname naming restrictions apply to the nameOne and nameTwo fields. You cannot use the following special characters:

- !
- #
- $
- %
- &
- (
-)
- +

v Save the changes and close the file.

6 Log in to the client GUI. The new server options are displayed in the Server drop-down menu.

Procedure 5-9 To change the default GUI preference and table layout, script result, or log file location on a client delegate server

Perform this procedure to customize the default file location for one or more of the following on a 5620 SAM client delegate server:

- user-defined GUI preferences:
  - saved table layouts
  - preferences saved using Application→Save Workspace
- script result files
- client log files

1 Close each 5620 SAM client that connects to the main server through the client delegate server by choosing Application→Exit from the 5620 SAM main menu.

2 Log in to the client delegate server station as the samadmin user.

3 Open a console window.

4 Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config.

5 To change the default saved GUI preferences and table layout file location:

i Open the nms-client.xml file using a plain-text editor.

ii Insert the following section directly above the </configuration> line at the end of the file:

```
<guiPreferences
        path="new_file_location"
    />
```

where *new_file_location* is the new default saved GUI table layout and GUI preferences file location

Note — The specified location can be an absolute file path or a file path relative to *install_dir*/nms, where *install_dir* is the client installation location, typically /opt/5620sam/client.

iii Save and close the nms-client.xml file. Subsequent 5620 SAM client sessions on the client delegate server save the GUI preferences and table layouts to files in the new location.

6 To change the default script result file location:

i Open the nms-client.xml file using a plain-text editor.

ii Insert the following section directly above the </configuration> line at the end of the file:

```
<cache
        directoryName="new_file_location"
    />
```

where *new_file_location* is the new default script result file location

Note — The specified location can be an absolute file path or a file path relative to *install_dir*/nms, where *install_dir* is the client installation location, typically /opt/5620sam/client.

iii Save and close the nms-client.xml file. Subsequent 5620 SAM client sessions on the client delegate server save the script results to files in the new location.

7 To change the default log file location:

i Open the nms-client-log4j.xml file using a plain-text editor.

ii Locate the following line:

```
 <param name="File"
value="${nms.logdirectory}/EmsClient.log"/>
```

iii Edit the line to read:

```
 <param name="File"
value="new_file_location/EmsClient.log"/>
```

where *new_file_location* is the new log file location

Note — The specified location must be an absolute file path.

iv Save and close the nms-client-log4j.xml file. Subsequent 5620 SAM client sessions on the client delegate server save the log files to files in the new location.

Procedure 5-10 To change the IP addresses in a collocated standalone 5620 SAM system

Perform this procedure when the main server/database station in a collocated standalone 5620 SAM system requires a different IP address, for example, when the management network topology changes.

Caution — The 5620 SAM system is out of service during part of this procedure. Perform this procedure only during a scheduled maintenance window.

Note — Command-line examples use the following to represent the Solaris CLI prompts:

- #—represents the prompt displayed for the root or samadmin user
- bash$—represents the prompt displayed for the Oracle management user

Do not type the # symbol or bash$ when entering a command.

1 Ensure that the 5620 SAM DVD-ROM used to install the 5620 SAM software is available.

2 Alcatel-Lucent strongly recommends that you back up the 5620 SAM database in advance of a system configuration change. Perform one of the following to back up the database.

a Use the 5620 SAM client GUI. See chapter 7 for information about performing database backups using the client GUI.

b Use a CLI script.

i Log in the main server/database station as the Oracle management user.

ii Open a console window.

iii Enter the following at the prompt to begin the database backup:

```
bash$ install_dir/install/config/samdb/SAMbackup.sh
backup_dir ↵
```

where
install_dir is the database installation location, typically /opt/5620sam/samdb
backup_dir is the directory that is to contain the database backup

3 Copy the database backup files from the backup directory specified in step 2 b iii to a secure location, such as a non-5620 SAM station, for safekeeping.

4 Disable the 5620 SAM server startup daemon.

i Enter the following at the prompt to switch to the root user.

```
bash$ su - ↵
```

ii Enter the following at the prompt to navigate to the /etc/rc3.d directory.

```
# cd /etc/rc3.d ↵
```

iii Enter the following at the prompt to disable the server startup daemon by renaming it:

```
# mv S975620SAMServerWrapper
inactive.S975620SAMServerWrapper ↵
```

iv Enter the following at the prompt to switch back to the Oracle management user:

```
# exit ↵
```

5 Stop the main server application. After this step, the 5620 SAM main server is not managing the network.

i Enter the following at the prompt to switch to the samadmin user.

```
bash$ su — samadmin ↵
```

ii Navigate to the server configuration directory. Enter the following at the prompt:

```
# cd install_dir/nms/bin ↵
```

where *install_dir* is the server installation location, typically /opt/5620sam/server

iii Enter the following at the prompt:

```
# ./nmsserver.bash stop ↵
```

iv Verify that the main server is stopped. Enter the following at the prompt:

```
# ./nmsserver.bash appserver_status ↵
```

v The server application is stopped when the command in step 5 iv returns the following text string:

```
Application Server is stopped
```

If the command returns anything other than the above text string, wait five minutes and repeat step 5 iv. Do not proceed unless the console displays the above text.

6 Enter the following at the CLI prompt to switch back to the Oracle management user:

```
# exit ↵
```

7 Enter the following at the prompt to switch to the root user.

```
bash$ su - ↵
```

8 Use a Solaris utility to change the IP address of the main server/database station to the new value.

9 Perform the following steps to change the database IP address.

i Enter the following at the prompt to switch back to the Oracle management user:

```
# exit ↵
```

ii Navigate to the database configuration directory. Enter the following at the prompt:

```
bash$ cd install_dir/install/config/samdb/ ↵
```

where *install_dir* is the database installation location, typically /opt/5620sam/samdb

iii Enter the following at the prompt:

```
bash$ ./changeIPAddress.sh old_IP_address new_IP_address ↵
```

where
old_IP_address is the old 5620 SAM database IP address
new_IP_address is the new 5620 SAM database IP address

10 Enter the following at the prompt to switch to the root user.

```
bash$ su - ↵
```

11 Navigate to the Solaris directory on the 5620 SAM software DVD-ROM. Enter the following at the prompt:

```
# cd /drive ↵
```

where *drive* is the DVD drive mount point

12 Perform one of the following to open the 5620 SAM server installer.

a On a Sun SPARC station:

i Enter the following at the CLI prompt:

```
# cd Solaris ↵
```

ii Enter the following at the CLI prompt:

```
# ./ServerInstall_SAM_R_r_revision.bin ↵
```

where
revision is the revision identifier, such as R1, R3, or another descriptor

b On a Sun X86-based station:

i Enter the following at the CLI prompt:

```
# cd Solarisx86 ↵
```

ii Enter the following at the CLI prompt:

```
# ./ServerInstall_x86_SAM_R_r_revision.bin ↵
```

where
R is the major release identifier, for example, 8
r is the minor release identifier, for example, 0
revision is the revision identifier, such as R1, R3, or another descriptor

A splash screen opens, and then the Introduction panel is displayed.

13 Click on the Next button in each panel until the Choose Installation Type panel appears.

14 Choose Main Server Configuration.

15 Click on the Next button until a panel that contains IP address information is displayed.

16 Enter the new IP address information, as required.

17 Repeat steps 15 and 16 until the final panel, which displays a Done button, appears.

18 Click on the Done button to close the 5620 SAM server configuration utility.

19 Enable the 5620 SAM server startup daemon.

i Navigate to the /etc/rc3.d directory. Enter the following at the prompt:

```
# cd /etc/rc3.d ↵
```

ii Enter the following at the prompt to rename the server startup daemon using the original name:

```
# mv inactive.S975620SAMServerWrapper
S975620SAMServerWrapper ↵
```

20 Enter the following at the prompt to switch to the samadmin user.

```
# su – samadmin ↵
```

21 Enter the following at the prompt to start the main server:

```
# install_dir/nms/bin/nmsserver.bash start ↵
```

where *install_dir* is the server installation location, typically /opt/5620sam/server

The main server starts. Initial server startup may take twenty minutes or more to complete. You do not need to wait for the server to start before performing the next step.

22 Configure each 5620 SAM single-user GUI client and client delegate server to use the new main server IP address.

i Log in to the single-user client or client delegate server station.

Note — On a client delegate server station, you must log in as the root user.

ii Open a console window.

iii Navigate to the client configuration directory. Enter the following at the prompt:

```
# cd install_dir/nms/config ↵
```

where *install_dir* is the client installation location, typically /opt/5620sam/client

iv Create a backup copy of the nms-client.xml file.

v Use a plain-text editor to open the nms-client.xml file.

vi Replace all occurrences of the old main server IP address in the file with the new main server IP address.

vii Save and close the nms-client.xml file.

viii Close the console window.

ix Repeat steps 22 i to viii on each additional single-user client and client delegate server station in the 5620 SAM system.

23 Perform the following steps on the main server/database station to verify that the 5620 SAM server is started.

i Enter the following at the CLI prompt:

```
# path/nms/bin/nmsserver.bash -s nms_status ↵
```

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server

The command returns server status information.

If the main server is not completely started, the first line of status information is the following:

```
Main Server is not ready...
```

The 5620 SAM server is completely started when the command returns the following line of output:

```
 -- SAM Server is UP
```

ii If the command output indicates that the server is not completely started, wait five minutes and enter the command again to check the output.

24 Enter the following at the prompt to switch back to the root user:

```
# exit ↵
```

25 Enter the following at the prompt to switch back to the Oracle management user:

```
# exit ↵
```

26 Log out of the main server/database station.

27 Restart each open 5620 SAM client GUI and client delegate server in the 5620 SAM system. When a client restarts, the client configuration is updated with the new IP address.

Procedure 5-11 To change the IP addresses in a collocated redundant 5620 SAM system

Perform this procedure when a new IP address is required by the primary or standby station, or both stations, in a collocated redundant 5620 SAM system; for example, when the management network topology changes.

Caution — The 5620 SAM system loses redundancy and is out of service during part of this procedure. Perform this procedure only during a scheduled maintenance window.

Note — Command-line examples use the following to represent the Solaris CLI prompts:

- #—represents the prompt displayed for the root or samadmin user
- bash$—represents the prompt displayed for the Oracle management user

Do not type the # symbol or bash$ when entering a command.

1 Ensure that the 5620 SAM DVD-ROM used to install the 5620 SAM software is available.

2 Alcatel-Lucent strongly recommends that you back up the 5620 SAM database in advance of a system configuration change. Perform one of the following to back up the database.

a Use the 5620 SAM client GUI. See chapter 7 for information about performing database backups using the client GUI.

b Use a CLI script.

i Log in the primary main server/database station as the Oracle management user.

ii Open a console window.

iii Enter the following at the prompt to begin the database backup:

```
bash$ install_dir/install/config/samdb/SAMbackup.sh
backup_dir ↵
```

where
install_dir is the database installation location, typically /opt/5620sam/samdb
backup_dir is the directory that is to contain the database backup

3 Copy the database backup files from the backup directory specified in step 2 b iii to a secure location, such as a non-5620 SAM station, for safekeeping.

4 Ensure that the primary main server and the primary database are running on one station, and the standby main server and standby database are running on the other station. If this is not the case, for example, the primary main server and the standby database are running on the same station, you must perform a server activity switch or database switchover to align the redundancy roles on the station. See chapter 7 for information about performing a server activity switch.

Reconfigure standby main server/database station

5 Perform the following steps on on the standby main server/database station to disable the 5620 SAM main server startup daemon.

Note — This step disables 5620 SAM system redundancy. Redundancy is not restored until the end of the procedure.

i Log in as the root user on the standby main server/database station.

ii Open a console window.

iii Enter the following at the prompt to navigate to the /etc/rc3.d directory.

```
# cd /etc/rc3.d ↵
```

iv Enter the following at the prompt to disable the server startup daemon by renaming it:

```
# mv S975620SAMServerWrapper
inactive.S975620SAMServerWrapper ↵
```

6 Perform the following steps to stop the main server application on the standby main server/database station.

i Enter the following at the CLI prompt to switch to the samadmin user:

```
# su - samadmin ↵
```

ii Navigate to the server binary directory. Enter the following at the prompt:

```
# cd install_dir/nms/bin ↵
```

where *install_dir* is the server installation location, typically /opt/5620sam/server

iii Enter the following at the prompt:

```
# ./nmsserver.bash stop ↵
```

iv Verify that the main server is stopped. Enter the following at the prompt:

```
# ./nmsserver.bash appserver_status ↵
```

v The server application is stopped when the command in step 6 iv returns the following text string:

```
Application Server is stopped
```

If the command returns anything other than the above text string, wait five minutes and repeat step 6 iv. Do not proceed unless the console displays the above text.

7 Enter the following at the CLI prompt to switch back to the root user:

```
# exit ↵
```

8 Use a Solaris utility to change the IP address of the standby main server/database station to the new value.

9 Run a script on the standby database to change the database IP address.

i Enter the following at the CLI prompt to switch to the Oracle management user:

```
# su - Oracle_management_user_name ↵
```

where *Oracle_management_user_name* is the name of the UNIX account with Oracle management privileges, typically oracle

ii Navigate to the database configuration directory. Enter the following at the prompt:

```
bash$ cd install_dir/install/config/samdb ↵
```

where *install_dir* is the database installation location, typically /opt/5620sam/samdb

iii Enter the following at the prompt:

```
bash$ ./changeIPAddress.sh old_IP_address_primary
new_IP_address_primary ↵

bash$ ./changeIPAddress.sh old_IP_address_standby
new_IP_address_standby ↵
```

where
old_IP_address_primary is the old primary 5620 SAM database IP address
new_IP_address_primary is the new primary 5620 SAM database IP address
old_IP_address_standby is the old standby 5620 SAM database IP address
new_IP_address_standby is the new standby 5620 SAM database IP address

10 Enter the following at the CLI prompt to switch back to the root user:

```
# exit ↵
```

11 Navigate to the Solaris directory on the 5620 SAM software DVD-ROM. Enter the following at the prompt:

```
# cd /drive ↵
```

where *drive* is the DVD drive mount point

12 Perform one of the following on the standby main server/database station to open the 5620 SAM server installer.

a On a Sun SPARC station:

i Enter the following at the CLI prompt:

```
# cd Solaris ↵
```

ii Enter the following at the CLI prompt:

```
# ./ServerInstall_SAM_R_r_revision.bin ↵
```

where
revision is the revision identifier, such as R1, R3, or another descriptor

b On a Sun X86-based station:

i Enter the following at the CLI prompt:

```
# cd Solarisx86 ↵
```

ii Enter the following at the CLI prompt:

```
# ./ServerInstall_x86_SAM_R_r_revision.bin ↵
```

where
R is the major release identifier, for example, 8
r is the minor release identifier, for example, 0
revision is the revision identifier, such as R1, R3, or another descriptor

A splash screen opens, and then the Introduction panel is displayed.

13 Click on the Next button in each panel until the Choose Installation Type panel appears.

14 Choose Main Server Configuration.

15 Click on the Next button until a panel that contains IP address information is displayed.

16 Enter the new IP address information, as required.

17 Repeat steps 15 and 16 until the final panel, which displays a Done button, appears.

18 Click on the Done button to close the 5620 SAM server configuration utility.

Reconfigure primary main server/database station

19 Disable the 5620 SAM server startup daemon on the primary main server/database station.

i Enter the following at the prompt to switch to the root user.

```
bash$ su - ↵
```

ii Navigate to the /etc/rc3.d directory. Enter the following at the prompt:

```
# cd /etc/rc3.d ↵
```

iii Enter the following at the prompt to disable the main server startup daemon by renaming it:

```
# mv S975620SAMServerWrapper
inactive.S975620SAMServerWrapper ↵
```

20 Stop the server application on the primary main server/database station.

i Enter the following at the CLI prompt to switch to the samadmin user:

```
# su - samadmin ↵
```

ii Navigate to the server binary directory. Enter the following at the prompt:

```
# cd install_dir/nms/bin ↵
```

where *install_dir* is the server installation location, typically /opt/5620sam/server

iii Enter the following at the prompt:

```
# ./nmsserver.bash stop ↵
```

iv Verify that the main server is stopped. Enter the following at the prompt:

```
# ./nmsserver.bash appserver_status ↵
```

v The server application is stopped when the command in step 6 iv returns the following text string:

```
Application Server is stopped
```

If the command returns anything other than the above text string, wait five minutes and repeat step 20 iv. Do not proceed unless the console displays the above text.

21 Enter the following at the CLI prompt to switch back to the root user:

```
# exit ↵
```

22 Use a Solaris utility to change the IP address of the primary main server/database station to the new value.

23 Enter the following at the CLI prompt to switch back to the Oracle management user:

```
# exit ↵
```

24 Perform the following steps on the primary main server/database station to change the database IP address.

i Navigate to the database configuration directory. Enter the following at the prompt:

bash$ **cd *install_dir*/install/config/samdb** ↵

where *install_dir* is the database installation location, typically /opt/5620sam/samdb

ii Enter the following at the prompt:

bash$ **./changeIPAddress.sh *old_IP_address_primary* *new_IP_address_primary*** ↵

bash$ **./changeIPAddress.sh *old_IP_address_standby* *new_IP_address_standby*** ↵

where
old_IP_address_primary is the old primary 5620 SAM database IP address
new_IP_address_primary is the new primary 5620 SAM database IP address
old_IP_address_standby is the old standby 5620 SAM database IP address
new_IP_address_standby is the new standby 5620 SAM database IP address

25 Enter the following at the prompt to switch to the root user.

bash$ **su -** ↵

26 Navigate to the Solaris directory on the 5620 SAM software DVD-ROM. Enter the following at the prompt:

cd /*drive* ↵

where *drive* is the DVD drive mount point

27 Perform one of the following to open the 5620 SAM server installer.

a On a Sun SPARC station:

i Enter the following at the CLI prompt:

```
# cd Solaris ↵
```

ii Enter the following at the CLI prompt:

```
# ./ServerInstall_SAM_R_r_revision.bin ↵
```

where
revision is the revision identifier, such as R1, R3, or another descriptor

b On a Sun X86-based station:

i Enter the following at the CLI prompt:

```
# cd Solarisx86 ↵
```

ii Enter the following at the CLI prompt:

```
# ./ServerInstall_x86_SAM_R_r_revision.bin ↵
```

where
R is the major release identifier, for example, 8
r is the minor release identifier, for example, 0
revision is the revision identifier, such as R1, R3, or another descriptor

A splash screen opens, and then the Introduction panel is displayed.

28 Click on the Next button in each panel until the Choose Installation Type panel appears.

29 Choose Main Server Configuration.

30 Click on the Next button until a panel that contains IP address information is displayed.

31 Enter the new IP address information, as required.

32 Repeat steps 30 and 31 until the final panel, which displays a Done button, appears.

33 Click on the Done button to close the 5620 SAM server configuration utility.

34 Perform the following steps to enable the 5620 SAM main server startup daemon on the primary main server/database station.

i Navigate to the /etc/rc3.d directory. Enter the following at the prompt:

```
# cd /etc/rc3.d ↵
```

ii Enter the following at the prompt to rename the server startup daemon using the original name:

```
# mv inactive.S975620SAMServerWrapper
S975620SAMServerWrapper ↵
```

35 Enter the following at the CLI prompt to switch to the samadmin user:

```
# su - samadmin ↵
```

36 Enter the following at the prompt to start the primary main server:

```
# install_dir/nms/bin/nmsserver.bash start ↵
```

where *install_dir* is the server installation location, typically /opt/5620sam/server

The main server starts. Initial server startup may take twenty minutes or more to complete. You do not need to wait for the server to start before performing the next step.

37 Configure each 5620 SAM single-user GUI client and client delegate server to use the new main server IP addresses.

i Log in to the single-user client or client delegate server station.

Note — On a client delegate server station, you must log in as the root user.

ii Open a console window.

iii Navigate to the client configuration directory. Enter the following at the prompt:

```
# cd install_dir/nms/config ↵
```

where *install_dir* is the client installation location, typically /opt/5620sam/client

iv Create a backup copy of the nms-client.xml file.

v Use a plain-text editor to open the nms-client.xml file.

vi Replace all occurrences of the old primary main server IP address in the file with the new primary main server IP address.

vii Replace all occurrences of the old standby main server IP address in the file with the new standby main server IP address.

viii Save and close the nms-client.xml file.

ix Close the console window.

x Repeat steps 37 i to ix on each client station.

38 Perform the following steps on the primary main server/database station to verify that the 5620 SAM main server is started.

i Enter the following at the CLI prompt:

```
# path/nms/bin/nmsserver.bash -s nms_status ↵
```

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server

The command returns server status information.

If the main server is not completely started, the first line of status information is the following:

```
Main Server is not ready...
```

The 5620 SAM server is completely started when the command returns the following line of output:

```
 -- Primary Server is UP
```

ii If the command output indicates that the main server is not completely started, wait five minutes and enter the command again to check the output.

39 When the primary main server is started, enter the following at the prompt to switch back to the root user.

exit ↵

40 Enter the following at the prompt to switch back to the Oracle management user.

exit ↵

41 Log out of the primary main server/database station.

42 Perform the following steps on the standby main server/database station to enable the 5620 SAM server startup daemon.

i Enter the following at the prompt to navigate to the /etc/rc3.d directory:

cd /etc/rc3.d ↵

ii Enter the following at the prompt to enable the server startup daemon by renaming it using the original name:

mv inactive.S975620SAMServerWrapper S975620SAMServerWrapper ↵

43 Enter the following at the CLI prompt to switch to the samadmin user:

su - samadmin ↵

44 Enter the following at the prompt to start the standby main server:

***install_dir*/nms/bin/nmsserver.bash start** ↵

where *install_dir* is the server installation location, typically /opt/5620sam/server

The standby main server starts. Initial server startup may take twenty minutes or more to complete.

45 Log out of the standby main server/database station.

46 Restart each open 5620 SAM client GUI and client delegate server in the 5620 SAM system. When a client restarts, the client configuration is updated with the new IP address.

Procedure 5-12 To change the IP address of a client delegate server

Perform this procedure when a client delegate server is assigned a new IP address.

Note — You must perform this procedure on each main server in the 5620 SAM system.

1 Close each 5620 SAM client that connects to the main server through the client delegate server by choosing Application→Exit from the 5620 SAM main menu.

2 Use a Solaris utility to change the IP address of the client delegate server station to the new value.

3 Log in to the main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

4 Open a console window.

5 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config on a Solaris station, or C:\5620sam\server\nms\config on a Windows station.

6 Open the nms-server.xml file using a plain-text editor.

7 Locate the following section, which lists the IP addresses of two client delegate servers as an example:

```
<clientDelegateServer
        enabled="true"
        ipAddresses="IP_address_1,IP_address_2"
/>
```

8 Update the IP addresses, as required.

9 Save and close the nms-server.xml file.

10 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin on a Solaris station or C:\5620sam\server\nms\bin on a Windows station.

11 Perform one of the following.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash read_config ↵
```

b If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat read_config ↵
```

The main server reads the nms-server.xml file and accepts subsequent client sessions from the new IP address of the client delegate server.

5.4 Security configuration procedures

The following procedures describe how to configure secure communication other than SSL between 5620 SAM components.

Note — See chapter 9 for information about configuring SSL on a 5620 SAM component.

Procedure 5-13 To configure HTTP or HTTPS for 5620 SAM GUI client updates

Perform this procedure to create an HTTP or HTTPS configuration on a 5620 SAM main server that is distributed to all 5620 SAM GUI clients. GUI clients use HTTP or HTTPS to download software upgrades and configuration changes from a main server.

Note 1 — You must perform this procedure on each 5620 SAM main server in a redundant deployment.

Note 2 — By default, HTTP is enabled on the 5620 SAM main server and clients, and HTTPS is disabled.

Note 3 — The Solaris command lines in this procedure use the # symbol to represent the CLI prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

Note 4 — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

1 Log in to the main server station as a user with local administrator privileges.

Note — If the server is installed on Solaris, you must log in as the samadmin user.

2 Open a console window.

3 Perform one of the following:

a If the main server is installed on Solaris, navigate to the following directory:

install_dir/nms/jboss/server/jms/deploy/jboss-web.deployer

where *install_dir* is the server installation location, typically /opt/5620sam/server

b If the main server is installed on Windows, navigate to the following directory:

install_dir\nms\jboss\server\jms\deploy\jboss-web.deployer

where *install_dir* is the server installation location, typically C:\5620sam\server

4 Create a backup copy of the server.xml file.

Caution — Do not store the backup copy of the file in the current directory, or the main server startup may be affected. Alcatel-Lucent recommends that you store the backup copy on a non-5620 SAM station.

5 Use a text editor to open the server.xml file.

6 Perform the following steps to enable HTTPS.

i Uncomment the section shown in Code 5-1 by moving the --> tag at the end of the section to the end of the first line.

Code 5-1: Disabled 5620 SAM client HTTPS configuration

```
<!-- SSL/TLS Connector configuration
<Connector port="8444" address="${jboss.bind.address}"
maxThreads="100" acceptCount="20" scheme="https" secure="true"
protocol="HTTP/1.1" SSLEnabled="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/samserver.keystore"
keystorePass="password" sslProtocol="TLS"/>
-->
```

ii Change the keystoreFile value in quotation marks to the path of the keystore file relative to ${jboss.server.home.dir}. The default ${jboss.server.home.dir} value is *install_dir*/nms/jboss/server/jms on Solaris and *install_dir*\nms\jboss\server\jms on Windows

where *install_dir* is the server installation location, typically /opt/5620sam/server on Solaris and C:\5620sam\server on Windows

iii Change the keystorePass value in quotation marks to the keystore password.

After the changes, the section appears as shown in Code 5-2.

Code 5-2: Enabled 5620 SAM client HTTPS configuration

```
<!-- SSL/TLS Connector configuration -->
<Connector port="8444" address="${jboss.bind.address}"
maxThreads="100" acceptCount="20" scheme="https" secure="true"
protocol="HTTP/1.1" SSLEnabled="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}relative_file_path"
keystorePass="password" sslProtocol="TLS"/>
```

7 Save and close the server.xml file.

8 Perform one of the following:

a If the main server is installed on Solaris, navigate to the following directory:

install_dir/nms/config/clientDeploy

where *install_dir* is the server installation location, typically /opt/5620sam/server

b If the main server is installed on Windows, navigate to the following directory:

install_dir\nms\config\clientDeploy

where *install_dir* is the server installation location, typically C:\5620sam\server

9 Create a backup copy of the nms-client.xml file.

Caution — Do not store the backup copy of the file in the current directory, or the main server startup may be affected. Alcatel-Lucent recommends that you store the backup copy on a non-5620 SAM station.

10 Use a text editor to open the nms-client.xml file.

11 Change the commandPort value shown in Code 5-3 from “8085” to “8444”.

Code 5-3: j2ee section of nms-client.xml before modification

```
<configuration>
<j2ee
ejbServerType="Jboss"
ejbServerHost="192.168.213.117"
ejbServerPort="1099"
commandPort="8085"
commandSecure="false"
jmsTopicName="5620-THIN-SAM-topic" />
```

Caution — Although the 5620 SAM client software subsequently uses port 8444, port 8085 on the main server remains open. For greater security, ensure that you disable port 8085 in the main server OS configuration if no other applications require it.

12 Change the commandSecure value from “false” to “true”. The section reads as shown in Code 5-4.

Code 5-4: j2ee section of nms-client.xml after modification

```
<configuration>
<j2ee
ejbServerType="Jboss"
ejbServerHost="192.168.213.117"
ejbServerPort="1099"
commandPort="8444"
commandSecure="true"
jmsTopicName="5620-THIN-SAM-topic" />
```

13 The Help→5620 SAM User Documentation menu option in the client GUI can be configured to open a local copy of the 5620 SAM documentation or a central copy on the main server. If the GUI clients are configured to open the documentation on the main server using a URL, you must update the URL to specify HTTPS.

Perform the following steps to update the documentation URL for all clients.

i Change "http:" in the location value shown in Code 5-5 to "https:".

ii Change "8085" in the location value shown in Code 5-5 to "8444".

Code 5-5: 5620 SAM user documentation URL for HTTP

```
<documentation
install="false"
location="http://192.168.200.221:8085" />
```

Caution — Although the 5620 SAM client software subsequently uses port 8444, port 8085 on the main server remains open. For greater security, ensure that you disable port 8085 in the main server OS configuration if no other applications require it.

The location reads as shown in Code 5-6.

Code 5-6: 5620 SAM user documentation URL for HTTPS

```
 <documentation
            install="false"
            location="https://192.168.200.221:8444" />
```

14 Save and close the nms-client.xml file.

15 Run the script that prepares the SSL configuration update for automatic distribution to clients.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# install_dir/nms/bin/nmsdeploytool.bash deploy ↵
```

where *install_dir* is the server installation location, typically /opt/5620sam/server

b If the main server is installed on Windows, enter the following at the prompt:

```
install_dir\nms\bin\nmsdeploytool.bat deploy ↵
```

where *install_dir* is the server installation location, typically C:\5620sam\server

16 To enable SSL on a 5620 SAM single-user client or client delegate server, you must restart the client to download the SSL configuration from the main server. Because the main server uses SSL, perform the following steps once on each single-user client or client delegate server station to configure SSL.

i Log in to the single-user client or client delegate server station.

Note — On a client delegate server station, you must log in as the root user.

ii Open a console window.

iii If the client software is installed on Solaris, enter the following at the prompt to start the client and to specify the use of HTTPS for the client file download:

```
# install_dir/nms/bin/nmsclient.bash secure server
server:8444 ↵
```

where
install_dir is the client installation location, typically /opt/5620sam/client
server is the IP address or the DNS name of the main server that has SSL enabled

iv If the client is installed on Windows, enter the following at the prompt to start the client and to specify the use of HTTPS for the client file download:

```
install_dir\nms\bin\nmsclient.bat secure server server:8444 ↵
```

where
install_dir is the client installation location, typically C:\5620sam\client
server is the IP address or the DNS name of the main server that has SSL enabled

The client downloads the SSL configuration. Subsequent client sessions use SSL and HTTPS by default.

17 For greater security, Alcatel-Lucent recommends that you disable HTTP on a 5620 SAM main server when HTTPS is enabled. Perform the following steps to disable HTTP on the main server, if required.

Note — Before you disable HTTP on the main server, ensure that all clients receive the automatic SSL configuration update, as described in step 16.

i Use a text editor to open the server.xml file. This is the same file that you edited in step 5.

ii To disable HTTP, comment the HTTP configuration shown in Code 5-7 by surrounding the < and /> tags with <! -- and --> tags.

Code 5-7: Enabled 5620 SAM client HTTP configuration

```
<Connector port="8085" address="${jboss.bind.address}"
     maxThreads="100" maxHttpHeaderSize="8192"
     emptySessionPath="true" protocol="HTTP/1.1"
```

```
    minSpareThreads="10" enableLookups="false" redirectPort="8444"
    acceptCount="20" connectionTimeout="60"
    disableUploadTimeout="true" />
```

After the change, the section reads as shown in Code 5-8.

Code 5-8: Disabled 5620 SAM client HTTP configuration

```
<!-- <Connector port="8085" address="${jboss.bind.address}"
    maxThreads="100" maxHttpHeaderSize="8192"
    emptySessionPath="true" protocol="HTTP/1.1"
    minSpareThreads="10" enableLookups="false" redirectPort="8444"
    acceptCount="20" connectionTimeout="60"
    disableUploadTimeout="true"/> -->
```

18 Open a console window on the main server station.

19 Perform one of the following to restart the 5620 SAM JMS server:

a If the main server is installed on Solaris, enter the following at the prompt:

```
# install_dir/nms/bin/nmsserver.bash jmsforce_restart
```

where *install_dir* is the server installation location, typically /opt/5620sam/server

b If the main server is installed on Windows, enter the following at the prompt:

```
install_dir\nms\bin\nmsserver.bat jmsforce_restart
```

where *install_dir* is the server installation location, typically C:\5620sam\server

Procedure 5-14 To enable HTTPS for 5620 SAM GUI clients

Perform this procedure to configure 5620 SAM single-user GUI clients and client delegate servers to use HTTPS for the auto-client update communication with a 5620 SAM main server.

Note 1 — In order to successfully complete this procedure, you must ensure that the 5620 SAM main server is configured for HTTPS communication with clients. For more information, see Procedure 5-13.

Note 2 — The Solaris command lines in this procedure use the # symbol to represent the CLI prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

Note 3 — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

1 Ensure that SSL is enabled on the main server to which the clients connect. See chapter 9 for information about enabling SSL on a 5620 SAM main server.

2 Enable SSL on the single-user GUI client and client delegate server stations that connect to the main server. See chapter 9 for information about enabling SSL on 5620 SAM GUI clients.

3 Log in to the main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

4 Open a console window.

5 Perform one of the following:

a If the main server is installed on Solaris, navigate to the following directory:

install_dir/nms/config/clientDeploy

where *install_dir* is the server installation location, typically /opt/5620sam/server

b If the main server is installed on Windows, navigate to the following directory:

install_dir\nms\config\clientDeploy

where *install_dir* is the server installation location, typically C:\5620sam\server

6 Create a backup copy of the nms-client.xml file.

7 Use a text editor to open the nms-client.xml file.

8 Change the commandPort value in the j2ee section shown in Code 5-9 from “8085” to “8444”.

Code 5-9: j2ee section of nms-client.xml file before modification

```
<configuration>
  <j2ee
            ejbServerType="Jboss"
            ejbServerHost="192.168.213.117"
            ejbServerPort="1099"
            commandPort="8085"
            commandSecure="false"
            jmsTopicName="5620-THIN-SAM-topic" />
```

Caution — Although the 5620 SAM client subsequently uses port 8444, port 8085 on the main server remains open. For greater security, ensure that you disable port 8085 in the main server OS configuration if no other applications require it.

9 Change the commandSecure value from “false” to “true”. The j2ee section appears as shown in Code 5-9.

Code 5-10: j2ee section of nms-client.xml file after modification

```
<configuration>
  <j2ee
            ejbServerType="Jboss"
            ejbServerHost="192.168.213.117"
            ejbServerPort="1099"
            commandPort="8444"
            commandSecure="true"
            jmsTopicName="5620-THIN-SAM-topic" />
```

10 Save and close the nms-client.xml file.

11 Run the script that prepares the configuration update for distribution to clients.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# install_dir/nms/bin/nmsdeploytool.bash deploy ↵
```

where *install_dir* is the server installation location, typically /opt/5620sam/server

b If the main server is installed on Windows, enter the following at the prompt:

```
install_dir\nms\bin\nmsdeploytool.bat deploy ↵
```

where *install_dir* is the server installation location, typically C:\5620sam\server

The updated configuration is ready for downloading by the GUI clients.

12 To enable HTTPS on a 5620 SAM single-user GUI client or client delegate server, you must restart the client software so that it can download the HTTPS configuration from the main server. Because HTTPS is not yet configured on the client station, you must perform the following steps once on each client or client delegate server station that connects to the server.

i Log in to the single-user client or client delegate server station.

Note — On a client delegate server station, you must log in as the root user.

ii Open a console window.

iii On a Solaris station, enter the following at the prompt to start the client and to specify the use of HTTPS for the client file download:

```
# install_dir/nms/bin/nmsclient.bash secure server
server:8444 ↵
```

where
install_dir is the client installation location, typically /opt/5620sam/client
server is the IP address or the DNS name of the main server that has SSL enabled

iv On a Windows station, enter the following at the prompt to start the client and to specify the use of HTTPS for the client file download:

```
install_dir\nms\bin\nmsclient.bat secure server server:8444 ↵
```

where
install_dir is the client installation location, typically C:\5620sam\client
server is the IP address or the DNS name of the main server that has SSL enabled

The client downloads the updated configuration, and subsequent client sessions use HTTPS by default.

Procedure 5-15 To disable HTTPS on a 5620 SAM single-user GUI client or client delegate server

Perform this procedure to disable HTTPS on a 5620 SAM single-user GUI client or client delegate server, and to configure the client or client delegate server to use HTTP for subsequent auto-client update communication with a 5620 SAM main server. This procedure is required when a single-user GUI client or client delegate server that uses HTTPS must connect to a main server that does not have SSL enabled.

Note 1 — A 5620 SAM single-user client or client delegate server that has HTTPS enabled cannot communicate with a 5620 SAM main server that does not have SSL enabled.

Note 2 — When you perform this step on a client delegate server, you affect each GUI client that connects through the client delegate server.

Note 3 — The Solaris command lines in this procedure use the # symbol to represent the CLI prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

Note 4 — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

1 Close the 5620 SAM client GUI, if the GUI is open, by choosing Application→Exit from the 5620 SAM main menu.

Note — If you are performing this procedure on a client delegate server, you must close each client GUI that connects through the client delegate server.

2 Perform one of the following.

- **a** To disable HTTPS and use HTTP for the next client GUI session only, go to step 11.
- **b** To disable HTTPS and use HTTP for all subsequent client GUI sessions, go to step 3.

3 Log in to the single-user client or client delegate server station.

Note — On a client delegate server station, you must log in as the root user.

4 Navigate to the client configuration directory, typically C:\5620sam\client\nms\config on Windows, or /opt/5620sam/client/nms/config on Solaris.

5 Create a backup copy of the nms-client.xml file.

6 Open the nms-client.xml file using a text editor.

7 Change the commandPort value shown in Code 5-11 from “8444” to “8085”.

Code 5-11: j2ee section of nms-client.xml file before modification

```
<configuration>
  <j2ee
            ejbServerType="Jboss"
            ejbServerHost="192.168.213.117"
            ejbServerPort="1099"
            commandPort="8444"
            commandSecure="true"
            jmsTopicName="5620-THIN-SAM-topic" />
```

8 Change the commandSecure value from “true” to “false”. The j2ee section appears as shown in Code 5-12.

Code 5-12: j2ee section of nms-client.xml file after modification

```
<configuration>
  <j2ee
            ejbServerType="Jboss"
            ejbServerHost="192.168.213.117"
            ejbServerPort="1099"
            commandPort="8085"
            commandSecure="false"
            jmsTopicName="5620-THIN-SAM-topic" />
```

9 Save and close the nms-client.xml file. HTTPS is disabled for subsequent GUI client sessions.

10 Perform the following steps to start the GUI client session using HTTP.

i Log in to the single-user client or client delegate server station.

Note — On a client delegate server station, you must log in as the root user.

ii Open a console window.

iii On a Solaris station, enter the following at the prompt:

```
# install_dir/nms/bin/nmsclient.bash server server:8085 ↵
```

where
install_dir is the client installation location, typically /opt/5620sam/client
server is the IP address or the DNS name of the main server that has SSL disabled

iv On a Windows station, enter the following at the prompt:

```
install_dir\nms\bin\nmsclient.bat server server:8085 ↵
```

where
install_dir is the client installation location, typically C:\5620sam\client
server is the IP address or the DNS name of the main server that has SSL disabled

The client connects to the main server using HTTP.

11 Use the client GUI, as required.

Procedure 5-16 To configure secure communication on the JGroups channel between two 5620 SAM main servers in a redundant deployment

Perform this procedure to enable secure communication on the JGroups channel between two 5620 SAM main servers in a redundant 5620 SAM system.

Note — You must perform this procedure on each main server in the 5620 SAM system.

Caution — This procedure requires a restart of each 5620 SAM main server, which is service-affecting.

Note 1 — The Solaris command lines in this procedure use the # symbol to represent the CLI prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

Note 2 — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

1 Log in to the main server station as the samadmin user.

2 Open a console window.

3 Navigate to the server deployment directory, typically /opt/5620sam/server/nms/jboss/server/default/deploy.

4 Open the cluster-service.xml file using a plain-text editor.

5 Locate the following XML tag that marks the beginning of the Config section:

```
<Config>
```

6 Insert the following line in the Config section after the line that begins with <VERIFY_SUSPECT and ends with />.

```
<ENCRYPT encrypt_entire_message="true" sym_init="128"
sym_algorithm="AES/ECB/PKCS5Padding" asym_init="512"
asym_algorithm="RSA"/>
```

The <VERIFY_SUSPECT and <ENCRYPT lines should look similar to the following and be present in the order shown:

```
<VERIFY_SUSPECT down_thread="true" timeout="15000"
up_thread="true"/>
```

```
<ENCRYPT encrypt_entire_message="true" sym_init="128"
sym_algorithm="AES/ECB/PKCS5Padding" asym_init="512"
asym_algorithm="RSA"/>
```

7 Save and close the cluster-service.xml file.

8 Open a console window.

9 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

10 Enter the following at the prompt to restart the main server:

```
# ./nmsserver.bash force_restart ↵
```

The main server restarts.

Procedure 5-17 To configure secure communication on the JGroups channel between a 5620 SAM main server and auxiliary server

Caution — This procedure requires a restart of the 5620 SAM main and auxiliary servers, which is service-affecting. Ensure that you attempt to perform this procedure only during a scheduled maintenance window.

1 Log in to the main server station as the samadmin user.

2 Open a console window.

3 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag that marks the beginning of the jgroup_config section:

```
<jgroup_config>
```

6 Insert the following line in the Config section after the line that begins with <VERIFY_SUSPECT and ends with />.

```
<ENCRYPT encrypt_entire_message="true" sym_init="128"
sym_algorithm="AES/ECB/PKCS5Padding" asym_init="512"
asym_algorithm="RSA"/>
```

The <VERIFY_SUSPECT and <ENCRYPT lines should look similar to the following and be present in the order shown:

```
<VERIFY_SUSPECT down_thread="true" timeout="15000"
up_thread="true"/>

<ENCRYPT encrypt_entire_message="true" sym_init="128"
sym_algorithm="AES/ECB/PKCS5Padding" asym_init="512"
asym_algorithm="RSA"/>
```

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt to restart the main server:

```
# ./nmsserver.bash force_restart ↵
```

The main server restarts.

10 Log in to the auxiliary server station as the samadmin user.

11 Open a console window.

12 Navigate to the server configuration directory, typically /opt/5620sam/auxserver/nms/config.

13 Open the nms-auxserver.xml file using a plain-text editor.

14 Locate the following XML tag that marks the beginning of the jgroup_config section:

```
<jgroup_config>
```

15 Insert the following line in the Config section after the line that begins with <VERIFY_SUSPECT and ends with />.

```
<ENCRYPT encrypt_entire_message="true" sym_init="128"
sym_algorithm="AES/ECB/PKCS5Padding" asym_init="512"
asym_algorithm="RSA"/>
```

The <VERIFY_SUSPECT and <ENCRYPT lines should look similar to the following and be present in the order shown:

```
<VERIFY_SUSPECT down_thread="true" timeout="15000"
up_thread="true"/>

<ENCRYPT encrypt_entire_message="true" sym_init="128"
sym_algorithm="AES/ECB/PKCS5Padding" asym_init="512"
asym_algorithm="RSA"/>
```

16 Save and close the nms-auxserver.xml file.

17 Navigate to the server binary directory, typically /opt/5620sam/auxserver/nms/bin.

18 Enter the following at the prompt to restart the auxiliary server:

```
# ./auxnmsserver.bash auxforce_restart ↵
```

The auxiliary server restarts.

19 Repeat steps 10 to 18 on each additional auxiliary server in the 5620 SAM system.

Procedure 5-18 To configure secure communication between a 5620 SAM main server and database

Note 1 — If the 5620 SAM system is a redundant system, you must perform this procedure on each main server/database pair.

Note 2 — The Solaris command lines in this procedure use the # symbol to represent the CLI prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

Note 3 — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

Update main server configuration

1 Log in to the main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<db
```

This section of the file contains the 5620 SAM database information that is configured in the following steps.

6 Perform one of the following:

a To enable encryption, edit the enableEncryption line to read:

```
enableEncryption="yes"
```

b To disable encryption, edit the enableEncryption line to read:

```
enableEncryption="no"
```

7 If you are enabling encryption, specify the type of encryption by editing the following line accordingly:

```
encryptionAlgorithm="encryption_alg"
```

where *encryption_alg* is the type of encryption algorithm

Note — The valid encryptionAlgorithm values are listed just above the <db tag in the nms-server.xml file. You can specify only one value.

8 Save and close the nms-server.xml file.

9 Open a console window on the main server station.

10 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin on a Solaris station or C:\5620sam\server\nms\bin on a Windows station.

11 Perform one of the following.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash read_config ↵
```

b If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat read_config ↵
```

The main server reads the nms-server.xml file and the new security settings are put into effect.

Update database configuration

12 Log in to the database station as a user with Oracle management privileges.

13 Navigate to the database configuration directory, typically /opt/5620sam/samdb/install/config/samdb on a Solaris station or C:\5620sam\samdb\install\config\samdb on a Windows station.

14 Create a backup copy of the nms-server.xml file.

15 Open the nms-server.xml file using a plain-text editor.

16 Locate the following XML tag:

```
<db driver="oracle.jdbc.driver.OracleDriver"
```

This section of the file contains the 5620 SAM database information that is configured in the following steps.

17 Perform one of the following:

a To enable encryption, edit the enableEncryption line to read:

```
enableEncryption="yes"
```

b To disable encryption, edit the enableEncryption line to read:

```
enableEncryption="no"
```

18 If you are enabling encryption, specify the type of encryption by editing the following line accordingly:

```
encryptionAlgorithm="encryption_alg"
```

where *encryption_alg* is the type of encryption algorithm

Note — The encryptionAlgorithm value must match the value specified on the main server station in step 7. You can specify only one value.

19 Save and close the nms-server.xml file.

20 Navigate to the Oracle configuration directory, typically /opt/5620sam/oracle10r2/NETWORK/ADMIN on a Solaris station or C:\5620sam\oracle\NETWORK\ADMIN on a Windows station.

21 Create a backup copy of the sqlnet.ora file.

22 Open the sqlnet.ora file using a plain-text editor.

23 Locate the following section label:

```
# Encryption
```

24 Perform one of the following:

a To enable encryption, edit the SQLNET.ENCRYPTION_SERVER line to read:

```
SQLNET.ENCRYPTION_SERVER = requested
```

b To disable encryption, edit the SQLNET.ENCRYPTION_SERVER line to read:

```
SQLNET.ENCRYPTION_SERVER = rejected
```

25 If you are enabling encryption, specify the type of encryption by editing the following line accordingly:

```
SQLNET.ENCRYPTION_TYPES_SERVER = (encryption_alg)
```

where *encryption_alg* is the type of encryption algorithm

Note — The SQLNET.ENCRYPTION_TYPES_SERVER value must match the encryptionAlgorithm value specified on the main server station in step 7. You can specify only one value.

26 Save and close the sqlnet.ora file.

5.5 Network management configuration procedures

The following procedures describe how to configure system-wide 5620 SAM functions related to the managed network.

Procedure 5-19 To change the system name of a managed device

Perform this procedure to change the system name of one of the following device types using a 5620 SAM utility:

- 7210 SAS-M24F
- 7210 SAS-M24F2XFP
- 7210 SAS-M24F2XFP [ETR]
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR

Note 1 — The 5620 SAM main server utility lists other NE types, but does not support changing the system name for devices that are not listed above.

Note 2 — The change can be implemented using SNMPv2c or SNMPv3.

Caution — This procedure requires a restart of a 5620 SAM main server, which is service-affecting. To avoid service interruption in a redundant deployment, schedule the system name change to coincide with a maintenance window and perform this procedure on the 5620 SAM main server. System name changes are automatically propagated to the standby server.

1 Stop the application server. After this step, the 5620 SAM main server is not managing the network.

i Open a console window on the 5620 SAM main server and log in as the samadmin user.

ii Navigate to the server configuration directory. Enter the following at the prompt:

```
# cd install_dir/nms/bin ↵
```

where *install_dir* is the server installation location, typically /opt/5620sam/server on Solaris, or C:\5620sam\server on Windows

iii Perform one of the following to stop the application server.

- If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash stop ↵
```

- If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat stop ↵
```

iv Perform one of the following to verify that the application server is stopped.

- If the main server is installed on Solaris, enter the following at the prompt:

  ```
  # ./nmsserver.bash appserver_status ↵
  ```

- If the main server is installed on Windows, enter the following at the prompt:

  ```
  nmsserver.bat appserver_status ↵
  ```

v The server application is stopped when the command in step 5 iv returns the following text string:

```
Application Server is stopped
```

If the command returns anything other than the above text string, wait five minutes and repeat step 5 iv. Do not proceed unless the console displays the above text.

2 Use a text editor to open the updateSysName.properties file in the current directory.

3 Follow the instructions in the file to update the SNMPv2c or SNMPv3 settings in the file, depending on the SNMP version that the device uses.

4 Save and close the updateSysName.properties file.

5 Perform one of the following steps to initiate a system name change for the device.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./updateSysName.bash ↵
```

b If the main server is installed on Windows, enter the following at the prompt:

```
updateSysName.bat ↵
```

6 Enter the ID of the device that you want to update.

7 Enter the new system name.

8 Perform one of the following steps to restart the 5620 SAM main server.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash start ↵
```

b If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat start ↵
```

The main server starts.

Procedure 5-20 To configure the 5620 SAM to save device configuration backups on a file system

Perform this procedure to configure the 5620 SAM to save device configuration backups as files in addition to saving them in the database. By default, the 5620 SAM saves device configuration backups only in the 5620 SAM database.

Note 1 — The samadmin user requires read and write permissions to each directory specified in this procedure.

Note 2 — The Solaris command lines in this procedure use the # symbol to represent the console prompt. Do not type the # symbol when you enter a command.

1 Perform one of the following.

   a If the 5620 SAM server is installed on Solaris, log in to the 5620 SAM server station as the samadmin user.

   b If the 5620 SAM server is installed on Windows, log in to the 5620 SAM server station as a user with local administrator privileges.

2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag, which marks the beginning of the section that you want to configure:

   <*device_type*backup

   where *device_type* is one of the following:
   Ran—for RAN devices such as the eNodeB
   AosSr—for OmniSwitch devices
   MPRSr—for 9500 MPR devices
   sr—for all other devices, such as the 7450 ESS, 7710 SR, and 7750 SR

   The same *device_type* identifier is used in the following steps.

6 To enable the storage of device backups on the main server file system, configure the following parameter by inserting the storage location between the quotation marks:

   *device_type*BackupDirectory="*location*"

   where *location* is an absolute or relative file path

Note — A relative file path that you specify in this step is relative to the following directory on the 5620 SAM main server:

- *installation_directory*/nms/bin for Solaris
- *installation_directory*\nms\bin for Windows

7 If required, configure the following parameters by changing the value between the quotation marks:

Note — The default value for each parameter is shown in this step.

```
diskUsageThreshold="80"

maxNumberOfFiles="5000"

purgeDiskUsageThreshold="95"

saveLatestOnly="true"

device_typeBackupSyncEnabled="false"

device_typeBackupSyncInterval="30"
```

The following are the parameter descriptions:

- diskUsageThreshold—The percentage of disk usage above which the 5620 SAM raises a major alarm. When the disk usage falls below this value, the alarm clears. The range is 0 to 95; the default is 80. A value of 0 means that the disk usage is not monitored.
- maxNumberOfFiles—The maximum number of backup files for this device type that are saved on the file system. When this value is exceeded, the 5620 SAM deletes the oldest backup files. The range is 0 to 100 000; the default is 5000. A value of 0 means that no limit is enforced.
- purgeDiskUsageThreshold—The percentage of disk usage above which the 5620 SAM deletes the oldest backup files and raises a major alarm. The files are deleted until the disk usage falls below the percentage specified by diskUsageThreshold. A value of 0 means that no file deletion occurs and, accordingly, no alarm is raised. The range is 0 to 95; the default is 95.
- saveLatestOnly—If set to true, specifies that only the latest device backup is saved. If set to false, specifies that device backups are saved according to the constraints specified by the diskUsageThreshold, maxNumberOfFiles, and purgeDiskUsageThreshold parameters.
- *device_type*BackupSyncEnabled—If set to true, specifies that the 5620 SAM synchronizes the backup files between the primary and standby main servers.
- *device_type*BackupSyncInterval—If *device_type*BackupSyncEnabled is set to true, specifies how often, in m, the 5620 SAM synchronizes the files.

8 To disable the storage of device backups on the main server file system, configure the following parameter by removing the storage location between the quotation marks, as shown in the following example:

```
device_typeBackupDirectory=""
```

9 Perform steps 5 to 8 to configure the storage of device backups for another device type, if required.

10 Save and close the nms-server.xml file.

11 Open a console window on the main server station.

12 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin on a Solaris station or C:\5620sam\server\nms\bin on a Windows station.

13 Perform one of the following.

a If the main server is installed on a Solaris station, enter the following at the prompt:

```
# ./nmsserver.bash read_config ↵
```

b If the main server is installed on a Windows station, enter the following at the prompt:

```
nmsserver.bat read_config ↵
```

The 5620 SAM main server reads the nms-server.xml file and puts the configuration change into effect. Subsequent device configuration backups are saved to the path specified in the nms-server.xml file.

The 5620 SAM saves the device backup files in the following directory under the location specified in step 5:

samNodeBackup*device_ID**timestamp*

where
device_ID is the unique identifier of a device
timestamp is the time when the backup is saved

Procedure 5-21 To configure automatic device configuration backup file removal

Perform this procedure to configure the 5620 SAM to automatically remove the configuration backup files for a device when the device is unmanaged.

Caution — This procedure requires a restart of the 5620 SAM server, which is service-affecting.

Note 1 — This procedure configures the removal of backup files only; device configuration backups in the database are retained.

Note 2 — The Solaris command lines in this procedure use the # symbol to represent the console prompt. The actual prompt may differ, depending on the type of command shell that is in use.

Do not type the # symbol when entering a command.

1 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

2 Create a backup copy of the nms-server.xml file.

3 Open the nms-server.xml file using a plain-text editor.

4 Search for the following XML tag:

```
</configuration>
```

5 Enter the following line above the </configuration> tag:

```
<nodeBackups removeBackupOnDelete="true"/>
```

6 Save and close the nms-server.xml file.

7 Open a console window on the main server station.

8 Navigate to the 5620 SAM server binary directory or folder, typically /opt/5620sam/server/nms/bin on a Solaris station or C:\5620sam\server\nms\bin on a Windows station.

9 Perform one of the following actions to restart the 5620 SAM server.

Caution — Restarting a 5620 SAM server is service-affecting. Ensure that you perform this step only during a scheduled maintenance window.

a If the main server is installed on a Solaris station, enter the following at the console prompt:

```
# ./nmsserver.bash force_restart ↵
```

b If the main server is installed on a Windows station, enter the following at the console prompt:

```
nmsserver.bat force_restart ↵
```

10 The 5620 SAM main server restarts. The 5620 SAM deletes the configuration backup files of NEs that are subsequently unmanaged.

Procedure 5-22 To configure service CAC

Perform this procedure to configure the service CAC functionality to enable 5620 SAM to automatically bind PBB tunnels to services based on available bandwidth.

Note 1 — This feature has limited availability. Contact your Alcatel-Lucent technical support representative for more information about the availability of this feature.

Note 2 — You must perform this procedure on each main server in the 5620 SAM system.

1 Close each 5620 SAM client that connects to the main server through the client delegate server, by choosing Application→Exit from the 5620 SAM main menu.

2 Use a Solaris utility to change the IP address of the client delegate server station to the new value.

3 Log in to the main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

4 Open a console window.

5 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

6 Open the nms-server.xml file using a plain-text editor.

7 Locate the following XML tag:

```
<require-CAC
```

The service CAC section should read as follows:

```
<require-CAC
        enabled="false"
        defaultBWThreshold="90"
        linkTunnelCacheMaxSize="1000"
        tunnelServiceCacheMaxSize="10000"
        serviceBWCacheMaxSize="50000"
    />
```

8 Change enabled="false" to enabled="true".

9 Save and close the nms-server.xml file.

10 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin on a Solaris station or C:\5620sam\server\nms\bin on a Windows station.

11 Perform one of the following.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash read_config <return>
```

b If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat read_config <return>
```

The main server reads the nms-server.xml file and enables the server CAC features on the client delegate server.

Procedure 5-23 To enable alarm reporting for duplicate NE system IP addresses

Perform this procedure to enable the 5620 SAM to verify the uniqueness of NE system IP addresses. When verification is enabled, the 5620 SAM raises an alarm when an NE reports a system IP address that is in use by another NE.

Note 1 — The Solaris command lines in this procedure use the # symbol to represent the CLI prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

Note 2 — CLI scripts that are configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

1 Log in to the main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

2 Open a console window.

3 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following tag that marks the beginning of the SNMP section:

```
<snmp
```

6 Add the following before the end of the SNMP section, ensuring that there is a space between the last character and the section end, which is marked by a /> tag:

verifyNodeIdentity=”1"

The SNMP section should read as follows:

```
<snmp
     ip="server_IP_address"
     ipv6=""
     port="port_number"
     trapLogId="log_ID"
     verifyNodeIdentity="1" />
```

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin on a Solaris station or C:\5620sam\server\nms\bin on a Windows station.

9 Perform one of the following.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash read_config ↵
```

b If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat read_config ↵
```

The main server reads the nms-server.xml file and alarm reporting for duplicate NE system IP addresses is enabled.

Procedure 5-24 To enable LSP on-demand resynchronization

Perform this procedure to modify the nms-server.xml file to enable LSP on-demand resynchronization. The 5620 SAM scheduled resynchronization functionality is then disabled for some LSP objects. See chapter 29 for more information.

Caution — Modify only the parameters specified in this procedure. Unauthorized modification of the nms-server.xml file can seriously affect network management and 5620 SAM performance.

1 Log in to the main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

2 Navigate to the server configuration directory, which is typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following line:

```
<lspOnDemand overrideEnabled="false" />
```

6 Change "false" to "true".

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, which is typically /opt/5620sam/server/nms/bin on a Solaris station or C:\5620sam\server\nms\bin on a Windows station.

9 Perform one of the following.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash read_config ↵
```

b If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat read_config ↵
```

The main server reads the nms-server.xml file and LSP on-demand resynchronization is enabled.

Procedure 5-25 To enable debug configuration file reloading for mirror services

Perform this procedure to ensure that the managed NEs reload the debug configuration file after an NE restarts. This ensures that the mirror services in the managed network resume operation after a reboot or CPM activity switch on the NE that hosts the mirror service. By default, debug configuration file reloading is disabled.

Caution — This procedure requires a restart of a 5620 SAM main server, which is service-affecting.

Note 1 — The Solaris command lines in this procedure use the # symbol to represent the CLI prompt. The actual prompt may differ, depending on the type of command shell that is in use. Do not type the # symbol when entering a command.

Note 2 — CLI scripts that configured to run on OmniSwitch devices fail if the CLI prompt contains the following characters: ~ ! @ $ % &

1 Log in to the main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

2 Open a console window.

3 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<serviceMirror
```

6 Specify the NE location of the debug configuration file. For example:

```
<serviceMirror
debugFilename=""
reloadDelay="10"
/>
```

where
reloadDelay specifies the time, in seconds, to wait before a reload request is sent
debugFilename specifies the location of the file on an NE, for example, cf3:/ServiceMirror.dbg

Note — The debugFilename value must be the debug configuration filename that is configured on the NEs that host mirror services.

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin on a Solaris station or C:\5620sam\server\nms\bin on a Windows station.

9 Perform one of the following to restart the main server.

Caution — Restarting a 5620 SAM main server is service-affecting. Ensure that you perform this step only during a scheduled maintenance window.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash force_restart ↵
```

b If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat force_restart ↵
```

10 The main server restarts.

If required, create a device backup policy to ensure that device configurations are not lost in the event of an NE failure. See chapter 21 for information about device backup policies.

Procedure 5-26 To create a default SNMPv2 OmniSwitch user on a 5620 SAM system

Perform this procedure to create a default SNMPv2 OmniSwitch user on a 5620 SAM system.

Caution — Modify only the parameters specified in this procedure. Unauthorized modification of the nms-server.xml file can seriously affect network management and 5620 SAM performance.

1 Log in to the main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<snmp
```

This section of the file contains the 5620 SAM SNMP information that is configured in the following steps.

6 Add the following before the end of the SNMP section, ensuring that there is a space between the last character and the section end, which is marked by a /> tag:

snmpV2UserName=”user_name”

where *user_name* is a user name that is configured on the switch

The SNMP section should read as follows:

```
<snmp
            ip="server_IP_address"
            port="port_number"
            trapLogId="log_ID"
            snmpV2UserName="user_name" />
```

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin on a Solaris station or C:\5620sam\server\nms\bin on a Windows station.

9 Perform one of the following.

a If the main server is installed on Solaris, enter the following at the prompt:

```
# ./nmsserver.bash read_config ↵
```

b If the main server is installed on Windows, enter the following at the prompt:

```
nmsserver.bat read_config ↵
```

The main server reads the nms-server.xml file and the new SNMPv2 user name is enabled.

6 — 5620 SAM system redundancy

6.1 5620 SAM system redundancy overview

You can deploy a 5620 SAM system on Solaris in a redundant configuration to provide greater fault tolerance by ensuring that there is no single point of software failure in the 5620 SAM management network. A redundant 5620 SAM deployment consists of the following components:

- primary and standby 5620 SAM main servers
- primary and standby 5620 SAM databases

Note 1 — For conciseness, a primary 5620 SAM main server is sometimes called a primary server in this chapter.

Note 2 — For conciseness, a standby 5620 SAM main server is sometimes called a standby server in this chapter.

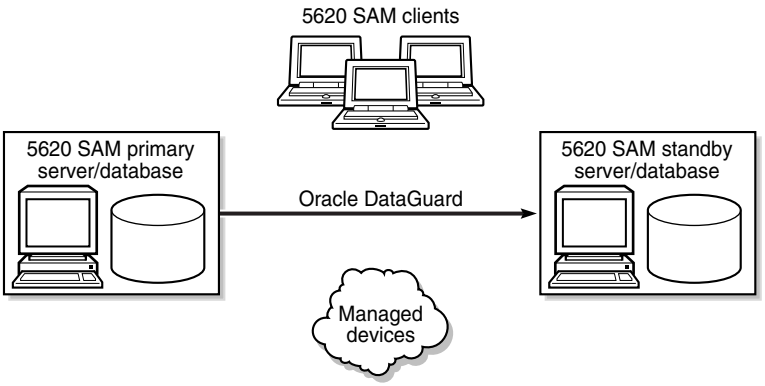
The current state of a component defines the primary or standby role of the component. The primary main server actively manages the network and the primary database is open in read/write mode. When a standby component detects a primary component failure, it automatically changes roles from standby to primary. You can also change the role of a component using the 5620 SAM client GUI or a CLI script.

The 5620 SAM supports collocated and distributed system redundancy. A collocated system requires two stations that each host a main server and database. A distributed system requires four stations that each host a main server or database. Each main server and database is logically independent, regardless of the deployment type.

Caution — For increased 5620 SAM system performance and fault tolerance, Alcatel-Lucent recommends that you deploy the primary server and database in the same geographical location and LAN.

Figure 6-1 shows a collocated redundant 5620 SAM system.

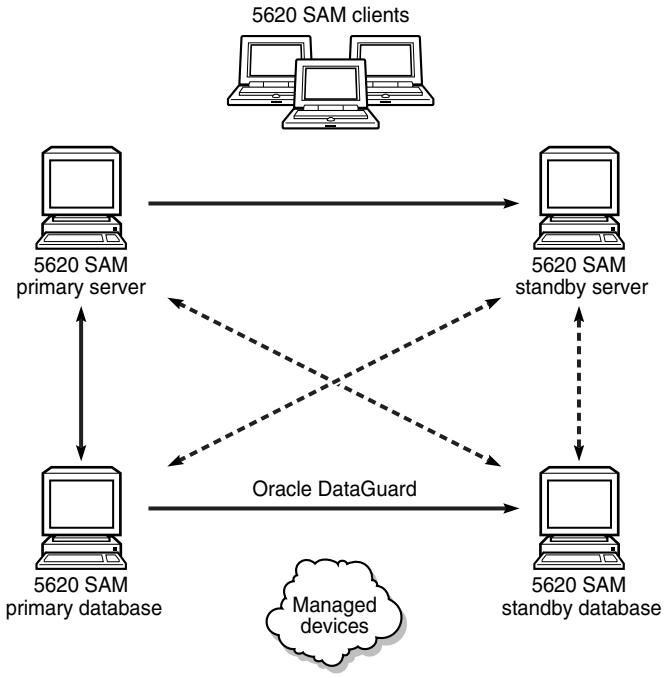
Figure 6-1 Collocated redundant 5620 SAM system



The primary and standby main servers can communicate with the redundant databases, and periodically verify server redundancy. If the standby server fails to reach the primary server within 60s, the standby server becomes the primary server. A 5620 SAM database uses the Oracle DataGuard function to maintain redundancy.

Figure 6-2 shows a distributed redundant 5620 SAM system.

Figure 6-2 Distributed redundant 5620 SAM system



In 5620 SAM redundancy server installation, the Oracle DataGuard synchronization level is set to real-time apply by default to keep the primary and secondary databases synchronized.

A main server role change is called a server activity switch. An automatic database role change is called a failover. A manual database role change is called a switchover.

A typical redundant 5620 SAM deployment has a primary server and database in a facility that is geographically separate from the standby server and database facility. To ensure that the primary components are in the same LAN after an activity switch or failover, you can configure automatic database realignment during 5620 SAM server installation. See "Automatic database realignment" for more information.

The 5620 SAM GUI clients always communicate with the current primary server. After a server activity switch, the GUI clients automatically connect to the new primary server, which is the former standby server. The 5620 SAM OSS clients also communicate with the current primary server, but after a server activity switch, the OSS clients do not automatically connect to the new primary server.

You can use the 5620 SAM GUI, or scripts on a 5620 SAM main server, to do the following:

- Check the redundant server and database status.
- Perform an activity switch from the primary to standby server.
- Reinstantiate the former primary database as the standby database.

5620 SAM system redundancy is configured during 5620 SAM component installation. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about configuring 5620 SAM redundancy.

The following general conditions apply to 5620 SAM system redundancy:

- The main servers and databases must each be redundant. For example, you cannot have redundant servers and a standalone database.
- The network that contains a redundant 5620 SAM system must meet the latency and bandwidth requirements described in the *5620 SAM Planning Guide*.

Note — To provide hardware fault tolerance in addition to software redundancy, Alcatel-Lucent recommends using redundant physical links between the primary and standby servers and databases to ensure there is no single point of network or hardware failure.

- The server and database stations require the same Solaris version and patch level.
- The primary and standby server stations must have identical disk layouts and partitioning.
- The primary and standby database stations must have identical disk layouts and partitioning.
- The following users can perform manual server activity switches or database switchovers:
  - the samadmin UNIX user on a main server station
  - a client GUI user that has update or execute access permissions on the db.DatabaseManager.switchover and db.DatabaseManager.reinstantiateStandby classes
  - a client GUI user that has the admin scope of command role

Auxiliary servers

5620 SAM auxiliary servers are optional servers that extend the network management processing engine by distributing server functionality, for example, statistics collection, among multiple stations in a 5620 SAM domain. Each auxiliary server is installed on a separate station in a 5620 SAM server cluster. An auxiliary server communicates only with the primary main server and database. Main and auxiliary servers can open sessions only on the primary database.

A 5620 SAM main server controls task scheduling and sends task requests to auxiliary servers. When a Preferred auxiliary server is unresponsive, the main server directs the requests to a Reserved auxiliary server. The Preferred or Reserved role of an auxiliary server is specified during 5620 SAM main server installation.

When an auxiliary server cannot connect to the primary main server or database, it re-initializes and continues trying to connect until it succeeds or, in the case of a database failover, until the main server directs it to the new database.

An auxiliary server does not cause, perform, or initiate redundancy activities such as failovers. However, an unused, or Reserved, auxiliary server may be called into service by the main server when another auxiliary server fails.

When an auxiliary server fails to respond to the primary main server, the main server tries repeatedly to establish communication before it raises an alarm. The alarm clears when the main server receives a response. 5620 SAM system performance may degrade when a main server loses contact with a number of auxiliary servers that exceeds the number of Preferred auxiliary servers in the 5620 SAM server cluster.

After startup, an auxiliary server waits for initialization information from a main server. An auxiliary server restarts if it does not receive all required initialization information within five minutes.

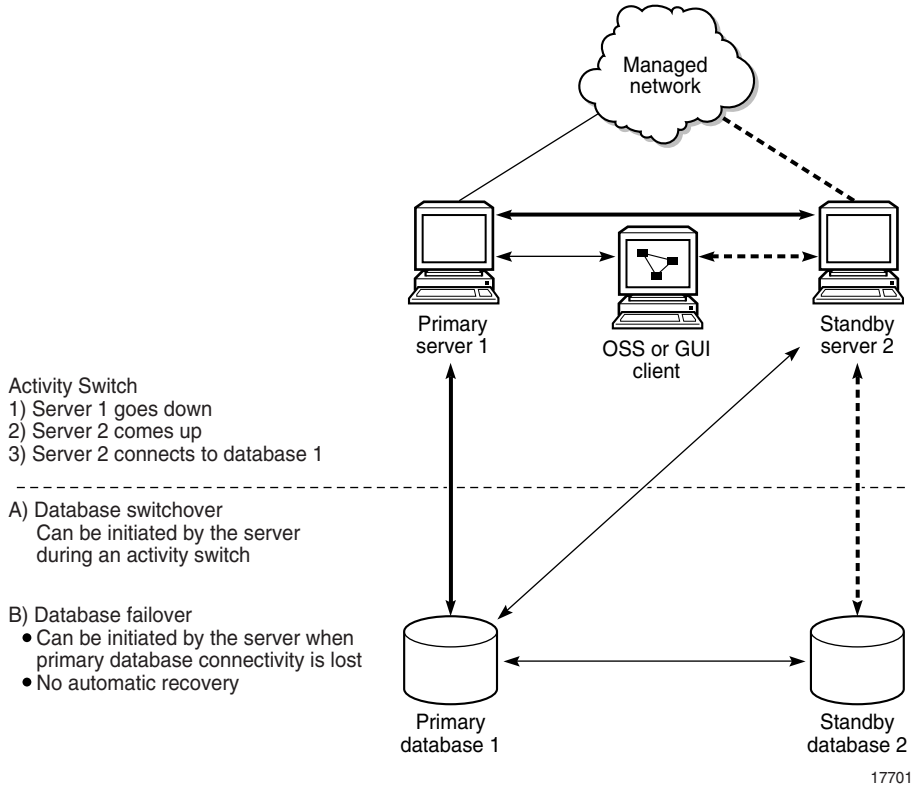
Note — Because an auxiliary server does not play an active role in 5620 SAM redundancy, the unqualified term "server" in this chapter refers to a 5620 SAM main server.

See the *5620 SAM System Architecture Guide* for more information about the interaction of 5620 SAM main and auxiliary servers.

Redundancy functions

Figure 6-3 shows the 5620 SAM system redundancy role-change events.

Figure 6-3 5620 SAM redundancy role-change events

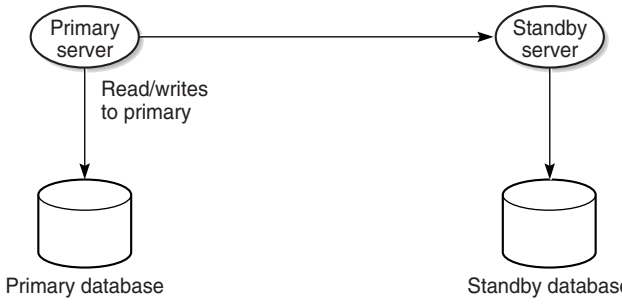


Server activity switches

The standby server initiates an automatic server activity switch when it cannot communicate with the primary server. A 5620 SAM administrator performs a manual server activity switch.

Figure 6-4 shows the server and database roles before an activity switch.

Figure 6-4 Server and database roles before server activity switch



A manual server activity switch is typically a planned server maintenance or testing operation. For security reasons, you cannot use a 5620 SAM GUI or OSS client to perform a server activity switch.

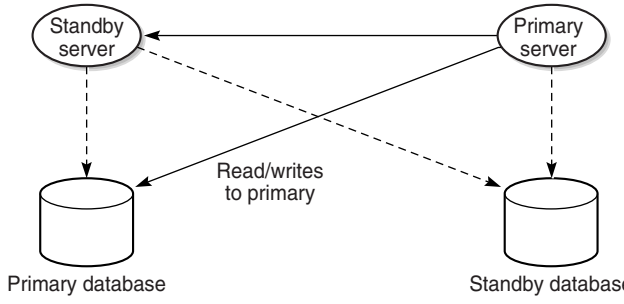
During a server activity switch, a main server does not process SNMP traps, attempt to synchronize NEs, or collect statistics. Auxiliary servers process outstanding requests during an activity switch, but do not communicate with a main server.

The following occurs during a server activity switch:

- The primary server raises alarms about the event.
- Each GUI client receives notification of the activity switch and displays a message about the server unavailability during the activity switch.

Figure 6-5 shows the server and database roles after a successful activity switch.

Figure 6-5 Server and database roles after server activity switch



The following occurs after a server activity switch:

- If automatic database realignment is enabled, the new primary server performs a database switchover.
- The GUI clients communicate with the new primary server and display the current redundancy status.
- The OSS clients must connect to the new primary server, as described in the *5620 SAM-O OSS Interface Developer Guide*.
- The new primary server establishes communication and synchronizes information with the 5620 SAM auxiliary servers.
- The auxiliary servers exchange information with the new primary server; no auxiliary servers exchange information with the former primary server.
- The Preferred or Reserved state of each auxiliary server changes, depending on the configuration of the new primary server.
- The new primary server attempts to redeploy the client requests that the former primary server did not complete before the activity switch.

The connected 5620 SAM GUI clients do not need to re-login if there is a failover or switchover of the server of database. During the failover or switchover, there may be inactivity for the connected clients, but when the new primary server and database are established, all connected user sessions will be seamlessly transferred to the new servers.

Database switchovers

A 5620 SAM administrator directs a main server to initiate a database switchover. Figure 6-6 shows the main server and database roles before a database switchover.

Figure 6-6 Server and database roles before database switchover

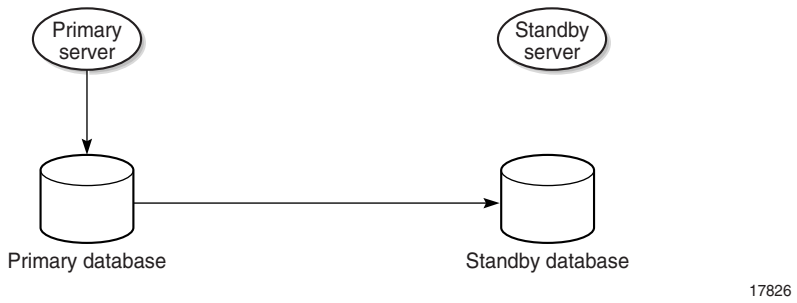
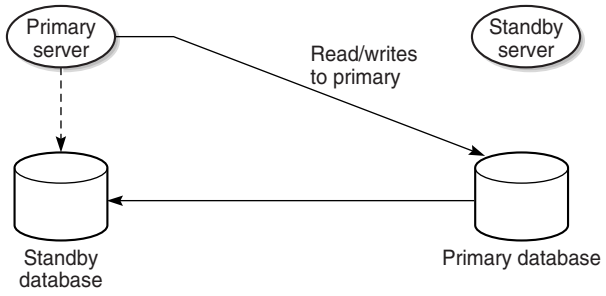


Figure 6-7 shows the server and database roles after a database switchover.

Figure 6-7 Server and database roles after database switchover



The following occurs after a successful database switchover:

- The primary server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary server directs each auxiliary server to use the new primary database.

When a database switchover fails, the primary and standby database roles do not change. No automatic database realignment occurs as a result of a switchover.

Database failovers

5620 SAM database failover functionality is enabled by default. A failover occurs when a main server cannot communicate with the primary database, but can communicate with the standby database and the managed NEs. When this happens, the main server directs the standby database to become the primary database.

A database failover occurs only under the following conditions.

- The standby database is configured, operational, and reachable.
- The main server can communicate with the managed NEs.

Figure 6-8 shows the server and database roles before a failover.

Figure 6-8 Server and database roles before database failover

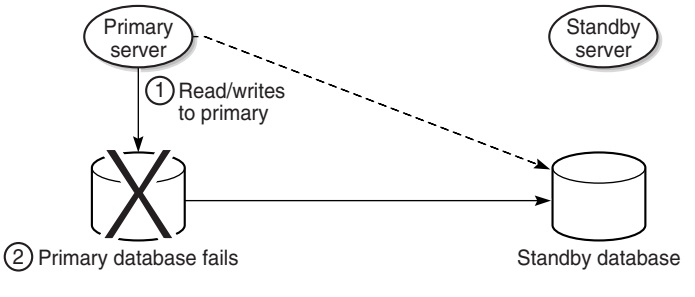
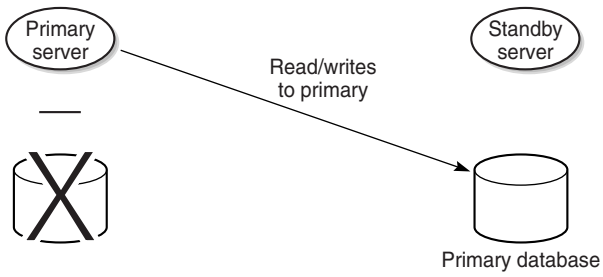


Figure 6-9 shows the server and database roles after a successful failover.

Figure 6-9 Server and database roles after database failover



Note — After a successful failover, database redundancy is not available. See "Re-establishing database redundancy" in this section for information about re-establishing database redundancy after a failover.

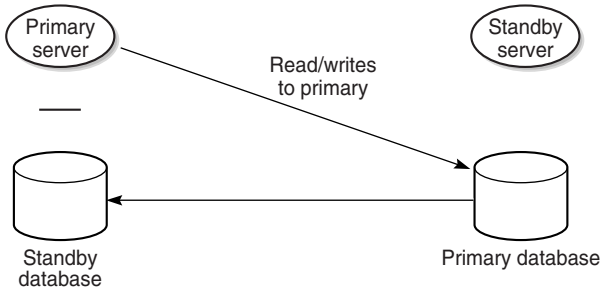
When a database failover fails, the primary server tries again to communicate with the primary database. If the primary database remains unavailable, the primary server tries again to initiate a failover.

Re-establishing database redundancy

After a failover, the former primary database is no longer part of the redundant configuration. To re-establish database redundancy, you must reinstantiate the former primary database as the new standby database. You can do this only when the failed database station is restored to full operation and has a configured proxy port that is in service. See Procedures 6-6 and 6-7 for more information about manually reinstantiating a redundant database.

Figure 6-10 shows a former primary database serving as the new standby database.

Figure 6-10 Server and database roles after database reinstantiation



Automatic database realignment

In a redundant 5620 SAM system that is geographically dispersed, the primary server and database may be in separate LANs or WANs after an activity switch or failover. The network latency that this introduces can affect 5620 SAM system performance. Automatic database realignment is an optional mechanism that attempts to ensure that each main server uses the local database.

The database with which a main server tries to align itself is called the preferred database of the main server. An operator enables automatic database realignment and specifies the preferred database during 5620 SAM server installation, or during server configuration after installation.

Note — For automatic database alignment to work, you must enable it and specify a preferred database on each main server in a redundant 5620 SAM system.

When a primary server starts, it verifies that the primary database is the preferred database. If the primary database is not the preferred database, the server performs a database switchover to reverse the primary and standby database roles. If the switchover is successful, the main servers and databases in the 5620 SAM system are aligned. If the switchover fails, each database reverts to the former role, and the main server raises an alarm about the failed switchover.

When you perform a database switchover and automatic database realignment is enabled, the primary server does not attempt database realignment. A switchover is a manual operation that is considered to be a purposeful act.

Performing a server activity switch when automatic database realignment is enabled triggers a database switchover.

Summary of redundancy operations

Table 6-1 summarizes the operations related to 5620 SAM main server redundancy.

Table 6-1 5620 SAM server redundancy operations

Type	Description	Notes
Server activity switch (automatic)	An automatic activity switch occurs when the primary server cannot communicate with the standby server. An automatic server activity switch involves the following sequence of high-level events. • The standby server cannot communicate with the primary server within 60 s, and the primary database cannot communicate with the primary server. • The standby server performs an activity switch to become the new primary server. (1) • If automatic database realignment is enabled, the new primary server attempts a database switchover. • The new primary server establishes a connection to the primary database and begins to manage the network. • The new primary server and the auxiliary servers synchronize the outstanding request information.	When the primary server detects a standby server communication failure, each GUI client receives notification of the failure. During an activity switch, each client GUI displays a main server status message. During an activity switch, a main server does not process SNMP traps from the network, and no NE resynchronizations occur. The auxiliary servers continue to process outstanding requests, and synchronize the request information with the new primary server after the activity switch. When the communication failure is resolved, each GUI client receives notification that redundancy is restored.
Server activity switch (manual)	A manual activity switch is typically performed for maintenance or testing purposes during a scheduled maintenance period. A manual server activity switch involves the following sequence of high-level events. • The new primary server establishes a connection to the primary database and begins to manage the network. • The new primary server and the auxiliary servers synchronize the outstanding request information. • If automatic database realignment is enabled, the new primary server attempts a database switchover. See Procedure 6-3 for information about performing a manual activity switch.	

Note
(1) This activity switch is allowed only if the primary server does not retain control of the primary database.

Table 6-2 summarizes the operations related to 5620 SAM database redundancy.

Table 6-2 5620 SAM database redundancy operations

Type	Description	Notes
Database switchover	A database switchover is a manual operation that reverses the primary and standby database roles, for example, for primary database maintenance, or to realign database roles with database stations after a server activity switch. A switchover can occur only when the primary and standby databases are functioning correctly and can communicate with each other. A database switchover involves the following sequence of high-level events. • A 5620 SAM administrator initiates the switchover on a primary or standby server. • The main server asks each auxiliary server to release all database connections. The switchover fails if all database connections are not released within 15 minutes. • The main server directs the standby database to become the primary database. • The main server restarts to fully synchronize information with the new primary database. See Procedure 6-4 for information about performing a database switchover.	No automatic database realignment occurs after a database switchover.
Database failover	A database failover is an automatic reversal of the primary and standby database roles, for example, after a primary database failure. A database failover involves the following sequence of high-level events. • No main server can communicate with the primary database within a period that is 2 min by default. • The currently active main server directs the standby database to become the primary database. • If automatic database realignment is enabled and the primary server and database are not aligned, the primary server performs an activity switch. • The primary server directs each auxiliary server to connect to the new primary database.	When the primary server detects a communication failure with the primary or standby database, the GUI clients are informed that the database is not reachable. After the cause of the communication failure is resolved, the GUI clients are notified that the database is reachable. After a failover, you must reinstantiate the former primary database as the new standby database. Database redundancy is not restored until reinstantiation is complete.
Re-establishing database redundancy	Re-establishing database redundancy is a user action that uses database reinstantiation to restore the former primary database as the new standby database. After a failover, the former primary database is not available for redundancy until an operator or the 5620 SAM reinstantiates it as the new standby database. See Procedures 6-6 and 6-7 for information about re-establishing database redundancy after a failover.	The following conditions must be true before you can re-establish database redundancy. • The failover completes successfully. • The station that contains the primary database is operational. • The former primary database proxy port is configured and in service.

Redundancy scenarios

The following are redundancy failure scenarios and the 5620 SAM response to each:

- primary server cannot communicate with primary database—If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs. If both the primary and standby servers cannot communicate to the primary database, the primary server initiates a database failover. If automatic database realignment is enabled and the primary server and new primary database are not aligned, the primary server performs a server activity switch.
- primary server cannot communicate with managed NEs—If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs. If automatic database realignment is enabled and the new primary server and the primary database are not aligned, the new primary server performs a database activity switch.
- primary server cannot communicate with primary database or managed NEs—If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs. If automatic database realignment is enabled and the primary server and new primary database are not aligned, the primary server performs a database activity switch.
- primary server cannot communicate with primary database, managed NEs, or standby server—The standby server activates to become the new primary server. If automatic database realignment is enabled, the new primary server initiates a database activity switch.
- primary and standby servers cannot communicate with primary database—The primary server initiates a database failover. If automatic database realignment is enabled and the primary server and new primary database are not aligned, the primary server performs a server activity switch.
- primary and standby servers cannot communicate with each other - primary server can communicate to primary database—The primary server continues to perform as a primary server and the primary database continues to perform as a primary database. An alarm will be raised to indicate the communication failure between primary server and standby server.
- primary and standby servers cannot communicate with each other - primary and standby servers can communicate to their respective preferred databases—The primary server continues to perform as a primary server and the primary database continues to perform as a primary database. The standby server will become the primary server and the standby database will become a primary database. There will be two separate primary servers and primary databases running in the network. An alarm will be raised to indicate the activity switch. The connected users will not get impacted as they continue their session with the original primary server. New users will continue to establish sessions with the original primary server. If a user explicitly tries to connect to a new primary server, the sessions will be established.

- primary and standby servers cannot communicate with each other—The primary server cannot communicate to its preferred database and the standby server cannot communicate with its preferred database.
- primary and standby server cannot communicate with the managed NEs—If both the primary server and standby server cannot communicate with the managed NEs but can communicate to the respective preferred databases, no server activity switch or database failover occurs. The NE status will be marked as not reachable and the appropriate reachability alarm will be raised.

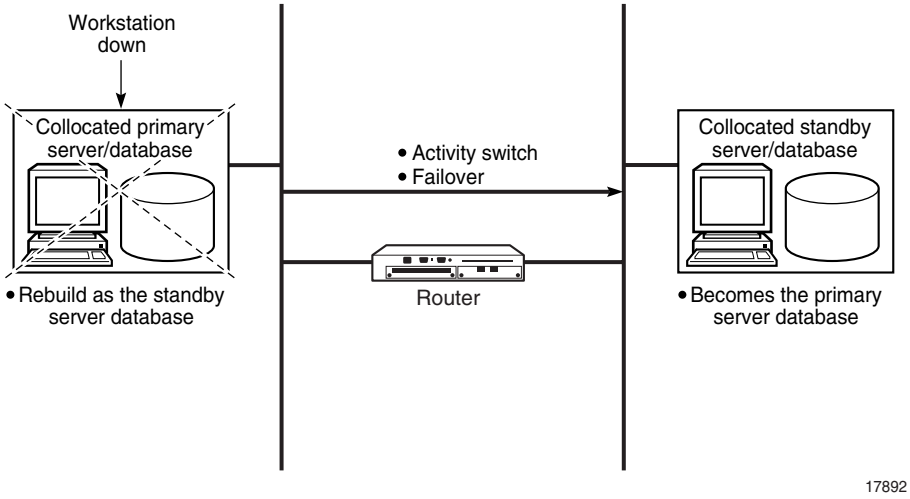
You can configure the following redundancy parameters to specify how a 5620 SAM system manages a loss of connection to the managed NEs:

- the number of elapsed seconds that constitute a loss of connectivity
- how often a main server refreshes the list of managed NEs
- the minimum number of NEs that must respond to a connectivity check

Contact your Alcatel-Lucent technical-support representative for more information.

Figure 6-11 shows the redundancy effect on a collocated configuration in which the station that hosts the primary server and database becomes unresponsive.

Figure 6-11 Primary database and server station down, collocated system

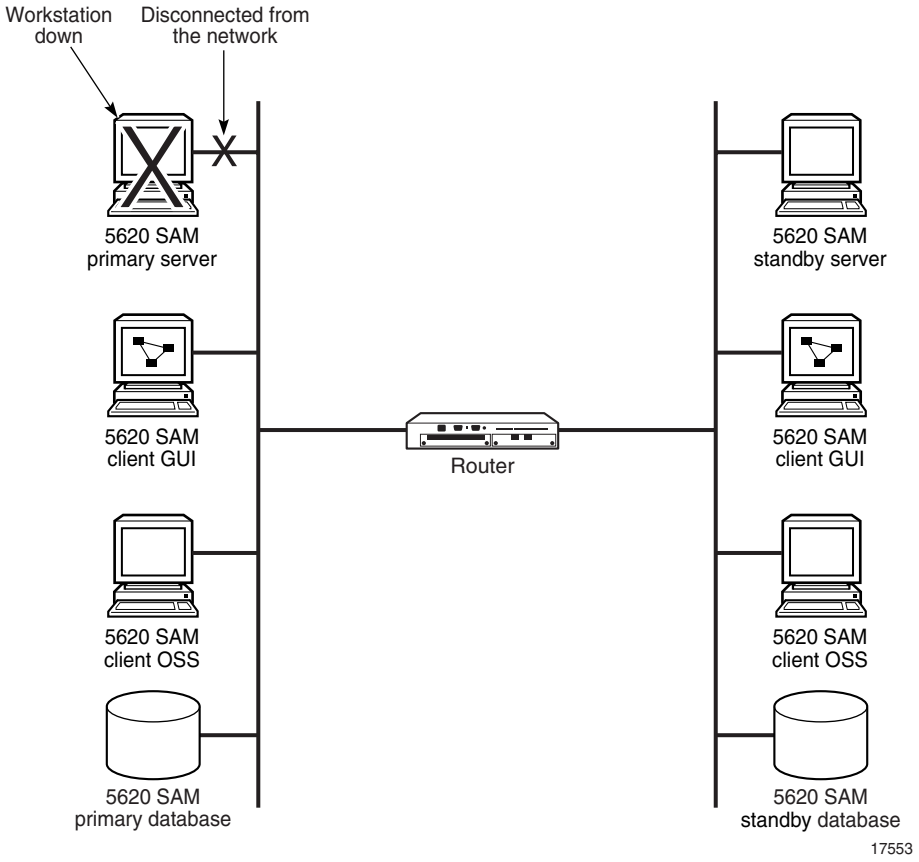


The following occurs when the primary station becomes unresponsive:

- The standby server and database become the primary server and database.
- Redundancy is not restored until the former primary station is rebuilt as the new standby station.

Figure 6-12 shows a primary server disconnection from the network in a distributed 5620 SAM system.

Figure 6-12 Primary server disconnected from network, distributed system

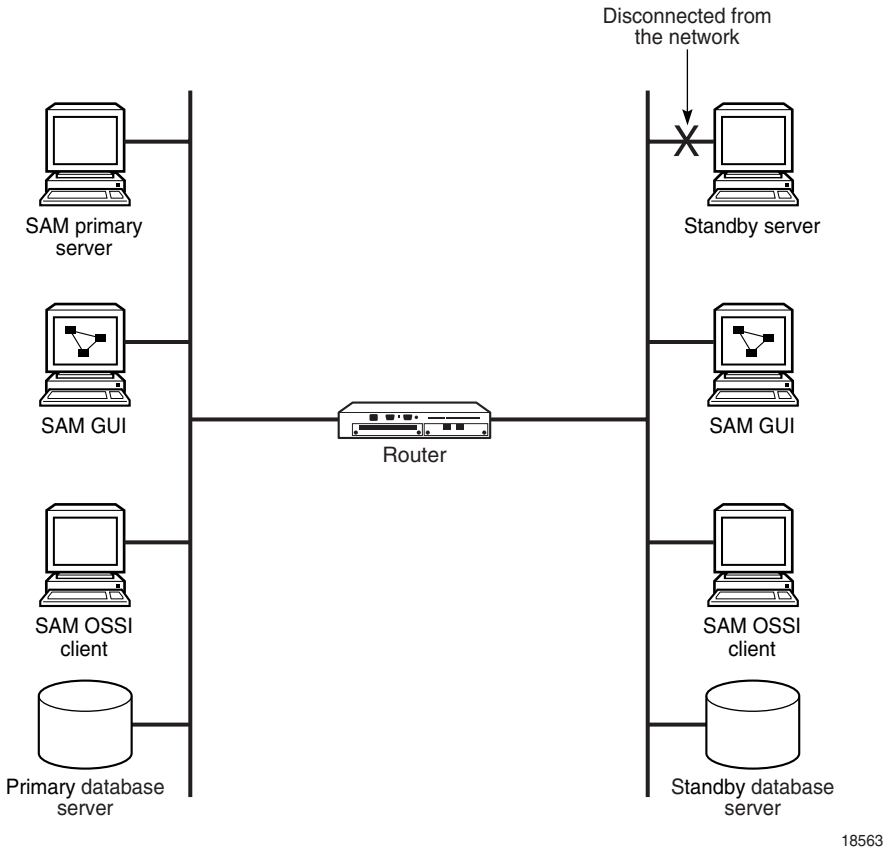


The following occurs when the primary server is disconnected from the management network:

- The standby server detects the loss of connectivity with the primary server and becomes the new primary server.
- The new primary server raises alarms about the unavailability of the former standby server and the activity switch.
- If automatic database realignment is enabled, the new primary server performs a database switchover.
- When connectivity is restored, the former primary server reconnects to the network as the new standby server.

Figure 6-13 shows a standby server disconnection from the network in a distributed 5620 SAM system.

Figure 6-13 Standby server disconnected from network, distributed system



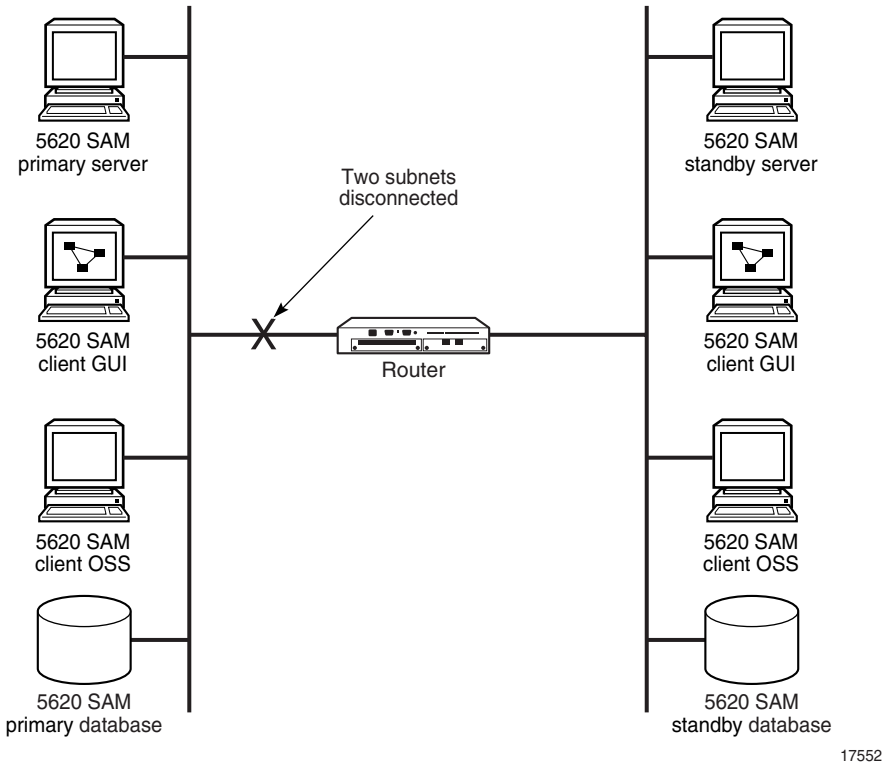
The following occurs when the standby server is disconnected from the network:

- The standby server tries to become the primary server because it cannot contact the primary server, so assumes that it is down.
- The primary server raises an alarm to indicate that the standby server is down.

After the standby server reconnects to the network, it resumes the role of standby server and the standby down alarm is cleared.

Figure 6-14 shows a network failure in a distributed 5620 SAM system.

Figure 6-14 Network failure, distributed system



The following occurs when the primary and standby servers are in separate subnets and cannot communicate:

- The original primary server raises an alarm about the standby server unavailability, and each GUI client displays the standby server status as Down.
- The standby server becomes a primary server. The original primary server continues to operate as a primary server.

Note — You can eliminate a single point of hardware or network failure by using redundant interfaces and redundant physical network paths. See the *5620 SAM Planning Guide* for more information.

6.2 Workflow for 5620 SAM system redundancy

1. Configure redundancy during 5620 SAM component installation. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.
2. Perform manual activity switches and switchovers as required.
   - **a** For 5620 SAM main servers:
     - **i** Verify the redundancy status of the 5620 SAM software.
     - **ii** Perform a manual activity switch on the primary server.
     - **iii** Validate the updated redundancy status.
   - **b** For 5620 SAM databases:
     - **i** Verify the redundancy status of the 5620 SAM software.
     - **ii** Perform a switchover, as required.
     - **iii** Validate the updated redundancy status.
3. After a failover, re-establish redundancy between the standby and primary databases.

6.3 5620 SAM system redundancy procedures

Use the following procedures to perform redundancy tasks.

Procedure 6-1 To view the 5620 SAM main server and database status

1. View the Standby Server and Standby DB status indicators in the 5620 SAM client GUI task bar. Each indicator should display Up.
2. Choose Administration→System Information. The System Information form opens with the General tab displayed.
3. View the general redundancy information:
   - Domain Name—the 5620 SAM domain name specified at installation
   - Redundancy Enabled—selected if redundancy is enabled
   - Alignment Enabled—selected if automatic database realignment is enabled; displayed only if the 5620 SAM system is redundant
   - Realignment Status—Aligned or Not Aligned
4. View the following information in the Primary Server panel:
   - Host Name—the host name of the primary or standalone main server
   - Status—Unknown, Down, or Up

5 View the following information in the Primary Database Server panel:

- Instance Name—the name of the primary database instance, also called a SID
- IP Address—the IP address that each main or auxiliary server uses to reach the primary database
- Host Name—the host name of the primary database, or of the database in a standalone 5620 SAM system

6 If the 5620 SAM system is redundant, view the following information in the Standby Server panel:

- Host Name—the host name of the standby main server
- Status—Unknown, Down, or Up

7 If the 5620 SAM system is redundant, view the following information in the Standby Database Server panel:

- Instance Name—the name of the standby database instance, also called a SID
- IP Address—the IP address that each main or auxiliary server uses to reach the standby database
- Host Name—the host name of the standby database

8 Click on the Properties button to display additional information about the primary or standalone 5620 SAM main server. The Main Server properties form opens.

9 View the following general main-server information:

- Host Name—the host name of the primary main server
- Server Type—Main
- Resource Managed—selected if the main server is included in 5620 SAM resource management

10 View the following information in the Client Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the 5620 SAM GUI and OSS clients through a NAT router
- Public IP Address—the IP address that the 5620 SAM GUI and OSS clients use to reach the main server through a NAT router

Note 1 — The Private IP Address and Public IP Address display 0.0.0.0 when the 5620 SAM clients and the main server use host names, rather than IP addresses, for communication.

Note 2 — The Private IP Address and Public IP Address display the same IP address when NAT is not used between the main server and clients.

11 View the following information in the Redundant Server Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the standby main server through a NAT router
- Public IP Address—the IP address that the standby main server uses to reach the primary main server through a NAT router
- Peer Public IP Address—the IP address that the standby main server uses to reach the main server

Note — The Private IP Address and Public IP Address display the same IP address when NAT is not used between the primary and standby main servers.

12 View the following information in the Auxiliary Server Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the auxiliary servers through a NAT router
- Public IP Address—the IP address that the auxiliary servers use to reach the primary main server

Note — The Private IP Address and Public IP Address display the same IP address when NAT is not used between the main server and the auxiliary servers.

13 Close the Main Server properties form. The System Information form reappears.

14 Click on the Database button to view more detailed database information, if required. See chapter 7 for information about the 5620 SAM database.

15 Click on the Faults tab to view alarm information, if required.

16 Close the System Information form.

Procedure 6-2 To view the 5620 SAM auxiliary server status

1 Choose Administration→System Information. The System Information form opens.

2 Click on the Auxiliary Servers tab button.

3 Review the list of auxiliary servers.

4 Select an auxiliary server in the list and click on the Properties button. The properties form for the auxiliary server opens.

5 Review the auxiliary server information, which includes the following:

- Host Name—the host name of the auxiliary server
- Port Number—identifies the port that the auxiliary server uses to communicate with each main server and database
- Auxiliary Server Type—Reserved or Preferred
- Server Status—Unknown, Down, Up or Unused
- Resource Managed—selected if the auxiliary server is included in 5620 SAM resource management
- Public IP address—the IP address that the main servers use to reach the auxiliary server
- Private IP address—displayed if NAT is used between the main servers and the auxiliary server

6 Perform one of the following:

a View the following main server information for a redundant 5620 SAM system:

- Server 1 Public IP address—the IP address that the auxiliary server uses to communicate with the primary or standby main server
- Server 2 Public IP address—the IP address that the auxiliary server uses to communicate with the primary or standby main server

b View the following main server information for a standalone 5620 SAM system:

- Server Public IP address—the IP address that the auxiliary server uses to communicate with the main server

7 Click on the Auxiliary Services tab button.

8 Review the list of auxiliary services.

9 Review the information for each auxiliary service, which includes the following:

- Service Name—the type of service, for example, statistics collection
- Selected—indicates whether this auxiliary server is currently used by a main server to process requests
- IP Address—the IP address that each main server uses to reach the auxiliary server
- Host Name—the host name of this auxiliary server
- Auxiliary Server Type—Reserved or Preferred

10 Close the Auxiliary Services form.

11 Click on the Faults tab to view alarm information, if required.

12 Close the System Information form.

Procedure 6-3 To perform a server activity switch

Perform this procedure to reverse the primary and standby roles of the main servers in a redundant 5620 SAM system. Consider the following before you perform a server activity switch.

- Each client GUI receives notification of a server activity switch.
- During a server activity switch, a main server does not process SNMP traps, attempt to synchronize NEs, or collect statistics.
- During a server activity switch, auxiliary servers process outstanding requests, but do not communicate with a main server.
- After a server activity switch, the new primary main server deploys outstanding configuration changes to NEs, establishes communication with the auxiliary servers, and synchronizes information with the auxiliary servers.
- A manual activity switch stops and starts the former primary main server. Server redundancy is unavailable until the former primary main server is fully initialized as the new standby main server.

1 Log in to the primary main server station as the samadmin user.

2 Open a console window.

3 Enter the following at the CLI prompt:

_install_dir_/nms/bin/nmsserver.bash force_restart ↵

where *install_dir* is the 5620 SAM server installation location, typically /opt/5620sam/server

The server activity switch begins. The primary main server restarts as the standby main server, and the former standby main server becomes the new primary main server.

4 Close the console window.

5 Clear alarms, as required. The activity switch alarms must be cleared manually.

6 Verify that the GUI and OSS clients can connect to the new primary main server.

Procedure 6-4 To perform a 5620 SAM database switchover using the 5620 SAM client GUI

Perform this procedure to use the 5620 SAM client GUI to switch the primary and standby database roles. Before you perform the procedure, ensure that you understand the following implications of a switchover.

- The primary and standby database roles are reversed.
- The primary main server connects to the new primary database.

- Archive logging begins on the new primary database.
- The primary main server directs each auxiliary server to connect to the new primary database.

1 Log in to the client GUI as a 5620 SAM user with the admin scope of command role.

2 Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.

3 Click on the Switchover button to begin the database switchover. A dialog box appears.

Note — The Switchover button is disabled when the proper switchover conditions are not in place, for example, when a switchover or failover is in progress.

4 Respond to the dialog-box prompt.

5 Click on the Yes button. The 5620 SAM server performs the database switchover.

6 Close the System Information form.

Procedure 6-5 To perform a 5620 SAM database switchover using a CLI script

Perform this procedure to use a CLI script to switch the primary and standby database roles. Before you perform the procedure, ensure that you understand the following implications of a switchover.

- The primary and standby database roles are reversed.
- The primary main server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary main server directs each auxiliary server to connect to the new primary database.

1 Log in to the primary main server station as the samadmin user.

2 Open a console window.

3 Enter the following at the CLI prompt:

install_dir*/switchoverdb.bash *username password ↵

where
install_dir is the 5620 SAM server installation location, typically /opt/5620sam/server
username and *password* are the login credentials for a 5620 SAM client account that has the required privilege level and scope of command

The script displays the following confirmation message:

```
The standby database will become the new primary database,
```

```
and the old primary will become the new standby.

Do you want to proceed? (YES/no) :
```

4 Enter the following case-sensitive text at the prompt to start the switchover:

YES ↵

The 5620 SAM server initiates a database switchover. Progress is indicated by a rolling display of dots in the console window. The database switchover is complete when the CLI prompt reappears.

5 Close the console window when the database switchover is complete.

Procedure 6-6 To reinstantiate a redundant database using the 5620 SAM client GUI

Perform this procedure to re-establish redundancy after a database failover or similar maintenance activity. This procedure reinstantiates the former primary database as the new standby database.

Before you start, the following conditions must be true:

- The primary database proxy and the standby database proxy are in contact with the 5620 SAM server.
- The database listener is operating.

1 Log in to the client GUI as a user with the 5620 SAM admin scope of command role.

2 Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.

3 Verify the database redundancy status matches the following:

- Failover State: Successful
- Switchover State: Not Attempted

4 Click on the Re-Instantiate Standby button. A dialog box appears.

5 Click on the Yes button to confirm. The database reinstantiation begins.

The client GUI status bar and the System Information form display the reinstantiation status. The Standby Re-instantiation State changes from In Progress to Success when reinstantiation is complete. The Last Attempted Standby Re-instantiation Time displays the start time of the current reinstantiation.

6 Close the System Information form when the reinstantiation is complete.

Procedure 6-7 To reinstantiate a redundant database using a CLI script

Perform this procedure to re-establish redundancy after a database failover or similar maintenance activity. This procedure reinstantiates the former primary database as the new standby database. Before you start, the following conditions must be true:

- The primary database proxy and the standby database proxy are in contact with the 5620 SAM server.
- The database listener is operating.

1 Log in to the primary main server station as the samadmin user.

2 Open a console window.

3 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

4 Enter the following at the CLI prompt:

./reinstantiatedb.bash -u *username* -p *password* ↵

where
username is the user name of a 5620 SAM client account that has the required privilege level and scope of command
password is the password for the user account

The script displays the following confirmation message:

```
This action will rebuild the standby database.

Do you want to proceed? (YES/no) :
```

5 Enter the following case-sensitive text at the prompt to begin reinstantiation:

YES ↵

The 5620 SAM server begins to reinstantiate the former primary database as the standby database. Progress is indicated by a rolling display of dots in the console window. Database reinstantiation is complete when the CLI prompt reappears.

6 Close the console window when the reinstantiation is complete.

7 — 5620 SAM database management

7.1 5620 SAM database management overview

The 5620 SAM database manager is used to perform 5620 SAM database administration and maintenance tasks that include the following:

- viewing and configuring database parameters
- backing up a database
- restoring a database
- managing database log storage
- troubleshooting a database

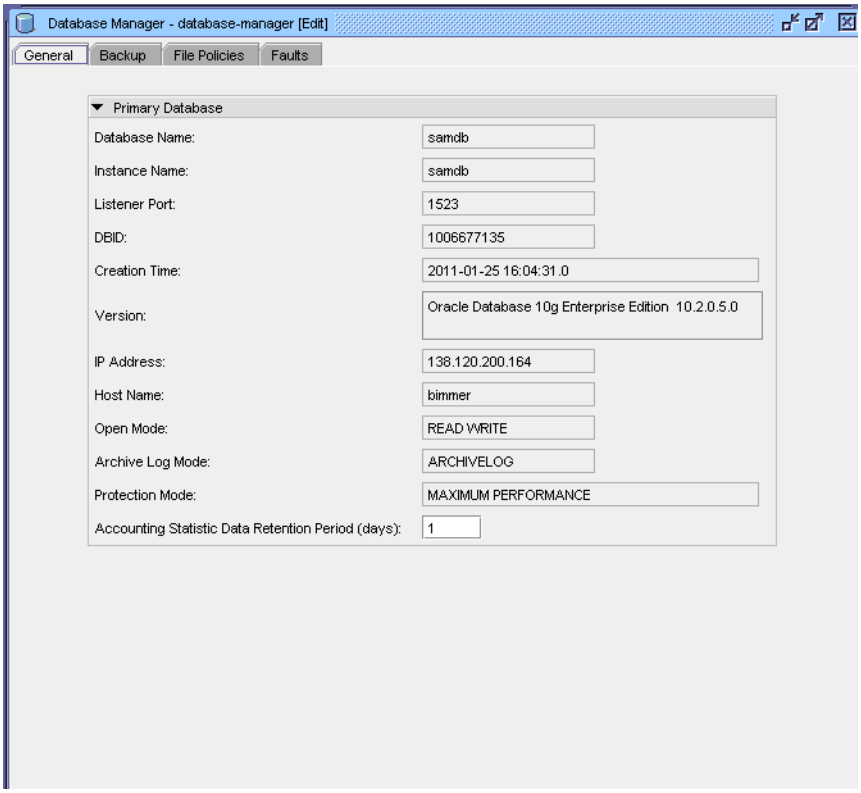
Note 1 — The 5620 SAM automatically backs up the Oracle encryption wallet during a database backup, and restores the wallet from the backup set during a database restore.

Note 2 — In a redundant deployment, the 5620 SAM automatically replicates the encryption wallet from the primary database to the standby database after the standby database is reinstantiated.

See the *5620 SAM Maintenance Guide* for information about restoring a 5620 SAM database.

Figure 7-1 shows the General tab of the Database Manager form.

Figure 7-1 Database Manager form — General tab



7.2 Workflow to manage the 5620 SAM database

1 Autodiscover the network. The database of the managed devices is stored in the 5620 SAM database.

2 Perform regular database management according to company policy.

- **i** Monitor the database as required.
- **ii** Back up the database as required. Alcatel-Lucent recommends that you back up the database daily.
- **iii** Manage disk space by configuring policies to limit the maximum size of database log files, such as the alert, trace, listener, and audit logs.

7.3 5620 SAM database procedures

Use the following procedures to perform database management tasks.

Procedure 7-1 To configure statistics data retention for the 5620 SAM database

1 Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens.

2 Configure the Accounting Statistic Data Retention Period (Days) parameter.

Caution — Configuring the Accounting Statistic Data Retention Period (Days) parameter can affect 5620 SAM system performance. Consult an Alcatel-Lucent support representative before you configure the parameter.

3 Click on the OK button. A dialog box appears.

4 Click on the Yes button.

5 Close the Database Manager (Edit) form.

Procedure 7-2 To view the database properties

Perform this procedure to view general information about the Oracle database that the 5620 SAM uses.

1 Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens and displays information that includes the following:

- Database Name—created during 5620 SAM installation; the default is samdb
- Instance Name—created during 5620 SAM installation; the default is samdb
- Listener Port—the port on the server used for database communication
- DBID—the Oracle database ID, sometimes referred to as the SID
- Creation Time—the database creation time
- Version—the Oracle version identifier, for example, Oracle Database 10g Enterprise Edition 10.1.0.5.0
- IP Address—the IP address that the server uses as the destination address for communicating with the database
- Host Name—the host name of the database station
- Open Mode—specifies the type of database access, either READ or READ WRITE
- Archive Log Mode—specifies whether to archive the database log files; this is configured during database installation
- Protection Mode—the database protection mode, which is set by default during installation to MAXIMUM PERFORMANCE

2 View the information.

3 Close the Database Manager (Edit) form.

Procedure 7-3 To back up the 5620 SAM database using the client GUI

Caution — Ensure that there is sufficient hard disk space to store the database backup. Alcatel-Lucent recommends that a separate database backup directory is created to store backup files. This backup directory should be at least five times larger than the expected database backup size. Contact your Alcatel-Lucent support representative or see the *5620 SAM Planning Guide* for more information.

Alcatel-Lucent recommends that you regularly back up the 5620 SAM database. A database backup provides a snapshot of the database that you can use to restore the network data. The reasons for performing a database backup include the following:

- To move a database from one workstation to another
- To recover from hardware or software errors

- To set aside a clean copy of the database before performing a system upgrade
- As a preventive measure before making major changes to the network

Note — During a database backup, the performance of database-related operations on the GUI or the OSS interface may be affected. Alcatel-Lucent recommends performing a database backup only during a period of low 5620 SAM activity.

1 The database must be in ARCHIVELOG mode to perform a backup. Perform Procedure 7-2 and ensure that Archive Log Mode is set to ARCHIVELOG.

2 Click on the Backup tab button.

3 Perform one of the following.

a Configure a scheduled full or partial database backup. A full backup backs up the entire 5620 SAM database whereas a partial backup contains no accounting statistics data.

i Configure the parameters.

Note — Ensure that the Scheduled Backup Directory location is not tampered with and has more than enough space to contain the number of database backups specified by the Number to Keep parameter.

ii Select the Schedule Enabled parameter.

b Perform an unscheduled full database backup. A full backup backs up the entire 5620 SAM database.

i Configure the Manual Backup Directory parameter.

Note — Ensure that the Manual Backup Directory location is not tampered with and has more than enough space to contain the database backup

ii Click on the Full Backup button. A dialog box appears.

iii Click on the Yes button. The full backup starts. The Backup State shown on the form changes to In Progress.

c Perform an unscheduled partial database backup. A partial backup contains no accounting statistics data.

i Configure the Manual Backup Directory parameter.

Note — Ensure that the Manual Backup Directory location is not tampered with and has more than enough space to contain the database backup

ii Click on the Partial Backup button. A dialog box appears.

iii Click on the Yes button. The partial backup starts. The Backup State shown on the form changes to In Progress.

4 View the information in the Backup Status panel, if required. This information includes the following:

- Scheduled Backup—whether a backup schedule is configured
- Backup State—the state of the current or previous backup operation; the Backup State is dynamically updated during a backup operation
- Next Scheduled Backup Time—the next scheduled backup time
- Last Successful Backup Time—when the previous successful backup completed
- Last Successful Backup Type—the type of previous successful backup completed
- Last Attempted Backup Time—when the previous attempted backup took place
- Last Attempted Backup Type—the type of backup that was last attempted
- Directory of the Last Successful Backup—the storage location of the previous successful backup

5 Close the Database Manager (Edit) form.

Note — After backing up and restoring a database, you must perform a full resynchronization of the network to discover the recent managed device information changes.

Procedure 7-4 To back up the database using a CLI script on Solaris

Caution — Ensure that there is sufficient hard disk space to store the database backup. Alcatel-Lucent recommends that a separate database backup directory is created to store backup files. This backup directory should be at least five times larger than the expected database backup size. Contact your Alcatel-Lucent support representative or see the *5620 SAM Planning Guide* for more information.

Alcatel-Lucent recommends that you regularly back up the 5620 SAM database. A database backup provides a snapshot of the database that you can use to restore the network data. The reasons for performing a database backup include the following:

- To move a database from one workstation to another
- To recover from hardware or software errors

- To set aside a clean copy of the database before performing a system upgrade
- As a preventive measure before making major changes to the network

Note — During a database backup, the performance of database-related operations on the GUI or the OSS interface may be affected. Alcatel-Lucent recommends performing a database backup only during a period of low 5620 SAM activity.

1 Log in as the Oracle management user on the database station. In a redundant 5620 SAM system, this is the station that holds the primary database.

2 Open a console window.

3 Enter the following at the console prompt to begin the database backup:

path*/install/config/samdb/SAMbackup.sh *backup_directory ↵

where
path is the 5620 SAM database installation location, typically /opt/5620sam/samdb
backup_directory is the directory that is to contain the database backup

Caution — When backing up the primary database, specify a backup directory that does not include the 5620 SAM database installation directory, or data loss may occur. A typical 5620 SAM database installation directory on Solaris is /opt/5620sam/samdb.

The database backup begins. A database backup can take several hours to complete.

4 Close the console window when the database backup is complete.

Procedure 7-5 To back up the database using a CLI script on Windows

Caution — Ensure that there is sufficient hard disk space to store the database backup. Alcatel-Lucent recommends that a separate database backup directory is created to store backup files. This backup directory should be at least five times larger than the expected database backup size. Contact your Alcatel-Lucent support representative or see the *5620 SAM Planning Guide* for more information.

Alcatel-Lucent recommends that you regularly back up the 5620 SAM database. A database backup provides a snapshot of the database that you can use to restore the network data. The reasons for performing a database backup include the following:

- To move a database from one workstation to another
- To recover from hardware or software errors

- To set aside a clean copy of the database before performing a system upgrade
- As a preventive measure before making major changes to the network

Note — During a database backup, the performance of database-related operations on the GUI or the OSS interface may be affected. Alcatel-Lucent recommends performing a database backup only during a period of low 5620 SAM activity.

1 Log in to the database station using an account with local administrator privileges.

2 Open a console window.

3 Enter the following at the console prompt to begin the database backup:

path*\install\config\samdb\SAMbackup.bat *backup_directory ↵

where
path is the 5620 SAM database installation location, typically C:\5620sam\samdb
backup_directory is the directory that is to contain the database backup

Caution — When backing up the primary database, specify a backup directory that does not include the 5620 SAM database installation directory, or data loss may occur. A typical 5620 SAM database installation directory on Windows is C:\5620sam\samdb.

The database backup begins. A database backup can take several hours to complete.

4 Close the console window when the database backup is complete.

Procedure 7-6 To manage alert, listener, trace, and audit database log files

You can use policies to manage the file size of stored alert, trace, listener, and audit log files. When the size and number of files are left unbounded, exceeding database disk space limits may become a problem. The default settings of the file policies reduce the number of log files that are kept.

Database log files are compressed and stored in the alert log directory (for trace, alert, and audit log files) or the listener directory for listener log files.

For historical or troubleshooting purposes, Alcatel-Lucent recommends that you archive the database log files.

1 Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens.

2 Click on the File Policies tab button.

3 Perform one of the following.

a Create a new database file policy.

i Click on the Database File Policies button. The Database File Policies form opens.

ii Click on the Create button. The File Policy (Create) form opens.

iii Configure the parameters:

- Policy ID
- Description
- Auto-Assign ID
- Purge Mode
- Max (Collective) Log Size (KB)
- Number of Archives

iv Click on the OK button. The File Policy (Create) form closes.

v Close the Database File Policies form.

b Modify an existing policy.

i Click on the Database File Policies button. The Database File Policies form opens.

ii If required, specify a filter and click on the Search button.

iii Select a policy from the list and click on the Properties button. The File Policy (Edit) form opens.

iv Configure the parameters:

- Description
- Purge Mode
- Max (Collective) Log Size (KB)
- Number of Archives

v Click on the OK button. The File Policy (Edit) form closes.

vi Close the Database File Policies form.

4 Associate the file policy with a database log type, if required.

i Click on the Select button beside one of the following:

- Alert Log File Policy
- Listener Logs File Policy
- Trace and Audit Logs File Policy

The Database File Policies - Database Manager (Edit) form opens.

ii Choose a policy from the list.

iii Click on the OK button. The Database File Policies - Database Manager (Edit) form closes and the policy identifier is displayed on the Database Manager (Edit) form.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Database Manager (Edit) form closes.

8 — 5620 SAM user security

8.1 5620 SAM user security overview

A 5620 SAM client GUI operator can use security management forms to configure and manage the following:

- 5620 SAM users and user groups, which are assigned the following configurable profiles:
  - scope of command profiles, which define the level of user control over objects in scope of command roles
  - span of control profiles, which define the 5620 SAM objects that users can view and manage
- 5620 SAM user-account and password expiry periods
- GUI inactivity timeout periods
- password history counts
- the number of active and allowed client sessions
- the GUI login form, which can display a customized login message
- user activity logs, which record the actions performed by each user

User accounts and user groups

You can use 5620 SAM user accounts and user groups to do the following:

- Provide GUI or OSS access to the 5620 SAM functional areas that match specific operator requirements.
- Restrict access to functions or objects based on operator expertise or authority.

Users have view access, read-write access, or no access to 5620 SAM objects and functions based on the following:

- the user group to which they belong
- the scope of command profile assigned to the user group.

The 5620 SAM user account called admin is created during 5620 SAM installation. The admin account is assigned the administrator scope of command role and a span of control profile that has Edit Access assigned to each default span. See "Scope of command" in this section for more information.

Note — To restrict user access to top-level 5620 SAM functions such as 5620 SAM and NE security management, Alcatel-Lucent recommends the following:

- Assign the administrator scope of command role to a minimal number of 5620 SAM user accounts.
- Assign each 5620 SAM user to a user group that has the minimum privileges for performing the required tasks.

Caution — Because the 5620 SAM is unable to obtain an authentication secret value from an NE, Alcatel-Lucent recommends that you use only the 5620 SAM to configure a shared authentication secret on an NE. If you configure a shared authentication secret on a managed NE using another interface, for example, a CLI, the 5620 SAM cannot synchronize the security policy with the NE.

Only the admin user, or a user whose scope of command includes write access to the security package, can perform the tasks listed in Table 8-1.

Table 8-1 5620 SAM security-related tasks

Task:	See:
Create a proprietary user login statement	Procedure 8-1
Specify expiry periods for user accounts, passwords, and GUI inactivity checks	Procedure 8-3
Specify responses to authentication failures	Procedure 8-4
Create or modify scope of command roles	Procedure 8-8
Create or modify scope of command profiles	Procedure 8-9
Create or modify span of control profiles	Procedure 8-11
Assign 5620 SAM objects to a span	Procedure 8-10
Create or modify user groups	Procedure 8-13
Create users and assign users to user groups	Procedure 8-14
Specify the maximum number of admin sessions	Procedure 8-14
Specify a default external user group	Procedure 8-17
Search for inactive user accounts	Procedure 8-19
Suspend and reinstate users	Procedure 8-20
Modify user passwords	Procedure 8-21
Send text messages and notifications to some or all GUI clients	Procedure 8-25
Shut down GUI or 5620 SAM-O JMS client sessions on a per-client basis	Procedure 8-26
View user logs	Procedure 8-27

(1 of 2)

Task:	See:
Enable LI management	Chapter 31

(2 of 2)

The following general rules apply to 5620 SAM users and user groups:

- Only database space limits the number of users and user groups that can be created.
- A user cannot belong to more than one user group.
- Only one session per user account can be open at the same time on a client station.
- A scope of command profile allows user-group access to one or more 5620 SAM functional areas.
- A span of control profile allows user-group access to one or more 5620 SAM managed objects.
- A user group is associated with only one scope of command profile that can contain multiple scope of command roles.
- A user group is associated with only one span of control profile that can contain multiple spans.
- The assigned user privileges determine the following for a GUI user:
  - the available 5620 SAM menu options
  - the parameters on object property forms that are configurable
- By default, each user group is assigned access to all 5620 SAM objects.
- A user inherits span of control access rights from their assigned user group.
- When you modify a user group, and a user in the group has an open client session, client operations may fail for the user. To put the new user group permissions into effect, the user must close the current client session and open a new session.
- You can modify, but not delete, a span of control profile that is assigned to a user group.

Password management

A 5620 SAM user password must observe the following constraints:

- be 8 to 100 characters long
- contain at least three of the following character types:
  - lowercase
  - uppercase
  - special
  - numeric
- not be the user account name in forward or reverse order
- not contain more than three consecutive instances of the same character
- be changed according to a configurable schedule to prevent account lockout
- not be reused as a new password for the same user account

Scope of command

The scope of command for a user defines what the user is allowed to do; it is a collection of one or more configurable roles, or sets of permissions. A scope of command profile that contains one or more roles, and the profile is subsequently applied to a user group. Each user in the group inherits the access rights specified in the scope of command profile.

Roles

A scope of command role specifies the read, create, update, and delete access permissions for a 5620 SAM object type or package. You can create custom roles by assigning specific access permissions to different 5620 SAM functional areas. These functional areas are organized in packages, methods, and classes.

Note 1 — When you enable the Create permission on a 5620 SAM package, method, or class, the Update permission is automatically enabled.

Note 2 — When you enable the Update permission on a 5620 SAM package, method, or class, the Create permission is not automatically enabled.

You can create an original scope of command role, or copy an existing role and modify the role permissions to create a new role. The 5620 SAM has several predefined scope of command roles. These roles are listed in Table 8-2 with a brief description of the access that each provides. A more specific role definition is available on each role properties form.

Note 1 — You cannot modify or delete a predefined role.

Note 2 — When you create a scope of command role, you must enable create, update/execute, and delete access to allow the modification of a class or package.

Table 8-2 Predefined 5620 SAM roles

Role	Access provided
Base Read-only	Read-only to all objects except for the objects in the SAM Security and Mirror Service Management roles
Administrator	GUI access, but no OSSI access, to all objects
User Management	5620 SAM user and group management
SAM Management and Operations	Database functions such as backup, restore, reinstantiation, and switchover Alarm administration such as acknowledgement, clearing, and setting severity-change thresholds General NE management functions such as discovery, deployment, mediation, polling, statistics management, and security management that includes modifying spans
Network Element Equipment Management	Physical equipment configuration and management
Service Management	Service, service component, and service template management functions, excluding mirror-service management

(1 of 2)

Role	Access provided
Old Service Template Management	Management of service templates deprecated in 5620 SAM Release 6.0
Subscriber Management	Customer and residential subscriber management
QoS/ACL Policy Management	General QoS and ACL policy management, Ethernet service and time of day suite policy management
Policy Management (except QoS/ACL)	Management of policies other than those in the QoS/ACL Policy Management role
Routing Management	Routing protocol, L2 forwarding, and bandwidth management
Tunnel Management	Service tunnel and underlying transport management
Network Element Software Management	NE software management functions
Fault Management	Functions such as alarm management and remote network monitoring
Service Test Management	STM functions such as creating, running and scheduling OAM tests
Script Management	XML API and CLI script management, excluding execution
Script Execution	XML API and CLI script execution
Mirror Service Management	Creation and management of mirror services and mirror-service components using the GUI
OSS Management	Use of the OSSI
Telnet/SSH Management	Telnet or SSH access to NEs from the GUI
Control Plane Assurance Manager (CPAM) Management	IP path and topology monitoring functions, and checkpoint and impact analysis functions in the 5650 CPAM
Control Plane Assurance Manager (CPAM) Topology	5650 CPAM route analysis functions
Control Plane Assurance Manager (CPAM) Topology Simulator	5650 CPAM route analysis functions using the topology simulator
Root Cause Analysis (RCA) Object Verification	RCA functions
Lawful Interception Management	LI configuration for mirror services, mediation policies, and NE security
Template Script Management	Service and tunnel template script management
Service Template Script Execution	Service template script execution
Tunnel Template Script Execution	Tunnel template script execution
Application Assurance (AA) Management	AA policy management
Format and Range Policy Management	Format and range policy management, service-creation span rules

(2 of 2)

Profiles

A scope of command profile contains one or more scope of command roles, and is assigned to a user group. Each user in the group inherits the permissions from the scope of command roles in the profile.

Span of control

The span of control for a user is a list of the objects over which the user has control, for example, a grouping of NEs or services. You can create an original span, or copy an existing span and modify the list of associated objects to create a new span. The objects that are in a span, or that can be added to a span, are called span objects.

The 5620 SAM has several predefined spans. Each new 5620 SAM object, for example, a discovered NE, is added to the corresponding predefined span. Table 8-3 lists the predefined 5620 SAM spans and the type of span objects in each.

Note — You cannot modify or delete a predefined span.

Table 8-3 Predefined 5620 SAM spans

Span	Included objects
Default Topology Group Span	Topology groups
Default Router Span	Managed NEs
Default Script Span	CLI and XML API scripts, service templates, tunnel templates, and auto-provision profiles
Default Test Suite Span	Test suites
Default Group Span	Ring groups and VLAN groups
Default Bulk Operation Span	Bulk operations
Default Service Span	Services
Default Customer Span	Customers
Default Transport Span	Optical wavelength services

Spans are specified in span of control profiles that are associated with user groups. A user can create a new 5620 SAM object only when the predefined span for the object type is in the span of control profile. For example, if you do not have the Default Group Span in your span of control profile, you cannot create a ring group.

NEs are added implicitly to a span when the parent topology group, ring group, or VLAN group is in a span. An object that is implicitly added to a span cannot be removed from the span, but an explicitly added object can be removed.

Note 1 — A user can view or configure a point-to-point connection only when each endpoint of the connection is in the user span of control. For example, if the endpoints of an LSP path are in different spans, you must have view or configuration privileges in each span in order to view or configure the LSP path.

Note 2 — During span modification, you can drag and drop NEs and topology groups into the span contents list.

Each user can control which objects the 5620 SAM displays in maps, lists, and navigation trees, based on the user span of control. The User Preferences form contains a parameter that globally specifies whether the Edit Access span objects of the user are shown by default. Objects that are not in a View Access span of the user are never displayed, regardless of the user preference. See chapter 2 for information about configuring the user span of control display preference.

In a list form, a user can override the global display preference using the Span On parameter. When the form is a filtered list form, such as a topology map, the Manage Services form or the Alarm Window, the associated advanced filter form contains a selector for filtering the search results based on the span of control. See chapter 2 for information about configuring span of control filters.

Profiles

A span of control profile is a collection of one or more spans that is assigned to a user group. Each span in a profile is assigned one of the following access designations during profile creation:

- View Access—The user can view the span objects, unless the scope of command permissions deny read access.
- Edit Access—The user can view and modify the span objects, unless the scope of command permissions deny access.
- Blocked Edit—The user can view but not modify the span objects, regardless of the scope of command permissions.
- Blocked View—The user cannot view or modify the span objects, regardless of the scope of command permissions.

Blocked Edit and Blocked View spans restrict access to a subset of the objects in another span in the same profile. For example, if multiple span of control profiles each contain the Default Service Span, you can add a customer-specific Blocked View or Blocked Edit span to each profile so that the user group associated with a profile can view or configure only the services of specific customers.

A Blocked Edit or Blocked View span takes precedence over other spans. For example, if a user has an Edit Access span that contains all services and a Blocked View span that contains Customer A and Customer B, the user cannot view or configure the services that belong to Customer A and Customer B.

Caution — Alcatel-Lucent recommends that you carefully plan and consider the effects of combining customer, service, and NE spans in a span of control profile. For example, a user can modify a service only when the service, customer, and participating NEs are in one or more Edit Access spans of the user, and none of these objects is in a Blocked Edit or Blocked View span.

To ensure that span conflicts do not interfere with network troubleshooting, the 5620 SAM allows a user to execute tests on NEs and service sites that are not in an Edit Access span of the user. However, activities such as policy distribution, software upgrades, and statistics collection can be performed only by a user with Edit Access spans that contain the target objects.

When you upgrade the 5620 SAM from a release earlier than 8.0 to Release 8.0 or later, the 5620 SAM automatically assigns all of the predefined spans to each existing span of control profile. The Default Customer and Default Service spans are assigned as Edit Access spans to preserve the existing user privileges; each of the other spans is assigned as a View Access span.

Span rules

By default, the 5620 SAM automatically adds a new service to the Default Service span. Using an OSS or GUI client, you can create policies called span rules that direct the 5620 SAM to add new services to other spans in addition to the Default Service span.

A span rule is associated with a format or range policy, and applies to the users and user groups named in the format or range policy. You can associate multiple range policies with one user and service type. This enables the automatic addition of a new service to a specific span based on the Service ID chosen during service creation.

During span rule creation, you must specify one of the following to indicate which spans receive the services that the user creates:

- the Edit Access spans of each user associated with the format or range policy
- each span that is explicitly named in the rule

The span rules associated with a format or range policy take effect for new services only if the format or range policy is administratively enabled and has a valid configuration that includes at least one user or user group.

See "Sample span rule configuration" in this chapter for a sample span rule configuration and implementation.

Remote authentication and authorization for users with no 5620 SAM user account

The 5620 SAM uses a JAAS security framework to provide authentication and authorization services. When a user logs in to the 5620 SAM, the authentication method used depends on the 5620 SAM login module configuration. The 5620 SAM supports the following remote authentication login modules:

- RadiusJaasLoginModule
- TacacsPlusJaasLoginModule

The JAAS security framework integrates the login modules with the 5620 SAM. During startup, the 5620 SAM reads a file that contains the JAAS login module configuration. Depending on the VSA configuration in the file, one of the following authentication and authorization methods is available for remote users that do not have a 5620 SAM user account:

- The remote server authenticates the user and the 5620 SAM assigns a user group.
- The remote server authenticates the user and assigns a user group.

When the 5620 SAM assigns a user group to a remote user, a default external user group must be present in the 5620 SAM. User authentication succeeds when the remote authentication server validates the user password. User authorization succeeds and the user is provided with access rights when the default external user group is associated with the user. The 5620 SAM then creates a temporary user account for the login session. In this scenario, when the default external user group is not specified, authorization fails and the user is denied access.

When the remote authentication server assigns a user group to a remote user, VSA support must be enabled in the JAAS login module configuration. In this scenario, a user group must be defined on the remote authentication server, and the remote server administrator must load the 5620 SAM RADIUS dictionary on the RADIUS server. The Sam-security-group-name VSA in the dictionary is used to configure a RADIUS remote user on the RADIUS server. The user group that is defined in the VSA must exist in the 5620 SAM. The remote authentication server administrator must specify the user group in the user configuration on the authentication server.

When the remote user logs in to the 5620 SAM, authentication succeeds when the remote authentication server validates the user password. Authorization succeeds and the user is provided with access rights when the user group defined on the remote server is sent to the 5620 SAM and validated. If the user group name matches a user group name in the 5620 SAM, the 5620 SAM creates a temporary user account for the login session. Otherwise, authorization fails and user access is not granted.

See Procedure 8-17 for information about how to configure remote authentication and authorization for remote-only users.

In RADIUS, the authentication success message that is sent to the 5620 SAM contains the user group name. In TACACS+, authentication must succeed before an authorization message containing the user group name is sent to the 5620 SAM.

Successful remote authentication for an OSS user requires that the remote server and the 5620 SAM use the same password format. The OSS users can log in using a clear text password or an MD5 hashed password if the remote authentication server supports MD5 password hashing. See the *5620 SAM-O OSS Interface Developer Guide* for more information.

When a remote 5620 SAM GUI or OSS session terminates, the 5620 SAM deletes the temporary user account for the session. The 5620 SAM also removes temporary OSS user accounts during 5620 SAM main server startup. You cannot modify a temporary user account.

Combined local and remote authentication

Many organizations already have existing TACACS+ or RADIUS authentication of users, based on long standing TACACS+ and RADIUS user accounts and passwords. You can incorporate new 5620 SAM user accounts for local 5620 SAM authentication with existing TACACS+ or RADIUS user accounts.

Consider the following:

- A system administrator can integrate the existing TACACS+ or RADIUS user accounts with 5620 SAM user accounts.
- You can create a 5620 SAM user name that exactly matches a TACACS+ or RADIUS user name.

- A 5620 SAM user name can be 1 to 80 characters in length, which is sufficient to match most remote authentication user names.
- 5620 SAM users who currently authenticate remotely can log in to the 5620 SAM using their RADIUS or TACACS+ passwords.
- 5620 SAM user authentication requires an account password that observes the 5620 SAM password constraints described in this chapter.

Note — When the samvsa parameter in the 5620 SAM JAAS configuration file is set to true, the 5620 SAM requires a user group from the remote server for authorization and the following conditions apply:

- If a 5620 SAM user account is associated with a local user group and configured to use remote authentication, the local user group is replaced by the remote user group.
- The user group sent by the remote server must exist in the 5620 SAM, otherwise, authentication fails.

The samvsa flag is set to false by default. See "Remote authentication and authorization for users with no 5620 SAM user account" in this chapter and Procedure 8-17 for more information about configuring the 5620 SAM VSA.

For example, a user named jane has the following accounts:

- a remote RADIUS account called jane and the password accessforjane
- a local 5620 SAM account called jane and the password LetJane1In!

When jane is authenticated by RADIUS, she gains access to the 5620 SAM by typing in jane and accessforjane. If the RADIUS server is down, jane is authenticated locally by the 5620 SAM after typing jane and LetJane1In!.

Client session control

Each 5620 SAM GUI client, 5620 SAM-O JMS client, or XML API request creates a 5620 SAM client session. You can view a list of the active 5620 SAM client sessions on the Sessions tab of the 5620 SAM User Security - Security Management form. Using this form, an admin user, or a user with an assigned security span of control, can also terminate one or more 5620 SAM GUI client sessions. When a 5620 SAM GUI client session is terminated in this manner, each client application receives a warning message and the connection is closed by the 5620 SAM server after a short delay.

Messaging connections

A list of active 5620 SAM GUI connections and 5620 SAM-O JMS connections can be viewed on the Messaging Connections tab of the 5620 SAM User Security - Security Management form. Using this form, an admin user, or a user with an assigned security span of control, can terminate one or more connections. When a 5620 SAM-O client connection is terminated, a notification is sent to the 5620 SAM-O client, but the admin user must also remove the 5620 SAM-O JMS client connection so that the server stops storing JMS messages for the session.

Client delegate sessions

The threshold for the number of 5620 SAM client sessions allowed on a client delegate server is configurable using the 5620 SAM GUI. When a user tries to open a client session that exceeds the threshold, the client delegate server opens the session, displays a warning message to the user, and raises an alarm. The threshold-crossing function can help to balance the session load across multiple client delegate servers. You require the Update user permission on the Server package to configure this threshold. See Procedure 8-23 for more information.

8.2 Sample 5620 SAM user authentication configuration

Figure 8-1 shows an example of how 5620 SAM user and user group authentication is performed.

Note 1 — RADIUS and TACACS+ authentication servers support multiple users. If the 5620 SAM cannot reach the first authentication server, the 5620 SAM sequentially attempts the user authentication using the remaining authentication servers.

Note 2 — If user authentication fails against the first authentication server in a sequence (for example, because of wrong password), there is no attempt to authenticate the user against the next authentication server in the sequence.

Note 3 — The EMS server log and 5620 SAM session log record unsuccessful user authentication attempts for known and unknown users. A user that is not defined in the 5620 SAM but belongs to an external AAA server is an example of an unknown user.

Figure 8-1 Sample 5620 SAM user and user group authentication

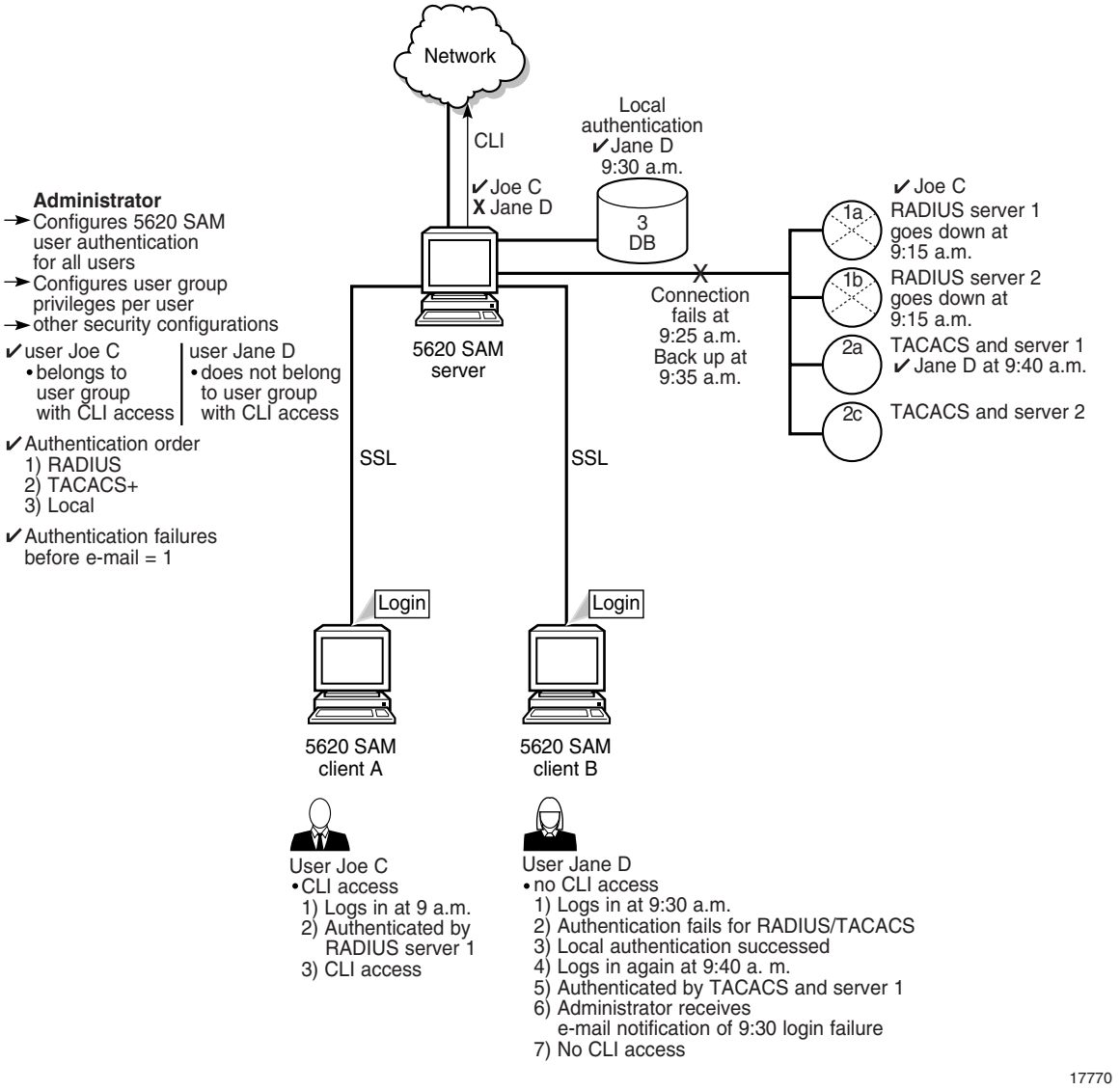


Table 8-4 lists the high-level tasks required to configure this sample.

Table 8-4 Sample 5620 SAM user authentication configuration

Task	Description
Pre-configurations	Ensure proper RADIUS or TACACS+ server configuration, according to your company requirements. PAP authentication is supported for RADIUS and TACACS+. The 5620 SAM server must be able to communicate with the authentication servers to validate users. All configuration tasks should be done with admin access. The 5620 SAM server IP address must be configured as the client of the RADIUS or TACACS+ server. The secret keys must match on the 5620 SAM server and the RADIUS or TACACS+ server.

(1 of 2)

Task	Description
1. Configure the remote authentication order for all users	Choose Administration→Security→5620 SAM RADIUS/TACACS+ User Authentication from the 5620 SAM main menu. Set the authentication order parameters to: • radius • tacplus • local Also specify the RADIUS and TACACS+ servers using the corresponding tabs on the same form.
2. Create scope of command profiles	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create a CLI scope of command profile and assign the default CLI management role to the profile. Create at least one scope of command profile that does not allow CLI access by assigning the *default* scope of command role, which has no access permissions to CLI management.
3. Create and configure user groups	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create a CLI user group and at least one user group that does not allow CLI access. Assign the scope of command profile with CLI management access to the CLI user group. Assign the scope of command profile with no CLI management access to the user group without CLI access. Authorization is done using user groups, so each user must belong to a user group with a local account on the 5620 SAM server.
3. Create and configure user accounts	You can create local users on the 5620 SAM by performing the following steps, or define remote users using RADIUS and TACACS+. The local users are available when RADIUS or TACACS+ authentication is not available. Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create users. Assign the appropriate user group to each user: one with CLI access and one without CLI access.
4.Configure notification	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Configure the authentication failure action parameters, including the parameters that allow the e-mail account of the administrator to be notified after login failure.

(2 of 2)

Consider the following:

- The 5620 SAM server acts as a network access server. A network access server is considered a client of a RADIUS or TACACS+ server.
- The sequence of activity between the 5620 SAM server, which is the authentication client, and the RADIUS or TACACS+ server, which is the authentication server, is the following:
  - client requests authentication
  - server replies to authentication request
  - client requests logout and authentication stops
- When the remote authentication servers are down and local authentication is used, the user must log in using 5620 SAM credentials, as described in "Combined local and remote authentication".

8.3 Sample span rule configuration

This section describes the configuration of a policy that directs the 5620 SAM to automatically add each service created for Customer X to an Edit Access span associated with the service creator. A user named Bob is designated the service administrator for Customer X; only Bob can create or edit Customer X services. A regular service user, by contrast, can only view the Customer X services.

Table 8-5 Sample span rule configuration

Task	Description
1. Create a span that contains the existing Customer X services.	• Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. • Choose Create→Span on the Span of Control tab. • Specify Customer X Services as the span name. • Use the Contents tab to specify the Customer X services.
2. Create a span of control profile for Bob.	• Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. • Choose Create→Profile on the Span of Control tab. • Add the Default Service Span as a View Access span to the span of control profile; the user cannot create a new service unless this is done. • Add the Customer X Services span as an Edit Access span to the span of control profile.
3. Create a range policy for each service type that the Customer X service administrator can create; in this sample, the services are IES and VPRN services.	• Choose Administration→Format and Range from the 5620 SAM main menu. • Choose Create→Range Policy. • Specify IES Service as the Object Type. • Specify Service ID as the Property Name. • Configure a range. • Use the Add button on the Users tab to assign the policy to Bob. • Choose Create→Range Policy. • Specify VPRN Service as the Object Type. • Specify Service ID as the Property Name. • Configure a range. • Use the Add button on the Users tab to assign the policy to Bob.
4. Create a span rule that contains the Customer X span.	• Choose Administration→Span Rules from the 5620 SAM main menu. • Specify Customer X Management as the name. • Set the Created In parameter to All listed spans. • Add the Customer X Services span using the Spans tab.

After the span rule is created, Bob creates a new VPRN service for Customer X. The 5620 SAM uses the VPRN range policy to automatically configure the service ID, and applies the associated Customer X Management span rule when Bob saves the service. As a result, the service is added to the Customer X Services span as well as to the Default Service Span. Because Bob has Edit Access to the Customer X Services span, he can reconfigure the service later, as required.

8.4 Workflow to manage 5620 SAM user and group security

1. Assess the requirements for user access to the different 5620 SAM functional areas and develop a strategy for implementing user security.
2. Create a proprietary client GUI login screen.
3. Set expiry periods for user accounts, passwords, and GUI inactivity timeouts.
4. Create scope of command roles in addition to the default roles, if required.
5. Create scope of command profiles according to types of tasks performed and assign scope of command roles accordingly.
6. Create spans in addition to the default spans, if required. Add 5620 SAM managed objects to the spans.

7 Create span of control profiles and assign spans.

8 Create user groups and assign scope of command and span of control profiles to each group, as required.

9 Create user accounts for performing the tasks that are assigned to each user group, as defined by the scope of command and span of control profiles associated with each user group.

10 Create span rules, as required, for automatically assigning new services to spans other than the Default Service Span.

11 Specify 5620 SAM RADIUS and TACACS+ authentication for 5620 SAM user accounts, as required. See chapter 18 for more information about managing security using RADIUS and TACACS+ authentication.

12 Configure authentication and authorization for remote users, if required, in which either the 5620 SAM provides the user group to which the user belongs or the remote authentication server provides the user group.

13 Manage user and group security by performing the following tasks, as required:

- create, modify and delete user groups
- create, modify and delete users
- suspend or re-instate users
- configure GUI inactivity timeout values
- configure password expiry

14 Monitor and manage the active client sessions, as required.

15 View the user and system logs, as required.

8.5 5620 SAM user and group security management procedures

This section provides procedures to create and manage users and user groups.

Procedure 8-1 To create a proprietary 5620 SAM login statement

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Configure the security statement parameters:

- Enabled
- Statement

3 Click on the OK button. A dialog box appears.

4 Click on the Yes button. The 5620 SAM User Security - Security Management (Edit) form closes.

The Statement parameter text is displayed on the login form during each subsequent client GUI login attempt.

Procedure 8-2 To reserve an admin account login

You can reserve one client GUI session, from the maximum number of sessions allowed by the license key, for admin users only. This allows an administrator to manage the existing client GUI sessions.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Configure the Reserve Administrator Login parameter.

3 Click on the OK button to save the changes and close the form. A dialog box appears.

4 Confirm the action by clicking on the Yes button.

5 Login as required.

Procedure 8-3 To configure expiry periods and a GUI inactivity timeout

You can configure global expiry periods for user accounts, passwords, and client GUI inactivity checks. You can configure per user group expiry periods for client GUI inactivity checks. You can enable a password history count.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Configure the Password History Duration and Password Reuse Cycle parameters.

3 Configure the global expiry period parameters:

- Account Expiry (days)
- Password Expiry (days)
- Client Timeout (minutes)
- Advance Password Expiry Notification (days)

If you set any of the parameters to 0, the corresponding expiry period check is disabled. To change the client inactivity check timeout for individual user groups, see Procedure 8-13.

4 Click on the OK button to save the changes and close the form. A dialog box appears.

5 Confirm the action by clicking on the Yes button.

When a user attempts to log in with an expired password, the user account is suspended. When a user updates her or his password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

Procedure 8-4 To configure authentication failure actions

You can specify an authentication message or a lockout for a user account that exceeds the configured number of login authentication attempts. Only non-admin accounts can be locked out, admin accounts always have access.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the E-mail tab button.

3 Configure the authentication failure action parameters:

- Attempts before lockout
- Attempts before e-mail
- E-mail Subject
- E-mail text

If you set the Attempts before lockout parameter to 0, the lockout function is disabled.

4 Click on the OK button to save the changes and close the form. A dialog box appears.

5 Confirm the action by clicking on the Yes button.

Procedure 8-5 To configure suspended account actions

You can specify a suspended account message for a user account when you suspend the user account using the User State parameter.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the E-mail tab button.

3 Configure the suspended account parameters:

- E-mail Subject
- E-mail text

4 Click on the OK button to save the changes and close the form. A dialog box appears.

5 Confirm the action by clicking on the Yes button.

Procedure 8-6 To configure automated e-mail delivery

Perform this procedure to specify the e-mail parameters for automated 5620 SAM messages to users and administrators; for example, when locking out a user account that exceeds the allowed number of authentication attempts.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the E-mail tab button.

3 Configure the outgoing e-mail server SMTP parameters:

- Server Name
- E-mail User Name
- E-mail User Password
- E-mail Address

4 Configure the Test Message parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The 5620 SAM User Security - Security Management (Edit) form closes.

Procedure 8-7 To configure client usage and activity logging

Activity log collection is enabled by default.

Note — A user with LI privileges can see and access LI-related activity and usage records. A 5620 SAM user with appropriate access can see all non-LI related activity and usage records.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM Usage and Activity Records from the 5620 SAM main menu. The 5620 SAM Usage and Activity Records form opens.

2 Click on the Log Policy button to specify how much data to collect and store in the log or whether to turn logging off. The appropriate logger configuration form opens.

   i Configure the parameters:

   - Retention Time (hours)
   - Administrative State

   Click on the Apply button to save the changes.

   ii Click on the Purge Log Records button to delete log records. Log records that meet storage specifications are stored and can be viewed. See the *5620 SAM Statistics Management Guide* for more information.

   iii Click on the OK or Cancel button to close the Edit Policy form.

3 Click on the Close button to close the 5620 SAM Usage and Activity Records form.

Note — The entries in the Activity Log Manager can assist you in identifying the user and action associated with a network problem. See the *5620 SAM Troubleshooting Guide* for more information.

Procedure 8-8 To create a scope of command role

Perform this procedure to create a set of user permissions that define an operator role. You can apply one or more scope of command roles to a user group using a scope of command profile.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab button.

3 Click on the Create button and choose Role. The Role (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Role ID
- Role Name
- Description

5 Perform the following steps to configure the permissions for the scope of command role.

i Click on the Permissions tab button. A list of the 5620 SAM packages, methods, and classes is displayed.

Note — When you enable the Create permission for a 5620 SAM package, method, or class, the Update/Execute permission is automatically enabled.

When you enable the Update/Execute permission for a 5620 SAM package, method, or class, the Create permission is not automatically enabled.

ii Select the required access permissions, which are displayed in the list column headings, for each package, class, or method that you want to assign to the scope of command role.

6 Click on the OK button. The Role (Create) form closes.

7 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-9 To create a scope of command profile

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab button.

3 Click on the Create button and choose Profile. The Scope of Command Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Profile ID
- Profile Name
- Description

5 Perform the following steps to assign one or more scope of command roles to the profile.

i Click on the Roles tab button.

ii Click on the Add button. The Select Scope Of Command Role(s) - Scope Of Command Profile form opens.

iii Select one or more roles and click on the OK button. The Select Scope of Command Role(s) - Scope Of Command Profile form closes and a dialog box appears.

iv Click on the OK button.

v Click on the OK button. The Scope of Command Profile (Create) form closes.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-10 To create a span of control

Perform this procedure to specify a set of 5620 SAM objects in a span of control and the type of user access available for the objects. You can apply one or more spans to a user group using a span of control profile.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Span of Control tab button.

3 Click on the Create button and choose Span. The Span (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Span ID
- Span Name
- Description

5 Click on the Contents tab button.

6 Click on the Add button and choose an object type from the menu. The Select *(object_type)* list form opens.

7 Select one or more objects and click on the OK button. The Select *(objects)* list form closes and the objects are listed on the Span (Create) form.

8 Click on the OK button. The Span (Create) form closes.

9 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-11 To create a span of control profile

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Span of Control tab button.

3 Click on the Create button and choose Profile. The Span of Control Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Profile ID
- Profile Name
- Description

5 Perform the following steps to assign one or more spans to the profile.

i Click on the Spans tab button. The predefined spans are listed.

ii Click on the Add button and choose an access type. The Select *access_type* Spans form opens.

iii Select one or more spans in the list and click on the OK button. The Select *access_type* Spans form closes, and a dialog box appears.

iv Click on the OK button. The spans are listed on the Span of Control Profile (Create) form with the type of access displayed in the Access Type column.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-12 To create a span rule

Perform this procedure to create a span rule. A span rule is a policy that specifies to which span of control profiles, in addition to the Default Service Span, a newly created 5620 SAM service is automatically assigned.

1 Using an account with an assigned security scope of command role, choose Administration→Span Rules from the 5620 SAM main menu. The Service Creation Span Rule (Create) form opens.

2 Configure the parameters:

- Auto-Assign ID
- Span Rule ID
- Name
- Created In

3 Perform the following steps to associate one or more spans with the rule.

i Click on the Spans tab button.

ii Click on the Add button. The Select Spans form opens.

iii Select one or more spans in the list.

iv Click on the OK button. The Select Spans form closes and the selected spans are listed on the Service Creation Span Rule (Crate) form.

4 Perform the following steps to associate one or more format or range policies with the rule.

i Click on the Format and Range Policies tab button.

ii Click on the Add button. The Select Format or Range Policies form opens.

iii Select one or more policies in the list.

iv Click on the OK button. The Select Spans form closes and the selected policies are listed on the Span Rule (Crate) form.

5 Click on the OK button. The Service Creation Span Rule (Create) form closes.

Procedure 8-13 To create a 5620 SAM user group

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the User Groups tab button.

3 Perform one of the following:

a Create a new group by clicking on the Create button. The User Group (Create) form opens with the General tab displayed.

b Modify an existing group by performing the following steps.

i Set the filter criteria.

ii Click on the Search button. A list of groups is displayed.

iii Select a group in the list and click on the Properties button. The User Group (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- User Group
- Description
- User Group State
- Apply Local Authentication Only
- Maximum User Sessions Allowed (maxUserSessionsAllowed)
- Account Expiry
- Password Expiry
- Override Global Timeout
- Client Timeout (minutes)

5 If the user group is indended for use by remote users, configure the parameters:

- Maximum GUI Sessions Allowed
- Maximum OSS Sessions Allowed
- Priority

6 Perform the following steps to assign a scope of command profile to the user group.

i Click on the Select button in the Scope of Command panel. The Select Scope of Command Profile form opens.

ii Select a profile in the list and click on the OK button. The Select Scope of Command Profile form closes, and the User Group (Create) form displays the scope of command profile name.

7 Perform the following steps to assign a span of control profile to the user group.

i Click on the Select button in the Span of Control panel. The Select Span of Control Profile form opens.

ii Select a profile in the list and click on the OK button. The Select Span of Control Profile form closes, and the User Group (Create) form displays the span of control profile name.

8 If you are creating a new user account, perform the following steps.

i Click on the OK button. The User Group (Create) form closes.

ii Go to step 15.

9 Click on the Format and Range Policies tab button.

10 Click on the Add button. The Select Format or Range Policies form opens.

11 Select one or more policies in the list and click on the OK button.

12 Click on the OK button. A dialog box appears.

Note — When you change the scope of command or span of control profiles of a group, the permissions of each user in the group are altered immediately when you click on the OK button.

13 Click on the Yes button. The User Group (Create) form closes.

14 If an active client GUI session is affected by the user group modification, restart the GUI client.

15 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-14 To create a 5620 SAM user account

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab button.

3 Perform one of the following:

a Create a new user account by clicking on the Create button. The User (Create) form opens with the General tab displayed.

b Modify an existing user account by performing the following steps.

i Set the filter criteria.

ii Click on the Search button. A list of user accounts is displayed.

iii Select an account in the list and click on the Properties button. The User (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- User Name
- Description
- User State
- E-mail Address
- Priority
- First Time Login Password Change
- User Password
- Confirm Password
- Maximum Sessions Allowed
- Maximum OSS Sessions Allowed
- Valid Client IP address
- Enable IP Address validation

Note — If the user account is for a remote user, you cannot configure the Maximum Sessions Allowed, Maximum OSS Sessions Allowed, or Priority parameters. For remote users, these parameters are derived from the user group configured on the user account.

5 You can test the validity of the user e-mail address by clicking on the Test E-mail button beside the E-mail Address parameter.

Note — Before you test the validity of the user e-mail address, ensure that the outgoing SMTP e-mail server and e-mail test message are configured. See Procedure 8-6 for information about configuring the outgoing e-mail server and test message.

6 Perform the following steps to choose a user group for the user account.

i Click on the Select button. The groupName form opens.

ii Select a user group in the list and click on the OK button. The groupName form closes, and the User (Create) form displays the user group name.

7 If you are creating a new user account, perform the following steps.

i Click on the OK button. The User Group (Create) form closes.

ii Go to step 13.

8 Click on the Format and Range Policies tab button.

9 Click on the Add button. The Select Format or Range Policies form opens.

10 Select one or more policies in the list and click on the OK button.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The User (Edit) form closes.

13 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-15 To copy a 5620 SAM user account

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab button.

3 Set the filter criteria and click on the Search button. A list of configured users opens.

4 Choose a user from the list and click on the Properties button. The User *type_of_user*, Group *user_group* (Edit) form opens.

5 Click on the Copy button. A User (Create) form opens for the second user.

6 Configure the parameters, as required. You must change the User Name parameter and configure the User Password and Confirm Password parameters.

7 Click on the OK button to save the changes and close the form.

8 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-16 To create RADIUS and TACACS+ authentication policies for 5620 SAM user accounts

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM RADIUS/TACACS+ User Authentication from the 5620 SAM main menu. The RemoteAuthenticationManager (Edit) form opens with the General tab displayed.

2 Configure the parameters:

- Authentication Order 1
- Authentication Order 2
- Authentication Order 3

3 Click on the RADIUS tab button to configure RADIUS authentication server parameters.

4 Click on the Add button. The SAM RADIUS Authentication Server (Create) form opens.

5 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Address
- Port
- Retry Attempts
- Timeout (seconds)
- Secret Name

6 Click on the OK button to save the changes.

7 Verify the action.

8 Click on the TACACS tab button to configure TACACS+ authentication server parameters.

9 Click on the Add button. The SAM TACACS Authentication Server (Create) form opens.

10 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Address
- Timeout (seconds)
- Secret Name

11 Click on the OK button to save the changes.

12 Verify the action.

13 Click on the Faults tab to view alarms, as required.

14 Click on the OK button to save the changes and close the form.

Procedure 8-17 To configure remote authentication and authorization for remote-only users

Note 1 — Ensure that remote authentication is enabled. See Procedure 8-16 for information about creating RADIUS and TACACS+ authentication policies.

Note 2 — See "Remote authentication and authorization for users with no 5620 SAM user account" in section 8.1 for information about remote authentication and authorization for remote-only users.

1 Perform one of the following:

a To configure remote authentication and authorization for remote-only users where the 5620 SAM provides the user group to which the user belongs, go to step 2.

Note — The samvsa flag must be set to false in the SamJaasLogin.config file. The default value is false. The SamJaasLogin.config file is located in the server installation configuration directory, typically C:\5620sam\client\nms\config or /opt/5620sam/server/nms/config.

b To configure remote authentication and authorization for remote-only users where the remote authentication server provides the user group to which the user belongs, go to step 3.

2 Specify the default external user group.

i Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

ii Configure the default external user group parameter: User Group.

iii Click on the Select button. The Select Group - TSecurityManager form opens.

iv Select a user group and click on the OK button. The Select Group - TSecurityManager form closes and the 5620 SAM User Security - Security Management (Edit) form refreshes with the selected user group.

v Click on the OK button. A dialog box appears.

vi Click on the Yes button. The 5620 SAM User Security - Security Management (Edit) form closes.

3 Modify the SamJaasLogin.config file.

Note — Ensure that you create a backup of the SamJaasLogin.config file before you make any modifications to it.

i Log in to the 5620 SAM main server station using an account with local administrator privileges.

Note — If the 5620 SAM main server is installed on Solaris, you must log in as the samadmin user.

ii Navigate to the server configuration directory, typically C:\5620sam\client\nms\config or /opt/5620sam/server/nms/config.

iii Open the SamJaasLogin.config file using a text editor.

iv If RADIUS authentication is enabled, find the RADIUSLogin section of the file and change the samvsa flag to true. The following is an example of the file text:

```
RADIUSLogin
{
  com.timetra.nms.jaas.provider.radius.auth.RadiusJaasLoginM
odule REQUIRED
debug=false
  samvsa=true
;
};
```

If TACACS+ authentication is enabled, find the TACACSLogin section of the file and change the samvsa flag to true. The following is an example of the file text:

```
TACACSLogin
{
  com.timetra.nms.jaas.provider.tacacs.auth.TacacsPlusJaasLo
ginModule REQUIRED
debug=false
  samvsa=true
;
};
```

v Save the changes to the file.

vi Close the file.

vii If the 5620 SAM main server is installed on Solaris, enter the following at the CLI prompt:

***path*/nms/bin/nmsserver.bash read_config** ↵

where
path is the 5620 SAM server installation location, typically opt/5620sam/server

viii If the 5620 SAM main server is installed on Windows, enter the following at the CLI prompt:

***path*\nms\bin\nmsserver.bat read_config** ↵

where
path is the 5620 SAM server installation location, typically C:\5620sam\server

The 5620 SAM server puts the configuration changes into effect.

4 Define the user group VSA on the remote authentication server.

Note — Step 4 must be performed by the remote authentication server administrator.

Perform one of the following:

a If RADIUS authentication is enabled:

i Copy the example of the RADIUS dictionary below to the RADIUS dictionary file. Enter changes to the file based on your RADIUS configuration.

ii Configure the RADIUS user profile and add a previously defined 5620 SAM user group name to the Sam-security-group-name VSA. The following is an example of the RADIUS user group VSA:

```
Sam-security-group-name="user_group_name_locally_defined
_in_5620SAM"
```

The VSA configuration file contains information such as usernames, passwords, and the 5620 SAM user group name. The user authentication process returns the user group name in the Sam-security-group-name VSA of the access-accept message.

The following is an example of the RADIUS dictionary text:

```
############################################################
###
#           Alcatel-Lucent 5620 SAM Server
dictionary.    #
#  $Id: dictionary.alcatel.sam,v
1.1 2006/08/18 10:00:22$ #
############################################################
####

VENDOR          Alcatel-Lucent                      123

BEGIN-VENDOR                            Alcatel-Lucent
```

```
ATTRIBUTE       Sam-security-group-name      3       stri
ng

END-VENDOR                                  Alcatel-Lucent
```

Note 1 — The user group must be a valid user group in the 5620 SAM.

Note 2 — The vendor ID must be 123.

b If TACACS+ authentication is enabled, define the 5620 SAM user group VSA in the user profile on the TACACS+ server. The following is an example of the TACACS+ user group VSA:

```
service=sam-app{
  sam-security-group="user_group_name_locally_defined_in_562
0SAM"
}
```

Note — The user group must be a valid 5620 SAM user group.

Procedure 8-18 To save activity or usage logs to a file

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM Usage and Activity Records from the 5620 SAM main menu. The 5620 SAM Usage and Activity Records form opens.

2 Choose a type of user log from the object drop-down list:

- Database Log to view information about changes to the database due to actions performed by the client
- Deployment Log to view information about deployment requests sent from the client
- Session Log to view information about the current client session, including operations performed and permissions for the logged-in user account
- User Read Log to view information about data viewed by users of the client
- User Request Log to view information about user requests sent from the client

3 Specify a filter to create a filtered list of logs, and click on the Search button. The list of logs opens.

4 Highlight the log records that appear in the search list.

5 Right-click on a column heading and choose Save to File from the contextual menu. The Save form appears.

6 Save the results.

- i To choose a directory in which to save the listed information, use the Save In parameter.
- ii To create a filename, use the File Name parameter.
- iii Choose HTML or CSV from the File of Type drop-down menu.
- iv Click on the Save button. The results of the inventory search are saved to the specified HTML or CSV file.

7 Click on the Close button to close the 5620 SAM Usage and Activity Records form.

Procedure 8-19 To search for inactive user accounts

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Users tab button.

3 Click on the Inactive User Search button and perform one of the following.

- a Choose >= 90 Days.
- b Choose >= 180 Days.
- c Choose Custom. The User Inactivity Period form opens.
  - i Enter a value for User inactive for >=.
  - ii Click on the OK button to close the form and return to the Inactive User Search form.

4 All user accounts are displayed that have been inactive for a number of days greater than or equal to the value entered in step 3.

5 Take action for inactive user accounts as required.

Procedure 8-20 To suspend or reinstate a 5620 SAM user account

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab.

3 Specify a filter to create a filtered list of users and click on the Search button.

4 Choose a user from the user list.

5 Click on the Properties button. The User *type_of_user* (Edit) form opens.

6 Suspend or re-instate the user.

   a To suspend the user, set the User State parameter to suspended.

   b To re-instate the user, set the User State parameter to active.

7 Click on the Apply button to save the changes.

8 Verify the action.

9 Close the form.

Procedure 8-21 To administratively change the password of a 5620 SAM user

The system administrator uses the Security Management form to maintain user accounts. The user can change their password in a separate form. If a user forgets their password, the system administrator can change the password and inform the user of the new password.

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab button.

3 Specify a filter to create a filtered list of users and click on the Search button.

4 Choose a user from the user list.

5 Click on the Properties button. The User *type_of_user* (Edit) form opens.

6 Configure the User Password parameter and the Confirm Password parameter.

7 Click on the Apply button to save the changes.

8 Verify the action.

9 Close the form.

When a user attempts to log in with an expired password, the user account is suspended. When a user updates her or his password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

Procedure 8-22 To change the password of the current 5620 SAM user

Users change their password in the Change Password form.

1 Start the 5620 SAM and login using your user name and password.

2 Choose Administration→Security→Change Password from the 5620 SAM main menu. The Password Change form opens.

3 Verify that the Login Name matches your user account name.

4 Configure the parameters:

- Old Password
- New Password
- Confirm Password

5 Click on the OK button to save the changes.

6 Confirm the action, as required.

7 Close the form.

When a user attempts to log in with an expired password, the user account is suspended. When a user updates her or his password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

Procedure 8-23 To configure the number of allowed client sessions for a client delegate server

Note — The 5620 SAM continues to accept new client sessions from a client delegate server after the allowed number of sessions is reached. The maximum number of sessions is to be used as a guide for balancing the client session load among multiple client delegate servers.

1 Using an account with Update permission on the Server package, choose Administration→System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.

2 Click on the Client Delegate Servers tab button.

3 Configure the filter criteria. A list of client delegate servers is displayed.

4 Select an entry in the list and click on the Properties button. The Client Delegate Server (Edit) form opens.

5 Configure the Maximum UI Sessions parameter.

6 Click on the OK button. The Client Delegate Server (Edit) form closes and the System Information form reappears.

7 Closes the System Information form.

Procedure 8-24 To view and manage the active 5620 SAM client sessions

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Sessions tab button.

3 Specify a filter to create a filtered list of GUI or 5620 SAM-O JMS client sessions and click on the Search button. The list of currently active client sessions opens.

4 Review the following session information:

- user name logged in for the client GUI session
- ID of the session
- time and date that the session started
- user group privileges for the session
- type of client, either a GUI (5620 SAM) or 5620 SAM-O JMS (SAMOSS) client
- IP address of the client

5 Perform one of the following:

a Close the form.

b Choose a session from the list and click on the Close Session button to shut down the client session.

Note — There are additional dependencies for closing a 5620 SAM-O session. See Procedure 8-26 for more information.

6 Validate the action.

7 Close the form.

Procedure 8-25 To send a text message to 5620 SAM GUI users

Administrative users can send broadcast messages to some or all active GUI users logged into the 5620 SAM. This is useful for sending maintenance and similar notifications to active users.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Sessions tab button.

3 Specify a filter to create a filtered list of GUI client sessions and click on the Search button. A list of active client sessions is displayed.

4 Select the required client sessions in the list.

5 Click on the Text Message button. The Text Message form opens.

6 Enter your text message in the Text Message form and click on OK. The text message is sent to the selected clients.

7 Close the Security Management (Edit) form.

Procedure 8-26 To disconnect a 5620 SAM-O JMS client connection or remove a durable subscription

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Messaging Connections tab button.

3 Specify a filter to create a filtered list 5620 SAM-O JMS client connections and click on the Search button. The list of currently active client connections opens.

4 Perform one of the following:

a Choose a JMS connection from the list and click on the Close Connection button to shut down the client connection. The connection to the server is terminated when you close a durable JMS connection, however, the subscription continues to store JMS messages.

b Choose a JMS connection from the list and click on the Remove Connection button to shut down the client connection and remove the durable subscription. The server stops storing the JMS messages for the session.

Note — When you remove a durable subscription, the OSS client can still attempt to connect to the 5620 SAM-O server. You can prevent an OSS client from attempting to connect by suspending the OSS user account. See Procedure 8-20 for more information.

5 Validate the action.

6 Close the form.

Procedure 8-27 To view client usage and activity logs

Activity log collection is enabled by default.

Note — A user with LI privileges can see and access LI-related activity and usage records. A 5620 SAM user with appropriate access can see all non-LI related activity and usage records.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM Usage and Activity Records from the 5620 SAM main menu. The 5620 SAM Usage and Activity Records form opens.

2 Choose a type of user log from the object drop-down list:

- Database Log to view information about changes to the database due to actions performed by the client
- Deployment Log to view information about deployment requests sent from the client
- Session Log to view information about the current client session, including operations performed and permissions for the logged in user account
- User Read Log to view information about data viewed by users of the client
- User Request Log to view information about user requests sent from the client

3 Specify a filter to create a filtered list of logs, and click on the Search button. The list of logs opens.

4 To edit the log, choose a log from the list and click on the Properties button. The log opens. Review the log information. See the *5620 SAM Troubleshooting Guide* for more information about reading and interpreting logs.

The information displayed depends on the type of log. For example, user read logs display:

- username logged in for the client session
- timestamp information
- type of operation performed; for example, configuration
- user account name that performed the operation
- target class against which the operation was performed
- information about the actions performed, based on the log type

When you are finished editing the log, click on the Close button to close the log.

5 Click on the Close button to close the 5620 SAM Usage and Activity Records form.

Note — The entries in the Activity Log Manager can assist you in identifying the user and action associated with a network problem. See the *5620 SAM Troubleshooting Guide* for more information.

Procedure 8-28 To delete a scope of command role

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab button.

3 Choose Role (Security) from the object drop-down list and click on the Search button. A list of scope of command roles is displayed.

4 Select a role in the list and click on the Delete button. A dialog box appears.

Note 1 — You cannot delete a predefined scope of command role.

Note 2 — You cannot delete a scope of command role that is assigned to a scope of command profile when the scope of command profile is assigned to a user group that contains users.

5 Click on the Yes button. The 5620 SAM deletes the scope of command role.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-29 To delete a scope of command profile

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab button.

3 Choose Profile (Security) from the object drop-down list and click on the Search button. A list of scope of command profiles is displayed.

4 Select a profile in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a scope of command profile that is assigned to a user group that contains users.

5 Click on the Yes button. The 5620 SAM deletes the scope of command profile.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-30 To delete a span of control

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Span of Control tab button.

3 Choose Span (Security) from the object drop-down list and click on the Search button. A list of spans is displayed.

4 Select a span in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a default span, or a span in a span of control profile that is assigned to a non-empty user group.

5 Click on the Yes button. The 5620 SAM deletes the span of control.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-31 To delete a span of control profile

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Span of Control tab button.

3 Choose Profile (Security) from the object drop-down list and click on the Search button. A list of span of control profiles is displayed.

4 Select a profile in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a span of control profile that is assigned to a non-empty user group.

5 Click on the Yes button. The 5620 SAM deletes the span of control profile.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-32 To delete a 5620 SAM user group

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the User Groups tab button.

3 Configure the filter criteria and click on the Search button. A list of user groups is displayed.

4 Select a group in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a user group that contains users.

5 Click on the Yes button. The 5620 SAM deletes the user group.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 8-33 To delete a 5620 SAM user account

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Users tab button.

3 Configure the filter criteria and click on the Search button. A list of user accounts is displayed.

4 Select an account in the list and click on the Delete button. A dialog box appears.

Note — When a user account is associated with a scheduled task, you must decide whether to remove the schedules. If you do not want to remove the schedules, no schedules are removed. If you do want to remove schedules, the schedules associated with the user account are removed if the schedule is not associated with a scheduled task. Schedules that are associated with a scheduled task are not removed.

5 Click on the Yes button. The 5620 SAM deletes the user account.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

9 — 5620 SAM SSL security

9.1 5620 SAM SSL security overview

SSL is used for data encryption, server authentication, and message integrity between a 5620 SAM main server and the following 5620 SAM components:

- single-user GUI clients
- client delegate servers
- OSS clients
- auxiliary servers

You can configure SSL on the EJB, JMS, and HTTP interfaces of single-user 5620 SAM GUI clients and client delegate servers, and on the JMS and HTTP interfaces of 5620 SAM OSS clients. When SSL is configured on an HTTP interface, it is called HTTPS.

Note — Alcatel-Lucent recommends using the JKS keystore format for 5620 SAM.

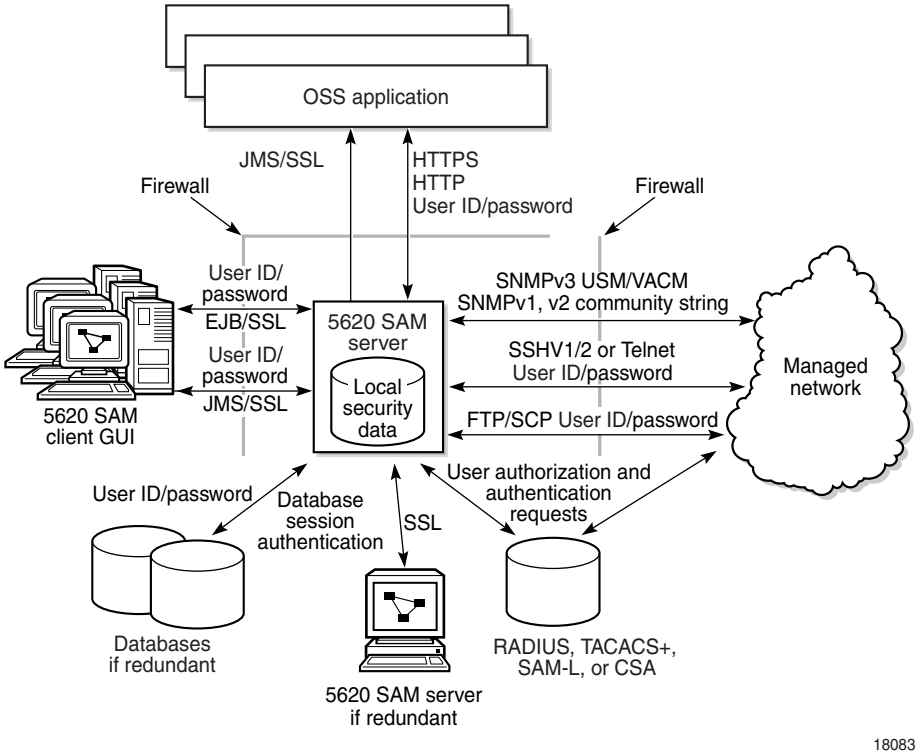
If the keystore is of a different type, for example, PKCS12, the java keytool utility can be used to convert the keystore to JKS format. The example below shows you how to convert a keystore from PKCS12 format to JKS.

```
<SAM_SERVER>/jre/bin/keytool -importkeystore -deststorepass changeit
-destkeypass changeit -destkeystore samserver.keystore -srckeystore
src_pkcs12_samserver.keystore -srcstoretype  PKCS12  -srcstorepass
srcpkcs12KeystorePassword -alias srckeystoreAlias
```

Use the following URL for more details on keyTool and keystore conversion:
http://download.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html

Figure 9-1 shows the communication channels between a 5620 SAM server and other 5620 SAM components.

Figure 9-1 5620 SAM security



SSL requires a security certificate that is created and signed by a certification authority, or generated locally. A locally generated certificate is called an autosigned certificate and is for use only in the local network. A server sends the security certificate to a client or to another server, which accepts the certificate, if it is trusted.

To use SSL, the server must be configured with a keystore file that contains the certificate and a keystore pass file that contains a password. An SSL client must be configured with a truststore that contains the certificate.

In a redundant 5620 SAM deployment, the standby server acts as a client when it connects to the primary server. For this reason, the primary and standby servers in a redundant deployment must each be configured to use the certificate keystore file.

The following conditions apply to SSL configuration in a 5620 SAM system:

- When the 5620 SAM JMS channel is configured to use SSL, all OSS clients, single-user GUI clients and client delegate servers must be configured to use SSL.
- HTTPS configuration for OSS clients is a separate activity from HTTPS configuration for single-user GUI clients and client delegate servers.

9.2 Workflow to configure SSL

Caution — Configuring SSL on a 5620 SAM server requires a shutdown of the server software and causes a network-management outage. Ensure that you configure SSL only during a scheduled maintenance period.

1. Generate an SSL keystore file.
2. If the security certificate is autosigned, create a truststore on each 5620 SAM single-user GUI client, client delegate server, and OSS client station, and then import the certificate into each truststore.
3. Enable SSL on the 5620 SAM server for the following, as required:
   - JMS notifications sent to 5620 SAM GUI and OSS clients
   - EJB communication with the 5620 SAM GUI clients
   - HTTPS communication with the 5620 SAM OSS clients
4. If the 5620 SAM is deployed in a redundant configuration, configure SSL on the other 5620 SAM main server.
5. Create an SSL configuration on the 5620 SAM main server for automatic distribution to the single-user GUI client and client delegate server stations.
6. Restart each GUI client and client delegate server to implement the new SSL configuration.
7. Configure SSL on each OSS client.
8. See the *5620 SAM Troubleshooting Guide* for information about SSL error messages that are displayed during the SSL configuration.

9.3 SSL configuration procedures

The following procedures describe how to configure SSL on a 5620 SAM server.

Note 1 — *server_installation_location* in the following procedures refers to the installation directory specified during the 5620 SAM server installation.

The default location for a Solaris main server is /opt/5620sam/server.

The default location for an auxiliary server is /opt/5620sam/auxserver.

The default location for a Windows main server is C:\5620sam\server.

Note 2 — When part of a file path is valid for Windows and UNIX, the following procedures use a forward slash (/) to delimit the directory names in the path. If the 5620 SAM server is installed on Windows, you must use a backward slash (\) as the delimiter.

Procedure 9-1 To enable SSL on a 5620 SAM main server

Perform this procedure on the 5620 SAM server to enable SSL encryption on a 5620 SAM main server for communication with other 5620 SAM components.

Caution 1 — Configuring SSL on a 5620 SAM server requires a shutdown of the server software and causes a network-management outage. Ensure that you configure SSL only during a scheduled maintenance window.

Caution 2 — Alcatel-Lucent strongly recommends that only a person with SSL security knowledge attempts to perform the procedures in this chapter. Contact your Alcatel-Lucent technical support representative if you require assistance with configuring SSL.

Note — When a 5620 SAM server is configured to use SSL, all 5620 SAM clients and servers that connect to the server must also be configured to use SSL. See procedure 9-2 for information about configuring SSL for GUI and OSS clients. See chapter 5 for information about configuring HTTPS for GUI and OSS clients.

1 Log in to the 5620 SAM server station using an account with local administrator privileges.

Note — If the 5620 SAM server is installed on Solaris, you must log in as the samadmin user.

2 Perform one of the following to generate a keystore file.

a If you obtain a security certificate from a certification authority, follow the instructions on the Sun web site at http://java.sun.com to generate a keystore file.

b Use the Sun keytool utility to generate a keystore file that contains an autosigned security certificate. Perform the following steps.

Generating a keystore with an underlying private key of the RSA type may create duplicate certificate signatures. Alcatel-Lucent strongly recommends that certificates be obtained from a certification authority.

i Open a console window on the 5620 SAM server.

ii Navigate to the <*server_install_dir*>/jre/bin directory.

iii Enter the following command at the CLI prompt:

keytool -genkey -alias *alias* -dname "CN=*common_name*, OU=*org_unit*, O=*org_name*, L=*locality*, S=*state*, C=*country*" -keyalg RSA -keypass *password* -storepass *password* -keystore *destination_file* -validity *days* ↵

where
alias is a case-insensitive alias that is required for subsequent Keytool commands and where the following comprise the X.500 distinguished name:
common_name is the name of a person
org_unit is a department or division name
org_name is a company name
locality is a city name
state is a state or region name
country is a country code, for example, US
password is a password used to secure the key and keystore
destination_file is the path and name of the keystore file
days is the number of days before the SSL key expires. If this option is not set, the default key validity is three months.

The following is an example keystore generation command:

```
keytool -genkey -alias bob -dname "CN=Bob Smith,
OU=Accounting, O=ABC Inc., L=Pittsburgh, S=Pennsylvania,
C=US" -keyalg RSA -keypass BobsPassword -storepass
BobsPassword -keystore /tmp/samserver.keystore -validity
365
```

In this example, the utility generates the keystore and stores keystore in the /tmp/samserver.keystore file. The keypass and storepass passwords must be the same. The SSL key is valid for one year.

Note — The default keystore file name in the 5620 SAM server configuration files is samserver.keystore. If you want to use a different name for the keystore file, you must update the keystore file name in the appropriate server configuration files.

For more information about creating a keystore file using the Java keytool utility, see the Sun Java web site at http://java.sun.com.

iv Record the password that you specify when you generate the key because it is required in steps 5 to 7.

Note — If the security certificate is autosigned, you will need to export the certificate from the server and then import the certificate to the truststore on each Windows client station, Solaris single-user client, or Solaris client delegate server station. For more information, see Procedure 9-2.

3 If the 5620 SAM server is installed on a Solaris station, perform the following steps to stop the 5620 SAM server application.

Note — After this step, the 5620 SAM server is not managing the network until after the server restart later in the procedure.

i Open a console window on the 5620 SAM server, if a console window is not already open.

ii Navigate to the <*server_install_dir*>/nms/bin directory.

iii Enter the following at the CLI prompt:

./nmsserver.bash stop ↵

iv Verify that the 5620 SAM server is stopped. Enter the following at the CLI prompt:

./nmsserver.bash appserver_status ↵

v The 5620 SAM server application is stopped when the command in step 3 iv returns the following text string:

```
Application Server is stopped
```

If the command returns anything other than the above text string, wait five minutes and repeat step 3 iv. Do not proceed unless the console displays the above text.

4 If the 5620 SAM server is installed on a Windows station, perform the following steps to stop the 5620 SAM server application.

Note — After this step, the 5620 SAM server is not managing the network until after the server restart later in the procedure.

i Navigate to the <*server_install_dir*>\nms\bin directory.

ii Enter the following at the CLI prompt:

nmsserver.bat stop ↵

iii Enter the following at the CLI prompt to verify that the 5620 SAM server is stopped:

nmsserver.bat appserver_status ↵

iv The 5620 SAM server application is stopped when the command in step 4 iii returns the following text string:

```
Application Server is stopped
```

If the command returns anything other than the above text string, wait five minutes and repeat step 4 iii. Do not proceed unless the console displays the above text.

5 To enable SSL for the JMS notifications that are sent to 5620 SAM GUI clients, OSS clients, client delegate servers and auxiliary servers:

Caution — When you configure SSL for JMS notifications on a 5620 SAM server, all OSS and GUI clients, client delegate servers, and auxiliary servers are affected. See procedure 9-2 for information about configuring SSL security on other 5620 SAM components.

Note 1 — If you are configuring the 5620 SAM for Lawful Intercept (LI) operation, you must perform this step.

Note 2 — The SSL configuration on an auxiliary server applies to the JMS channel only. See chapter 5 for information about configuring secure communication on the JGroups channel between a 5620 SAM main server and a 5620 SAM auxiliary server.

i Copy the keystore file generated in step 2 to the <*server_install_dir*>/nms/jboss/server/default/conf/ directory.

Note — To simplify the SSL configuration, Alcatel-Lucent recommends copying the keystore file to the location named in this step, as it is the location specified by default in the remoting-bisocket-service.xml file. If you want to store the keystore file in a different location, you must edit remoting-bisocket-service.xml and replace the following text with the absolute file path and name of the keystore file:

- ${jboss.server.home.dir}/conf/samserver.keystore

Contact your Alcatel-Lucent technical-support representative for more information.

ii Navigate to the <*server_install_dir*>/nms/jboss/server/jms/deploy/jboss-messaging.sar directory.

iii Create a backup copy of the remoting-bisocket-service.xml file.

Caution — Do not store the backup copy of the file in the current directory, or the 5620 SAM server startup may be affected. Alcatel-Lucent recommends that you store the backup copy on a non-5620 SAM station.

iv Use a text editor to open the remoting-bisocket-service.xml file.

v Replace the word ‘password’ shown in Code 9-1 with the keystore password recorded in step 2.

vi Comment the first Bisocket Transport Connector section shown in Code 9-1 by surrounding it with <! -- and --> tags.

vii Uncomment the second Bisocket Transport Connector section shown in Code 9-1 by removing the <! -- and --> tags that surround it.

Code 9-1: Original remoting-bisocket-service.xml file

```
<!--  Please comment the following section to enable SSL -->
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.messaging:service=Connector,transport=bisocket" display-name="Bisocket
Transport Connector">
.
.
.
</mbean>
<!--  Please uncomment the following section and specify the keystore path and
password to enable SSL. All other connector parameters should be configured as above.
-->
<!--    <mbean code="org.jboss.remoting.transport.Connector"
          name="jboss.messaging:service=Connector,transport=bisocket"
          display-name="Bisocket Transport Connector">
.
.
.
<attribute name="KeyStoreURL">${jboss.server.home.dir}/conf/samserver.keystore</att
ribute>
      <attribute name="KeyStorePassword">password</attribute>
</mbean>  -->
```

viii Ensure that the modified sections of the file appear as shown in Code 9-2.

Code 9-2: Modified remoting-bisocket-service.xml file

```
<!--  Please comment the following section to enable SSL -->
<!--    <mbean code="org.jboss.remoting.transport.Connector"
 name="jboss.messaging:service=Connector,transport=bisocket"
 display-name="Bisocket Transport Connector">
.
.
.
</mbean> -->
 <!--  Please uncomment the following section and specify the keystore path and
password to enable SSL. All other connector parameters should be configured as above.
-->
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.messaging:service=Connector,transport=bisocket"
display-name="Bisocket Transport Connector">
.
.
.

<attribute name="KeyStoreURL">${jboss.server.home.dir}/conf/samserver.keystore</att
ribute>
      <attribute name="KeyStorePassword">your_keystore_password</attribute>
</mbean>
```

ix Save the changes to the file.

x Close the file.

xi Navigate to the <*server_install_dir*>/nms/bin directory.

xii Create a backup copy of the script that sets the 5620 SAM environment variables. The script file is named setenv.rc on a Solaris station, and setenv.bat on a Windows station.

xiii Use a text editor to open the setenv.rc or setenv.bat file.

xiv If the 5620 SAM server is installed on a Solaris station, uncomment the line shown in Code 9-3 by removing the "#" symbol and space from the beginning of the line.

Code 9-3: setenv.rc file

```
#JVM_OPTIONS_SSL="-Djavax.net.ssl.trustStore=<absolute path of the
KeyStore file>"
```

xv Modify the path shown in Code 9-3 so that it specifies an absolute path to the cacerts.trustStore file, as shown in Code 9-4.

Code 9-4: setenv.rc file with absolute path to cacerts.trustStore

```
JVM_OPTIONS_SSL="-Djavax.net.ssl.trustStore=
<server_install_dir>/nms/config/ssl/trustStore/cacerts.trustStore"
```

xvi If the 5620 SAM server is installed on a Windows station, uncomment the line shown in Code 9-5 by removing "rem " from the beginning of the line.

Code 9-5: setenv.bat file

```
rem     set JVM_OPTIONS_SSL=-Djavax.net.ssl.trustStore=
<absolute path of the KeyStore file>
```

xvii Modify the path shown in Code 9-5 so that it specifies an absolute path to the cacerts.trustStore file, as shown in Code 9-6.

Code 9-6: setenv.bat file with absolute path to cacerts.trustStore

```
set JVM_OPTIONS_SSL="-Djavax.net.ssl.trustStore=
<server_install_dir>\nms\config\ssl\trustStore\cacerts.trustStore"
```

xviii Save the changes and close the file.

xix Navigate to the <*server_install_dir*>/nms/config/clientDeploy/ directory.

xx Create a backup copy of the script that sets the 5620 SAM environment variables. The script file is named setenv.rc on a Solaris station, and setenv.bat on a Windows station.

xxi Use a text editor to open the setenv.rc or setenv.bat file.

xxii If the 5620 SAM server is installed on a Solaris station, uncomment the line shown in Code 9-7 by removing the "#" symbol and space from the beginning of the line.

Code 9-7: setenv.rc file

```
#JVM_OPTIONS_SSL="-Djavax.net.ssl.trustStore=<absolute path of the
KeyStore file>"
```

xxiii Modify the path shown in Code 9-7 so that it specifies an absolute path to the cacerts.trustStore file, as shown in Code 9-8.

Code 9-8: setenv.rc file with absolute path to cacerts.trustStore

```
JVM_OPTIONS_SSL="-Djavax.net.ssl.trustStore=
<server_install_dir>/nms/config/ssl/trustStore/cacerts.trustStore"
```

xxiv If the 5620 SAM server is installed on a Windows station, uncomment the line shown in Code 9-9 by removing "rem " from the beginning of the line.

Code 9-9: setenv.bat file

```
rem     set JVM_OPTIONS_SSL=-Djavax.net.ssl.trustStore=
<absolute path of the KeyStore file>
```

xxv Modify the path shown in Code 9-9 so that it specifies an absolute path to the cacerts.trustStore file, as shown in Code 9-10.

Code 9-10: setenv.bat file with absolute path to cacerts.trustStore

```
set JVM_OPTIONS_SSL="-Djavax.net.ssl.trustStore=
<server_install_dir>\nms\config\ssl\trustStore\cacerts.trustStore"
```

xxvi Save the changes and close the file.

xxvii If your 5620 SAM system includes auxiliary servers, perform steps 5 xi to 5 xviii on each auxiliary server.

You must FTP the keystore file generated in step 2 to each auxiliary server. The file location on the auxiliary server is <*aux_server_install_dir*>/nms/config/ssl/truststore/. For more information about the truststore, see Procedure 9-2.

6 To enable SSL for all 5620 SAM GUI client sessions:

Note 1 — This step configures single-user GUI client and client delegate server communication only; OSS client communication is not affected.

Note 2 — If you are configuring the 5620 SAM for LI operation, you must perform this step.

i Navigate to the <*server_install_dir*>/nms/jboss/server/default/conf/ directory.

ii Copy the keystore file generated in step 2 to the current directory, <*server_install_dir*>/nms/jboss/server/default/conf/.

iii Navigate to the <*server_install_dir*>/nms/jboss/server/jms/conf/ directory.

iv Copy the keystore file generated in step 2 to the current directory, <*server_install_dir*>/nms/jboss/server/jms/conf/.

Note — To simplify the SSL configuration, Alcatel-Lucent recommends copying the keystore file to the location named in this step, as it is the location specified by default in the jboss-service.xml file. If you want to store the keystore file in a different location, you must edit jboss-service.xml and replace the following text with the absolute file path and name of the keystore file:

- ${jboss.server.home.dir}/conf/samserver.keystore

Contact your Alcatel-Lucent technical-support representative for more information.

v If you are running a redundant system, FTP the keystore file generated in step 2 to the standby server. The file location on the standby server is <*server_install_dir*>/nms/jboss/server/jms/conf/samserver.keystore.

vi Navigate to the <*server_install_dir*>/nms/jboss/server/default/conf/ directory.

vii Create a backup copy of the jboss-service.xml file.

Caution — Do not store the backup copy of the file in the current directory, or the 5620 SAM server startup may be adversely affected. Alcatel-Lucent recommends that you store the backup copy on a non-5620 SAM station.

viii Use a text editor to open the jboss-service.xml file.

ix Comment the first Socket Transport Connector section shown in Code 9-11 by surrounding it with <! -- and --> tags.

x Uncomment the second Socket Transport Connector section shown in Code 9-11 by removing the <! -- and --> tags that surround it.

xi Replace the word ‘password’ shown in Code 9-11 with the keystore password recorded in step 2.

Code 9-11: Original jboss-service.xml file

```
<!--  Please comment the following section to enable SSL -->
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:service=Connector,transport=socket"
display-name="Socket transport Connector">
.
.
.
</mbean>
<!--  Please uncomment the following section and specify the keystore path
and password to enable SSL. All other connector parameters should be configured
as above. -->
<!--    <mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:service=Connector,transport=socket"
```

```
display-name="Socket transport Connector">
.
.
.
<attribute name="KeyStoreURL">${jboss.server.home.dir}/conf/samserver.keystore</att
ribute>
<attribute name="KeyStorePassword">password</attribute>
</mbean> -->
```

xii Ensure that the modified sections of the file appear as displayed in Code 9-12.

Code 9-12: Modified jboss-service.xml file

```
<!--  Please comment the following section to enable SSL -->
<!--    <mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:service=Connector,transport=socket"
display-name="Socket transport Connector">
.
.
.
</mbean> -->
<!--  Please uncomment the following section and specify the keystore path
and password to enable SSL. All other connector parameters should be configured
as above. -->
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:service=Connector,transport=socket"
display-name="Socket transport Connector">
.
.
.
<mbean code="org.jboss.remoting.security.SSLSocketBuilder"
name="jboss.remoting:service=SocketBuilder,type=SSL"
display-nameless Server Socket Factory Builder">
<attribute name="KeyStoreURL">${jboss.server.home.dir}/conf/samserver.keystore</att
ribute>
<attribute name="KeyStorePassword">your_keystore_password</attribute>
</mbean>
```

xiii Save the changes to the file.

xiv Close the file.

7 To enable SSL for HTTPS communication with all OSS clients:

Note 1 — This step enables HTTPS for OSS client communication only; single-user client and client delegate server communication is not affected. See chapter 5 for information about configuring HTTPS for 5620 SAM single-user GUI clients and client delegate servers.

Note 2 — If you are configuring the 5620 SAM for LI operation, you must perform this step.

i Copy the keystore file that is generated in step 2 to the <*server_install_dir*>/nms/jboss/server/default/conf/directory.

Note — To simplify the SSL configuration, Alcatel-Lucent recommends copying the keystore file to the location named in this step, as it is the location specified by default in the server.xml file. If you want to store the keystore file in a different location, you must edit server.xml and replace the following text with the absolute file path and name of the keystore file:

- ${jboss.server.home.dir}/conf/samserver.keystore

Contact your Alcatel-Lucent technical-support representative for more information.

ii Navigate to the <*server_install_dir*>/nms/jboss/server/default/deploy/jboss-web.deployer directory.

iii Create a backup copy of the server.xml file.

Caution — Do not store the backup copy of the file in the current directory, or the 5620 SAM server startup may be affected. Alcatel-Lucent recommends that you store the backup copy on a non-5620 SAM station.

iv Use a text editor to open the server.xml file.

v Uncomment the second section shown in Code 9-13 by moving the --> tag at the end of the section to the end of the first line in the section, as shown in Code 9-14.

Code 9-13: Original server.xml file

```
<Connector port="8080" address="${jboss.bind.address}"
maxThreads="10" maxHttpHeaderSize="8192"
emptySessionPath="true" protocol="HTTP/1.1"
enableLookups="false" redirectPort="8443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true" />

    <!-- SSL/TLS Connector configuration
<Connector port="8443" address="${jboss.bind.address}"
maxThreads="10" acceptCount="100" scheme="https" secure="true"
protocol="HTTP/1.1" SSLEnabled="true" clientAuth="false"
```

```
keystoreFile="${jboss.server.home.dir}/conf/samserver.keystore"
keystorePass="password" sslProtocol="TLS"/>
-->
```

vi Change *your_keystore_password* shown in Code 9-14 to the keystore password recorded in step 2.

Code 9-14: Modified server.xml file

```
<!--  <Connector port="8080" address="${jboss.bind.address}"
         maxThreads="10" maxHttpHeaderSize="8192"
         emptySessionPath="true" protocol="HTTP/1.1"
         enableLookups="false" redirectPort="8443" acceptCount="100"
         connectionTimeout="20000" disableUploadTimeout="true" /> -->

    <!-- SSL/TLS Connector configuration -->
    <Connector port="8443" address="${jboss.bind.address}"
         maxThreads="10" acceptCount="100" scheme="https" secure="true"
         protocol="HTTP/1.1" SSLEnabled="true" clientAuth="false"
         keystoreFile="${jboss.server.home.dir}/conf/samserver.keystore"
         keystorePass="your_keystore_password" sslProtocol="TLS"/>
```

vii For additional security, Alcatel-Lucent recommends disabling HTTP if HTTPS is used. To disable HTTP, comment the first section shown in Code 9-13 by surrounding the < and /> tags with <! -- and --> tags as shown in Code 9-14.

viii Save the file.

ix Close the file.

8 Start the 5620 SAM server software.

Note — You must enable SSL on the 5620 SAM single-user GUI clients and client delegate servers before they can communicate with the main server using SSL. See procedure 9-2 for information about using the auto-client update functionality to deploy the SSL configuration to 5620 SAM single-user GUI clients and client delegate servers.

Procedure 9-2 To enable SSL for 5620 SAM GUI clients

Perform this procedure to enable SSL on all GUI clients that connect to a 5620 SAM main server. This procedure uses the auto-client update function to deploy an updated security configuration to each single-user GUI client station and each client delegate server station.

Note 1 — When you perform this step on a client delegate server, you affect each GUI client that connects through the client delegate server.

Note 2 — When you are modifying the cacerts.trustStore file, be aware that SSO/SANE certificates are stored in the same file. When enabling SSL, you cannot overwrite the existing trustStore file with a new file, or change the path in the setenv.rc file.

1 Enable SSL on the main server to which the clients connect. See procedure 9-1 for information about enabling SSL on a 5620 SAM main server for GUI clients.

2 Navigate to the *install_dir*/nms/config/clientDeploy directory on the main server, where *install_dir* is the server installation location, typically /opt/5620sam/server.

3 If 5620 SAM single-user GUI clients on Solaris connect to the main server, or if a client delegate server is used, perform the following steps to export security certificates from the 5620 SAM main server, and import the certificates to the clients.

i Export certificates from the 5620 SAM server.

```
<JAVA_HOME>/bin/keytool -export -alias <aliasName> -file
<outputCerficateFileName> -keystore  <server.keystore
filename > -storepass <password>
```

ii (Optional) Change the default password for the server trust store (the default password is "changeit").

```
<JAVA_HOME>/bin/keytool -storepasswd -keystore
trustStore/cacerts.trustStore
```

iii Import server certficates into the 5620 SAM cacerts.trustStore on the client system.

```
<JAVA_HOME>/bin/keytool -import -v -trustcacerts -alias
<aliasName> -file <certificateFileNameToImport> -keystore
cacerts.trustStore -storepass <password>
```

4 If 5620 SAM GUI clients on Windows connect to the main server, perform the following steps to export security certificates from the 5620 SAM main server, and import the certificates to the clients.

i Export certificates from the 5620 SAM server.

```
<JAVA_HOME>\bin\keytool -export -alias <aliasName> -file
<outputCerficateFileName> -keystore  <server.keystore
filename > -storepass <password>
```

ii (Optional) Change the default password for the server trust store (the default password is "changeit").

<*JAVA_HOME*>\bin\keytool -storepasswd -keystore trustStore\cacerts.trustStore

iii Import server certificates into the 5620 SAM cacerts.trustStore on the client system.

<*JAVA_HOME*>\bin\keytool -import -v -trustcacerts -alias <*aliasName*> -file <*certificateFileNameToImport*> -keystore cacerts.trustStore -storepass <*password*>

iv Navigate to the <*client_install_dir*>\nms\bin\ directory.

v Create a backup copy of the setenv.bat file.

vi Use a text editor to open the setenv.bat file.

vii Uncomment the line shown in Code 9-15 by removing "rem " from the beginning of the line.

Code 9-15: setenv.bat file

```
rem     set JVM_OPTIONS_SSL=-Djavax.net.ssl.trustStore=
<absolute path of the KeyStore file>
```

viii Modify the path shown in Code 9-15 so that it specifies an absolute path to the cacerts.trustStore file, as shown in Code 9-16.

Code 9-16: setenv.bat file with absolute path to cacerts.trustStore

```
set JVM_OPTIONS_SSL="-Djavax.net.ssl.trustStore=
<drive_letter>:<server_install_dir>\nms\bin\cacerts.trustStore"
```

ix Save the changes and close the file.

5 Open a console window on the main server.

6 Run the script that prepares the SSL configuration update for automatic distribution to clients.

a If the main server is installed on Solaris, enter the following at the prompt:

<*install_dir*>/nms/bin/nmsdeploytool.bash deploy ↵

where *install_dir* is the server installation location, typically /opt/5620sam/server

b If the main server is installed on Windows, enter the following at the prompt:

<*install_dir*>\nms\bin\nmsdeploytool.bat deploy ↵

where *install_dir* is the server installation location, typically C:\5620sam\server

The updated configuration is ready for downloading by the GUI clients.

7 Close the console window.

8 You must start the 5620 SAM client software to download the SSL configuration. However, when SSL is enabled on a 5620 SAM main server, the main server uses HTTPS for client downloads. Because SSL is not configured on the client station, you must perform the following steps once on each single-user client or client delegate server station to download and apply the SSL configuration.

i Log in to the single-user client or client delegate server station.

Note — On a client delegate server station, you must log in as the root user.

ii Open a console window.

iii If the client software is installed on Solaris, enter the following at the prompt to start the client software and to specify the use of HTTPS for the client file download:

***install_dir*/nms/bin/nmsclient.bash secure server *server*:8444** ↵

where
install_dir is the client installation location, typically /opt/5620sam/client
server is the IP address or the DNS name of the main server that has SSL enabled

iv If the client software is installed on Windows, enter the following at the prompt to start the client software and to specify the use of HTTPS for the client file download:

***install_dir*\nms\bin\nmsclient.bat secure server *server*:8444** ↵

where
install_dir is the client installation location, typically C:\5620sam\client
server is the IP address or the DNS name of the main server that has SSL enabled

Note — The "secure" startup option is required only the first time you connect to a main server that has SSL enabled.

The client software downloads the SSL configuration, and subsequent client sessions use SSL and HTTPS by default.

Procedure 9-3 To configure SSL for web-based client installation

Perform this procdure if you are running the web-based client installer against a 5620 SAM main server that is configured for SSL encrypted communication.

1 Navigate to the *install_dir*/nms/jboss/server/jms/deploy/samcommandservlet.war/WEB-INF/ directory on the main server, where *install_dir* is the server installation location, typically /opt/5620sam/server.

2 Use a text editor to open the web.xml file.

3 Modify the following properties:

i Modify the Secure property (shown in Code 9-17) so that the parameter value is set to HTTPS (as shown in Code 9-18).

Code 9-17: web.xml file, Secure property (default)

```
<context-param>
<param-name>property:secure</param-name>
<param-value>http</param-value>
<description>property identifying if its http/https for
jnlp</description>
</context-param>
```

Code 9-18: web.xml file, Secure property (modified for HTTPS)

```
<context-param>
<param-name>property:secure</param-name>
<param-value>https</param-value>
<description>property identifying if its http/https for
jnlp</description>
</context-param>
```

ii Modify the Port property (shown in Code 9-19) so that the parameter value is set to 8444 (as shown in Code 9-20).

Code 9-19: web.xml file, Port property (default)

```
<context-param>
<param-name>property:port</param-name>
<param-value>8085</param-value>
<description>property identifying port to use for jnlp</description>
</context-param>
```

Code 9-20: web.xml file, Port property (modified for port 8444)

```
<context-param>
<param-name>property:port</param-name>
<param-value>8444</param-value>
<description>property identifying port to use for jnlp</description>
</context-param>
```

4 Save and close the web.xml file.

Procedure 9-4 To configure SSL on a 3GPP OSS interface

Perform this procedure to enable SSL communication on the 3GPP OSS interface of a 5620 SAM main server.

Note — In a redundant 5620 SAM deployment, you must perform this procedure on each 5620 SAM main server in the deployment.

1 Ensure that SSL communication is enabled on the 5620 SAM main server OSS interfaces, as described in the "*5620 SAM SSL security*" chapter of the *5620 SAM User Guide*.

2 Log in to the 5620 SAM main server as the samadmin user.

3 Open the *path*/nms/cnbi/home/config/cnbi.properties file using a plain-text editor

where *path* is the 5620 SAM main server installation location, typically opt/5620sam/server

4 Locate the following line:

```
CNBI.SAMO.ServerCertFile=
```

5 Edit the line to read:

```
CNBI.SAMO.ServerCertFile=SSL_certificate_filespec
```

where *SSL_certificate_filespec* is the absolute path to the SSL keystore file on the main server

6 Locate the following line:

```
CNBI.SAM0.URL=
```

7 Change "http:" in the line to "https:".

8 Save the file.

9 Close the file.

10 Open a console window on the main server station.

11 Navigate to the following directory:

path/nms/bin

where *path* is the 5620 SAM main server installation directory, typically /opt/5620sam/server

12 Enter the following at the prompt:

```
bash$ ./nmsserver.bash cnbiread_config ↵
```

The main server loads the updated configuration, and SSL is enabled on the 3GPP OSS interface.

13 Close the console window.

14 Log out of the 5620 SAM main server.

10 — 5620 SAM integration with other Alcatel-Lucent systems

10.1 5620 SAM integration overview

You can configure the 5620 SAM to operate interactively with other Alcatel-Lucent systems. Depending on the nature of the integration, you can use an interface on one system to perform functions on, or retrieve information from, the other system.

For information about 5620 SAM interworking with non-Alcatel-Lucent systems, see the *5620 SAM Integration Guide*.

10.2 5620 SAM and 5650 CPAM integration

When the 5650 CPAM software is enabled on a 5620 SAM system, the 5650 CPAM functions are available from the 5620 SAM main menu. The 5650 CPAM provides real-time control IGP topology capture, inspection, visualization, and troubleshooting. The integration with the 5620 SAM allows the 5650 CPAM to cohesively associate routing information to infrastructure such as network routes, service tunnels, LSPs, edge-to-edge service traffic paths, and OAM tests.

5650 CPAM and 5620 SAM integration supports the following operational activities:

- **network planning**
  Planning activities are optimized with real-time topology and strong linkages between services and infrastructure layers in the 5620 SAM GUI and 5620 SAM-O OSS interfaces.
- **network operations**
  Real-time topology and multi-layer highlighting allows you to rapidly assess the state of services, tunnels, and routing on the IGP and IP/MPLS maps.
- **network troubleshooting**
  Historical OAM trace, SPF and RSVP path, and checkpoints allow you to rapidly detect and resolve service level issues whose root cause is in the IP or MPLS layers.
- **network restoration**
  Checkpoints and real-time views of IP/MPLS and service and tunnel infrastructure allow you to restore and plan networks.
- **proactive assurance**
  5650 CPAM alarms, network route and tunnel inspection lists, validation functions, checkpoints, and multi-layer views allow you to detect routing faults.

The 5650 CPAM provides a tight eastbound and westbound integration with the 5620 SAM. This integration allows for a real-time view of the network including routing topology and associated configurations whether performed on the GUI, OSS interface, or by CLI. The 5650 CPAM can leverage 5620 SAM redundancy and offer tight navigation between protocol maps and 5620 SAM-managed objects, such as protocol links. In addition, the 5620 SAM GUI supports the management of the 7701 CPAA platform.

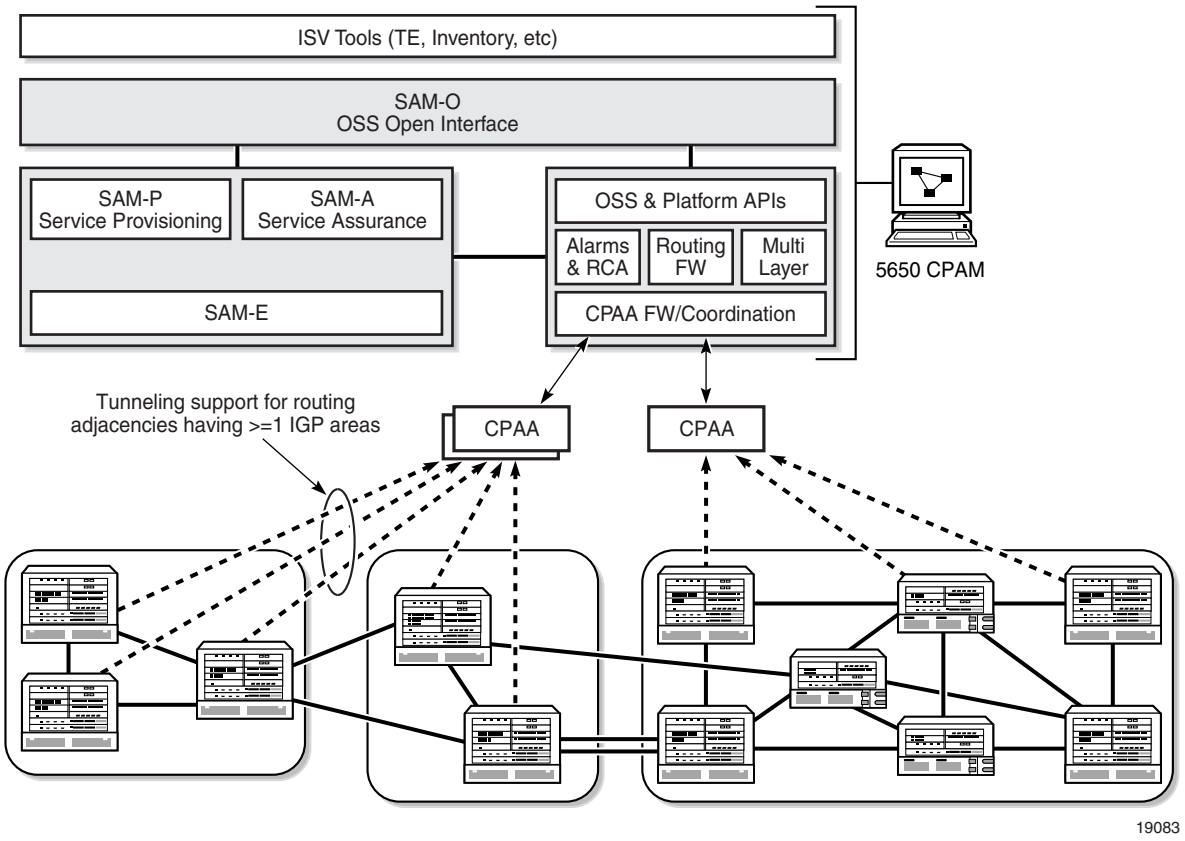
The 5620 SAM-O OSS interface module includes 5650 CPAM packages and methods that provide a smooth integration path for the export of real-time protocol or IP-level topology to advanced OSS applications, such as TE tools.

When the 5650 CPAM and the 5620 SAM share the same database, the 5650 CPAM can access objects managed by 5620 SAM and display them on the 5650 CPAM topology views. Without integration with the 5620 SAM, the following functions are not available:

- service, LSP, multicast, and OAM highlights
- historical LSP active paths
- LDP and RSVP interface display on the MPLS view

Figure 10-1 shows the 5650 CPAM architecture. See the 5650 CPAM documentation suite for information about how to configure application interoperation.

Figure 10-1 5650 CPAM and 5620 SAM integration



There are two main components to the control plane assurance management solution:

- a server component, the 5650 CPAM route controller
- a route analyzer component, the 7701 CPAA

The 5650 CPAM server component contains 7701 CPAA control frameworks, applications, and coordination functions for the distributed 7701 CPAAs and provides the applications that are required to leverage the data provided by the 7701 CPAA platform.

The 5650 CPAM route controller, or server, communicates with several GUI and OSSI clients using the same API as the 5620 SAM. When the 5650 CPAM route controller is integrated with a 5620 SAM, the 5620 SAM and 5650 CPAM versions must be compatible. In addition, the 5650 CPAM route controller can run independently with one or multiple 5620 SAM servers.

The 7701 CPAA is a mountable rack that provides an analysis and distributed computing platform. This platform uses a passive version of the industry-tested and -proven 7750 SR routing code base to guarantee a high degree of interoperability with customer networks. The 7701 CPAA acts as a special-purpose routing element whose role is to passively peer with the network.

The 7701 CPAA is supported by the 5620 SAM as a special-purpose NE.

5650 CPAM deployment

The 5650 CPAM is supported on Solaris platforms only. For system configuration requirements, contact the appropriate Alcatel-Lucent NSM representatives or see the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information. System configurations depend on the size of the managed network.

The 5650 CPAM requires a license key to operate. The license key specifies the number of appliances, routers, and GUI clients that the system can support, and the expiry date of the license key.

The 5650 CPAM can be installed by entering the 5650 CPAM license key during the 5620 SAM installation.

If the 5620 SAM is already installed and running, you must enable the 5650 CPAM by adding the appropriate 5650 CPAM license key to the nms-server.xml file. You do not have to re-start the server. You must run the nmsserver.bat or .bash file with the read_config option to activate the 5650 CPAM. If the 5650 CPAM is installed and running without the 5620 SAM, you can enable the 5620 SAM by adding the appropriate 5620 SAM license key to the nms-server.xml file.

The 5650 CPAM works with the 5620 SAM to manage the same network using the same database instance. The 5650 CPAM network may include devices that are not managed by the 5620 SAM.

For example, network A is managed by the 5620 SAM, Release 7.0 and network B is managed by the 5620 SAM, Release 8.0. The 5650 CPAM is connected to both networks. In the integration scenario, the Release 8.0 5620 SAM system and the 5650 CPAM system manage the same network using the same database instance. The network managed by the 5650 CPAM is normally larger than the network managed by the 5620 SAM because it may include several devices that the 5620 SAM does not support.

Database upgrade

The 5620 SAM and the 5650 CPAM share the same database in an integrated deployment.

5650 CPAM uninstallation

You can uninstall the 5650 CPAM from a 5620 SAM/5650 CPAM integration by removing the 5650 CPAM license key from the nms-server.xml file. You must run the nmsserver.bat or .bash file with the read_config option to deactivate the 5650 CPAM.

5650 CPAM menus

Table 10-1 describes the 5650 CPAM menus.

Table 10-1 5650 CPAM menus

Menu item	Description	Dependencies
Tools→Route Analysis	Access all 5650 CPAM management menus	Disabled if the 5650 CPAM license key is not enabled
Application→Flat Maps	View the following flat topology maps: • IGP Topology • OSPF Topology • ISIS Topology • MPLS Topology • Multicast Topology	Does not appear if the 5650 CPAM license key is not enabled

10.3 5620 SAM and 5620 NM integration

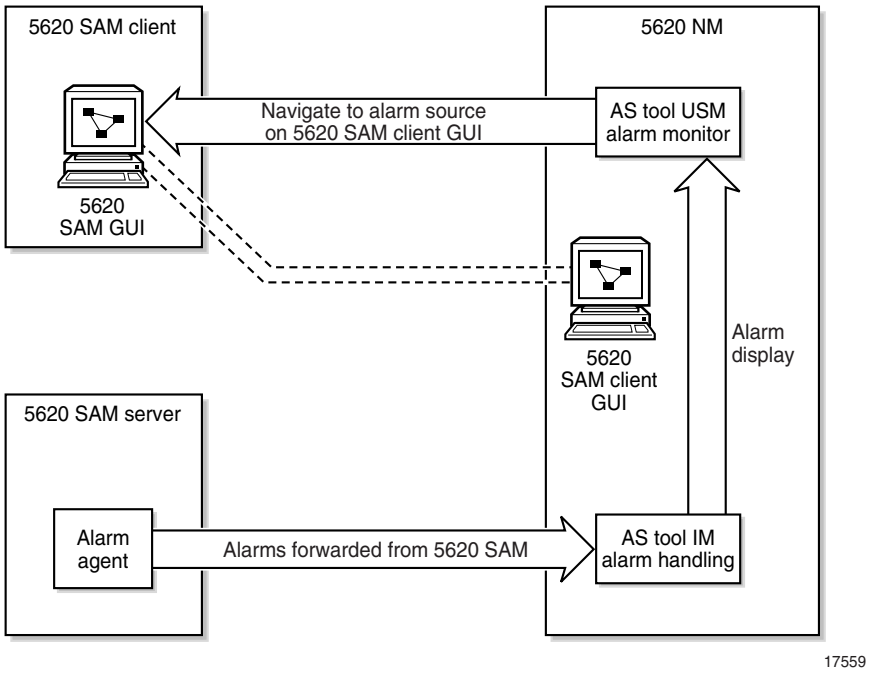
You can integrate the 5620 SAM and 5620 NM, which enables an operator to do the following.

- Navigate the 5620 SAM GUI using a 5620 NM client.
- Forward alarms from the 5620 SAM to the 5620 NM AS tool IM.
- Display 5620 SAM alarms graphically on the 5620 NM AS tool USM.
- Monitor services end-to-end using supported NM integration functions.

Note — Before you can integrate the 5620 SAM and 5620 NM, you must enable navigation from external systems during a 5620 SAM main server installation or upgrade, or enable it after an installation or upgrade using the 5620 SAM server configuration utility. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about enabling navigation from external systems.

Figure 10-2 shows how navigation to the 5620 NM and 5620 NM AS tool for alarm management occurs.

Figure 10-2 Alarm navigation



Before you start

Consider the following before you attempt to integrate the 5620 SAM and 5620 NM:

- The *5620 NM Release Notice* lists the 5620 SAM releases that are compatible with various 5620 NM releases.
- The 5620 NM and 5620 SAM integration software is on the 5620 SAM software DVD-ROM.
- For 5620 SAM GUI navigation using a 5620 NM client, the 5620 SAM client must be installed on the same station that runs the 5620 NM client X-window access application.
- For alarm forwarding, the 5620 SAM and 5620 NM client software can be installed on the same or different stations.
- The platform for the 5620 NM software must meet the minimum requirements in the *5620 Network Manager Installation and Upgrade Guide*.
- You must configure the 5620 SAM to interwork with the 5620 NM software; for example, configure the 5620 SAM server to forward alarms and configure the 5620 SAM client to allow navigation from external systems.

5620 SAM client GUI startup and navigation restrictions

The following restrictions apply to 5620 SAM client GUI navigation using a 5620 NM client.

- When the client GUI is starting, 5620 NM navigation requests are blocked.
- A 5620 SAM client accepts navigation requests after the client GUI user logs in.

- Each navigation request is submitted only after a login timeout expires. This timeout helps to decrease the number of requests that are sent when a user submits and then immediately cancels a request.
- A 5620 SAM client delegate server acts as a single 5620 SAM client instance; you cannot configure a client delegate server to integrate with more than one 5620 NM client.
- The following navigation rules apply when multiple client GUIs are running.
  - A navigation request is cancelled when the client GUI is shut down.
  - All navigation requests are handled by the first registered client GUI.
  - If no client GUI is registered, a 5620 SAM server starts a new client GUI when it receives a navigation request.
  - If the currently registered 5620 SAM client GUI shuts down, another registered client GUI handles the navigation requests.

10.4 Workflow for 5620 SAM and 5620 NM integration

1 Ensure that the appropriate 5620 SAM integration software is installed and appropriately configured on the 5620 NM. See Procedure 10-1 for more information.

2 Configure the 5620 SAM client and server to support GUI navigation. See Procedure 10-1 for more information.

3 Start the 5620 SAM GUI.

4 Start the 5620 NM client GUI. See Procedure 10-2 for more information.

5 Perform the required network management function using the appropriate GUI, as described in section 10.3.

10.5 5620 SAM and 5620 NM integration procedures

The following procedures describe how to configure 5620 SAM and 5620 NM integration.

Procedure 10-1 To configure 5620 SAM and 5620 NM GUI integration

Perform this procedure to enable the use of a 5620 SAM client GUI through a 5620 NM client GUI.

1 Include the required 5620 SAM integration package in the 5620 NM installation. Consult the 5620 NM documentation for integration software installation and configuration information.

2 If required, configure the 5620 SAM server to forward alarms to the 5620 NM, as described in section 10.3.

3 Perform the following steps when the “Navigation from External Systems” panel is displayed during the 5620 SAM server installation.

i Select the “Enable Navigation from External Systems” parameter.

ii Specify a value for the “TCP port for accepting GUI navigation requests” parameter.

4 Install a 5620 SAM client on a station that displays the 5620 NM client GUI. This is typically a station that runs an X-Window terminal emulator, but it can also be the 5620 NM database networkstation or the 5620 NM operator server networkstation, if a client GUI is locally displayed.

5 Perform the following steps on the station where the 5620 SAM client is installed to ensure that anti-aliasing is disabled.

i Open the *path*/nms/config/nms-client.xml file with a plain-text editor, for example, vi

where *path* is the 5620 SAM client installation location, typically /opt/5620sam/client

ii Search for the following XML tag that marks the beginning of the topologyMaps section:

```
<topologyMaps
```

iii Edit the antiAliasActive entry in the topologyMaps section to read “false” as shown below.

```
<topologyMaps
     iconReductionThreshold="40"
     labelHideThreshold="35"
        snapToGridInterval="25"
        antiAliasActive="false"
     />
```

6 Open a console window on the on the station where the 5620 SAM client is installed.

7 Start the navigator proxy script by entering the following at the CLI prompt:

```
# cd /opt/5620samclient/bin
# .install_navigation_daemon.bash
```

8 Start the 5620 SAM client by entering the following at the CLI prompt:

```
# ./nmsclient.bash
```

9 Use the 5620 SAM client GUI to create a 5620 NM user account that has a non-administrative privilege level with the appropriate scope of command role applied. See chapter 8 for more information about configuring user accounts and how to apply a scope of command role.

10 Copy the sam-jaxb.jar file from the nms_common_core.jar file from the /opt/5620sam/server/nms/lib/common/generated directory on the 5620 SAM installation DVD-ROM to the opt/netmgt/jnm/lib directory on the 5620 NM database networkstation.

11 Copy the following files from the /integration/5620NM/client/samadaptor directory on the 5620 SAM installation DVD-ROM to the /opt/netmgt/samadaptor/lib directory on the 5620 NM database networkstation:

- jbasiccomp.jar
- jnavapi.jar
- navrmi.jar
- samAdaptor.jar

12 Open the X-Window terminal emulator on the station that has the newly installed 5620 SAM client.

13 Log in to the 5620 NM operator server networkstation as a user with administrative privileges.

14 Open a console window on the 5620 NM operator server networkstation.

15 Start the 5620 NM client. The 5620 NM client GUI is displayed on the local station, and the 5620 SAM client GUI is available as a 5620 NM main menu item.

16 Use the 5620 SAM client account created in step 9 to perform the required interworking functions, as described in described in section 10.3, and the *5620 Network Manager User Guide*.

Procedure 10-2 To start the 5620 NM GUI

1 Log in to the 5620 SAM single-user client or client delegate station

2 Start the X-terminal software.

3 Use the X-terminal software to start the 5620 NM GUI on the Solaris station that has the 5620 NM Operator Position installed.

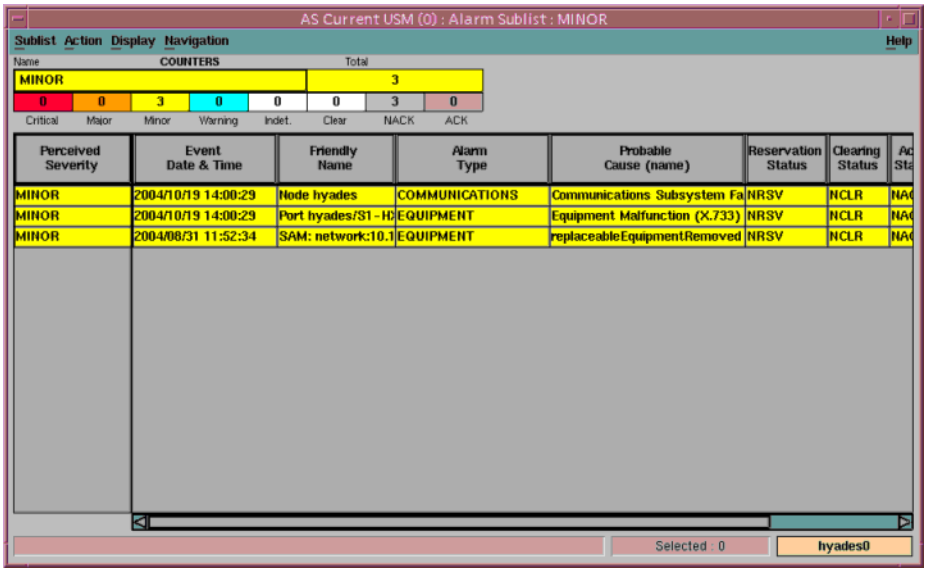
Procedure 10-3 To navigate from the 5620 NM AS tool USM to the 5620 SAM client GUI

See the *5620 SAM Troubleshooting Guide* for more information about troubleshooting using alarms.

1 Choose a counter summary window or alarm sublist from the AS tool USM.

2 Choose a sublist or an alarm in a sublist. 5620 SAM alarms are preceded by SAM in the Friendly Name field of the alarm sublist, as shown in Figure 10-3.

Figure 10-3 5620 SAM alarm in the AS tool USM



3 From the 5620 NM AS tool USM menu, choose Navigation→External Equipment→Show Equipment to navigate to the property form that lists the alarm on the 5620 SAM client GUI. The appropriate form is displayed. If the 5620 SAM client GUI is running, a new object properties form is displayed.

4 If the client GUI is not running, perform the following steps.

i Open the 5620 SAM client GUI.

ii View the object property form that is displayed on the 5620 NM client GUI.

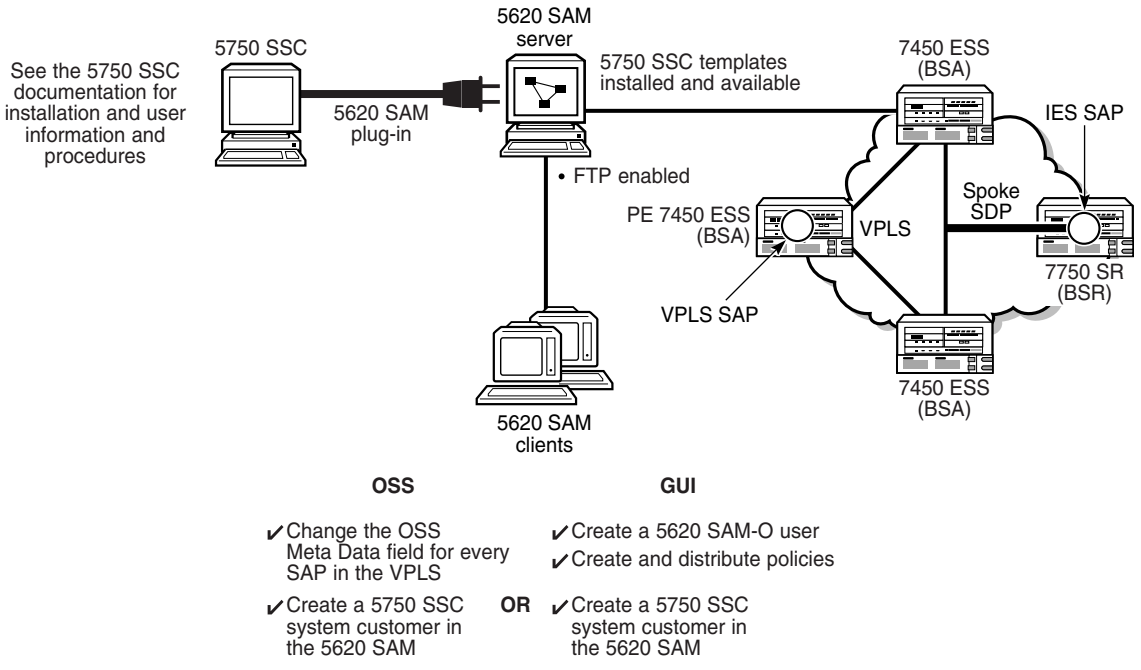
5 After the alarm issue is resolved, clear the alarm using the 5620 SAM client GUI. Alarm status changes are shown in the 5620 NM AS tool USM.

10.6 5620 SAM and 5750 SSC integration

The 5620 SAM can be configured to interoperate with the 5750 Subscriber Services Controller. The 5750 SSC provides centralized control of subscriber access services for triple play service delivery; for example, DHCP to identify subscribers and trigger service configuration.

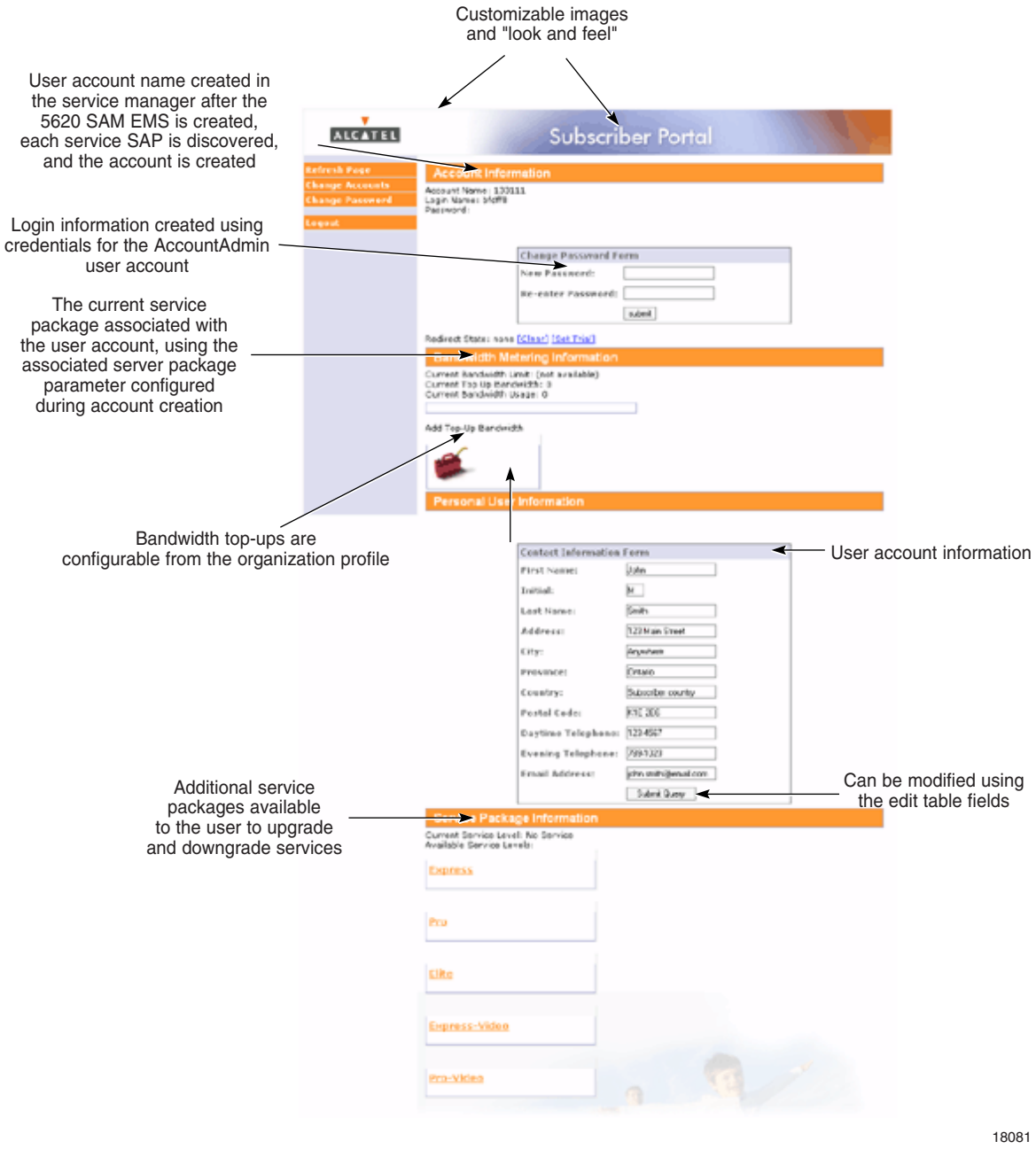
Figure 10-1 shows the integration requirements for the 5620 SAM and the 5750 SSC. See the 5750 SSC documentation suite for information about how to configure application interoperation.

Figure 10-4 5750 SSC and 5620 SAM integration



You use the 5750 SSC Service Manager to create and manage subscriber services, including user account information and QoS levels. The 5750 SSC user accounts represent the residential subscribers of triple play services. The information configured in the 5750 SSC Service Manager is used to build the subscriber web portal for user self-management. Figure 10-5 shows a subscriber web portal and how the component pieces are assembled from 5750 SSC subscriber management configurations.

Figure 10-5 Subscriber web portal



Device management

11 — Device support

11.1 Device support overview

The 5620 SAM supports the following devices:

- eNodeB
- 7750 MG
- 5780 DSC
- 9471 MME
- 1830 PSS 32/16, 1830 PSS 1 GBE MD4H, AHP
- 7750 SR
- 7750 SR-c4
- 7750 SR-c12
- 7710 SR
- 7705 SAR
- 7450 ESS
- 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA
- Telco
- OS 6250M
- OS 6250SME
- OS 6850
- OS 6855
- OS 6400
- OS 9600
- OS 9700
- OS 9700E
- OS 9800
- OS 9800E
- 7210 SAS-E
- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 9500 MPR
- generic NEs

The 5620 SAM supports up to three major releases of the devices. For example, the 5620 SAM can manage a 7750 SR, Release 7.0, 6.1, 6.0, or Release 5.0. Earlier releases of the devices are not supported.

Note — Releases 6.0 and 6.1 are part of the same major release.

The 5620 SAM supports the minor releases of a device when the major release is supported.

Note — There may be restrictions if a device does not follow the basic rules for MIB changes. When a device introduces maintenance releases, you may need to upgrade the 5620 SAM to a release that supports the changes on the device.

The following documents describe the compatibility and functionality for the devices managed by the 5620 SAM.

- See the *5620 SAM NE Compatibility Guide* for information about compatible and supported device releases.
- See the appropriate user documentation for information about device-specific CLI commands, parameters, and installation. Contact your Alcatel-Lucent technical support representative for information about specific network or facility considerations.

Note — The 5620 SAM functions and features vary for the supported devices. When a function or feature is not supported by the device, the feature or function cannot be selected from the GUI, or does not appear on the GUI. The documentation describes the major variations in support, including device-specific procedures for specific implementations.

The documentation does not describe the following minor GUI variations for each device:

- partial support for the parameter list on a form
- partial support for the buttons and tab buttons on a form

The *5620 SAM Parameter Guide* describes device-specific support for parameters and variations in default values, when applicable.

eNodeB support

The eNodeB is an enhanced BTS system for UE access to the LTE RAN network and LTE services in the 700 MHz spectrum. The eNodeB is available as a compact or distributed system that consists of a BBU, and TRDU (compact) or RRH (distributed) device components.

The *5620 SAM User Guide* and other non-LTE documents in the 5620 SAM documentation suite do not describe eNodeB management. Management and configuration of the eNodeB with the 5620 SAM is described in the following documents:

- *5620 SAM LTE RAN User Guide*—Describes eNodeB discovery, configuration, troubleshooting, maintenance, security, and administration including feature and capacity licensing with the 5620 SAM.
- *5620 SAM LTE Parameter Reference*—Describes eNodeB device MIM parameters as represented in the 5620 SAM schema, in addition to parameters on LTE and LTE service forms in the 5620 SAM GUI.
- *5620 SAM LTE Alarm Reference*—Describes 5620 SAM LTE domain alarms and eNodeB device alarms.

9471 MME support

The 5620 SAM allows you to view the properties for the equipment, instance, interface function, application function, and packet handler for the 9471 MME. The 9471 MME equipment is represented in the 5620 SAM equipment navigation tree. You can view the 9471 MME properties by choosing Manage→Mobile Core→MME Instances from the 5620 SAM GUI main menu.

The *5620 SAM User Guide* and other non-LTE documents in the 5620 SAM documentation suite do not describe 9471 MME management. Management and configuration of the 9471 MME with the 5620 SAM is described in the following documents:

- *5620 SAM LTE ePC User Guide*—Describes 9471 MME discovery, configuration, troubleshooting, maintenance, security, and administration including feature and capacity licensing with the 5620 SAM.
- *5620 SAM LTE Parameter Reference*—Describes 9471 MME device parameters as represented in the 5620 SAM schema, in addition to parameters on LTE and LTE service forms in the 5620 SAM GUI.
- *5620 SAM LTE Alarm Reference*—Describes 5620 SAM LTE domain alarms and 9471 MME device alarms.

7750 MG support

The 5620 SAM supports the discovery and management of the 7- or 12-slot 7750 MG. The 7750 MG can be configured as an SGW or a PGW in the LTE network.

The *5620 SAM User Guide* and other non-LTE documents in the 5620 SAM documentation suite do not describe 7750 MG management. Management and configuration of the 7750 MG with the 5620 SAM is described in the following documents:

- *5620 SAM LTE ePC User Guide*—Describes 7750 MG discovery, configuration, troubleshooting, maintenance, security, and administration including feature and capacity licensing with the 5620 SAM.
- *5620 SAM LTE Parameter Reference*—Describes 7750 MG device parameters as represented in the 5620 SAM schema, in addition to parameters on LTE and LTE service forms in the 5620 SAM GUI.
- *5620 SAM LTE Alarm Reference*—Describes 5620 SAM LTE domain alarms and 7750 MG device alarms.

5780 DSC support

The 5620 SAM allows you to view the properties for the equipment, instance, diameter proxy agent, and policy charging rules for the 5780 DSC. The 5780 DSC equipment properties are represented in the 5620 SAM equipment navigation tree. The instance, diameter proxy agent, and policy charging rules properties are accessed from the main menu in the 5620 SAM GUI by choosing Manage→Mobile Core→DSC Instances.

The *5620 SAM User Guide* and other non-LTE documents in the 5620 SAM documentation suite do not describe 5780 DSC management. Management and configuration of the 5780 DSC with the 5620 SAM is described in the following documents:

- *5620 SAM LTE ePC User Guide*—Describes 5780 DSC discovery, configuration, troubleshooting, maintenance, security, and administration including feature and capacity licensing with the 5620 SAM.
- *5620 SAM LTE Parameter Reference*—Describes 5780 DSC parameters as represented in the 5620 SAM schema, in addition to parameters on LTE and LTE service forms in the 5620 SAM GUI.
- *5620 SAM LTE Alarm Reference*—Describes 5620 SAM LTE domain alarms and 5780 DSC device alarms.

1830 PSS support

The 1830 Photonic Service Switch (PSS) product family provides increased network flexibility and operational automation using zero-touch, transparent photonic networking. Photonic networks use simplified and accelerated operations to transform WDM into true transport networking with advanced flexibility, performance, automation, and integration.

The 5620 SAM supports the 1830 PSS product family of devices which includes:

- 1830 PSS 32—central office device, Release 2.5 and 2.5.1
- 1830 PSS 16—end office device, Release 2.5 and 2.5.1
- 1830 PSS 1—edge aggregation devices that collect lower rate signals for input to the 1830 PSS network. These include:
  - 1830 PSS 1 GBE edge device, Release 2.5
  - 1830 PSS 1 MD4H edge device, Release 1.5
  - 1830 PSS 1 AHP amplifier, Release 1.0

7750 SR support

The Alcatel-Lucent 7750 SR is a multi-service edge router designed for service providers, cable MSO, and enterprise customers that deliver residential, business and mobile services on a single IP/MPLS network. The 7750 SR is optimized for the delivery of high-performance data, voice and video services.

The 7750 SR is available in the following chassis sizes - 1 slot, 4 slots, 7 slots, and 12 slots - all of which offer a wide range of interfaces with density and service performance.

Leveraging the strength of the Alcatel-Lucent SR OS, the 7750 SR delivers the service flexibility to achieve the service continuity, service richness and service assurance critical to ensuring customer satisfaction and market leadership.

In order to determine which network ports are eligible to transport traffic of individual SDPs, the Network Domain feature has been introduced. This information is used for the SAP-ingress queue allocation algorithm applied to VPLS SAPs. See chapter 27 for more information.

7750 SR-c12

The 7750 SR-c12, which supports up to 12 CMAs or 6 MDAs, has a forwarding capacity of 40 Gb/s, native uplink support, and a faster control plane processor than the 7750 SR.

7750 SR-c4

The 7750 SR-c4, which supports up to 4 CMAs or 2 MDAs, has a forwarding capacity of 40 Gb/s, native uplink support, and a faster control plane processor than the 7750 SR. ICM-2 is a preconfigured MDA that you cannot add or delete using the 5620 SAM.

The 7750 SR-c4 supports:

- 7710 SR-c4, Release 8.0 or later, cards
- 7750 SR-c4 CFM-C4-XP
- 7750 SR-c4 IOM-C4-XP
- 5-port GIGE XP SFP CMA
- 1-port GIGE XP SFP CMA
- DC PEMs

7750 SR workflow

Table 11-1 lists the high-level network and element management tasks performed using the 5620 SAM for 7750 SR NEs. You can use this workflow to:

- to install, configure, create, and manage 7750 SR end-user NEs and services
- determine which workflow functions meet your user needs, then perform those functions

Table 11-1 Information on how to install, configure, create, and manage 7750 SR NEs and services

Procedure	See
View licensing information	Procedure 5-1
View 7750 SR device support	7750 SR support in this section
To change the license key in a standalone 5620 SAM system	Procedure 5-4
To change the license key in a redundant 5620 SAM system	Procedure 5-5
To configure secure communication between a 5620 SAM main server and database	Procedure 5-18
To configure the device for 5620 SAM management	Procedure 12-1
To change the system name	Procedure 5-19
In-band and out-of-band management procedures	Section 12.6
Equipment window overview	Section 16.1

(1 of 2)

Procedure	See
Implementing QoS workflow on the 7750 SR, 7450 ESS, 7710 SR, and 7705 SAR	Section 60.4

(2 of 2)

7710 SR support

The Alcatel-Lucent 7710 SR is a feature rich multiservice edge router available in modular, compact form factors. It is ideally suited for locations where lower throughput requirements are required to aggregate lower-speed subscribers over a wide variety of interfaces.

Designed for smaller PoPs, distributed hub sites and enterprise customer offices, the 7710 SR enables service providers to extend IP transformation to the furthest edge of their networks. The 7710 SR delivers unmatched service richness, service assurance and service velocity, giving service providers, cable MSOs and enterprise customers a competitive edge by allowing them to optimize their infrastructure buildouts with a fully featured router in a smaller footprint.

Optimized for the delivery of high-performance data, voice and video services, the Alcatel-Lucent 7710 SR is available in two chassis sizes to support up to 4 and up to 12 interface positions and a wide variety of interface types and speeds.

As a member of the industry-leading Alcatel-Lucent SR portfolio, the Alcatel-Lucent 7710 SR inherits the performance and reliability capabilities of Alcatel-Lucent's proven feature set and meets service-provider requirements for IP/MPLS platforms that are future-proof for innovative, profitable service delivery. Leveraging the strength of the Alcatel-Lucent Service Router Operating System (SR OS), the Alcatel-Lucent 7710 SR delivers unmatched service assurance, service richness and service velocity.

In order to determine which network ports are eligible to transport traffic of individual SDPs, the Network Domain feature has been introduced. This information is used for the SAP-ingress queue allocation algorithm applied to VPLS SAPs. See chapter 27 for more information.

7710 SR workflow

Table 11-2 lists the high-level network and element management tasks performed using the 5620 SAM for 7710 SR NEs. You can use this workflow to:

- to install, configure, create, and manage 7710 SR end-user NEs and services
- determine which workflow functions meet your user needs, then perform those functions

Table 11-2 Information on how to install, configure, create, and manage 7710 SR NEs and services

Procedure	More information
View licensing information	Procedure 5-1
View 7710 SR device support	7710 SR support

(1 of 2)

Procedure	More information
To change the license key in a standalone 5620 SAM system	Procedure 5-4
To change the license key in a redundant 5620 SAM system	Procedure 5-5
To configure secure communication between a 5620 SAM main server and database	Procedure 5-18
To configure the device for 5620 SAM management	Procedure 12-1
To change the system name	Procedure 5-19
Equipment window overview	Section 16.1
To configure a 7710 SR channelized TDM DS1 or E1 port	Procedure 17-75
Implementing QoS workflow on the 7750 SR, 7450 ESS, 7710 SR, and 7705 SAR	Section 60.4

(2 of 2)

7705 SAR support

The 7705 SAR is a cost-optimized IP/MPLS aggregation and mobile backhaul router that is well suited to the growing transport needs of the mobile RAN. Located at cell sites, the 7705 SAR uses pseudowires over MPLS to aggregate mobile 2G and 3G traffic and backhaul it to the core network. The 7705 SAR supports ATM, TDM, and Ethernet traffic.

7705 SAR workflow

Table 11-3 lists the high-level network and element management tasks performed using the 5620 SAM for 7705 SAR NEs. You can use this workflow to:

- to install, configure, create, and manage 7705 SAR end-user NEs and services
- determine which workflow functions meet your user needs, then perform those functions

Table 11-3 Information on how to install, configure, create, and manage 7705 SAR NEs and services

Procedure	See
View licensing information	Procedure 5-1
View 7705 SAR device support	7705 SAR support
To change the license key in a standalone 5620 SAM system	Procedure 5-4
To change the license key in a redundant 5620 SAM system	Procedure 5-5
To configure secure communication between a 5620 SAM main server and database	Procedure 5-18
To configure the device for 5620 SAM management	Procedure 12-1
In-band and out-of-band management procedures	Section 12.6

(1 of 2)

Procedure	See
7705 SAR-F daughter cards	7705 SAR-F daughter cards in chapter 15
Equipment window overview	Section 16.1
To enable or disable ICMP extensions on the 7705 SAR	Procedure 17-12
To modify the IEEE 1588 PTP clock on the 7705 SAR	Procedure 17-35
To modify the IEEE 1588 PTP port on the 7705 SAR	Procedure 17-36
To configure a 7705 SAR ASAP channelized TDM DS1 or E1 port	Procedure 17-76
Implementing QoS workflow on the 7750 SR, 7450 ESS, 7710 SR, and 7705 SAR	Section 60.4
7705 SAR fabric profiles	7705 SAR fabric profiles in chapter 44
To configure an 7705 SAR fabric profile	Procedure 44-23

(2 of 2)

7450 ESS support

The Alcatel-Lucent 7450 ESS sets a new market standard for enabling the delivery of profitable Ethernet business services in metro, national and international network environments. It also provides high density service-aware Ethernet aggregation for consumer triple-play services over IP/MPLS-based networks. The Alcatel-Lucent 7450 ESS is purpose-built for the service provider market, with an architecture that supports a wide range of interfaces and offers unmatched density and performance. The 7450 ESS allows service providers to offer new, revenue-generating services for both the consumer and business markets.

In order to determine which network ports are eligible to transport traffic of individual SDPs, the Network Domain feature has been introduced. This information is used for the SAP-ingress queue allocation algorithm applied to VPLS SAPs. See chapter 27 for more information.

7450 ESS workflow

Table 11-4 lists the high-level network and element management tasks performed using the 5620 SAM for 7450 ESS NEs. You can use this workflow to:

- to install, configure, create, and manage 7450 ESS end-user NEs and services
- determine which workflow functions meet your user needs, then perform those functions

Table 11-4 Information on how to install, configure, create, and manage 7450 ESS NEs and services

Procedure	More information
View licensing information	Procedure 5-1
View 7450 ESS device support	7450 ESS support

(1 of 2)

Procedure	More information
To change the license key in a standalone 5620 SAM system	Procedure 5-4
To change the license key in a redundant 5620 SAM system	Procedure 5-5
To configure secure communication between a 5620 SAM main server and database	Procedure 5-18
To configure the device for 5620 SAM management	Procedure 12-1
To change the system name	Procedure 5-19
In-band and out-of-band management procedures	Section 12.6
Equipment window overview	Section 16.1
Implementing QoS workflow on the 7750 SR, 7450 ESS, 7710 SR, and 7705 SAR	Section 60.4

(2 of 2)

7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco device support

The 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices support Ethernet and service-aware Ethernet aggregation across IP/MPLS networks. Typically, these devices are connected in rings or trees to 7450 ESSs to distribute L2 VPN or BTV services in VLANs.

The 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA can backhaul TDM lines through the core network using two 4-port CES modules. A 5620 SAM operator configures a CES module to receive E1 or T1 transmission, and then creates an interface on a logical port in the CES module to enable circuit emulation with dot1q encapsulation.

The 7250 SAS-ES and 7250 SAS-ESA support all of the functionality of the 7250 SAS. The 7250 SAS-ES and 7250 SAS-ESA also support two additional GigE uplink ports that enable the following features:

- hierarchical QoS
- RSVP-TE and FRR
- MPLS LSR functionality
- VPLS

The 7250 SAS-ESA also supports dry contact sensors. Four dry contact sensor inputs are available in a connector on the back panel of the 7250 SAS-ESA. The sensor inputs can be used to monitor the status of external equipment such as doors, power modules, fans, and batteries. When a sensor input detects a change in the state of a dry contact, the 7250 SAS-ESA sends an SNMP trap to the 5620 SAM. Depending on how the sensor inputs are configured, a change in the state of a dry contact can raise or clear an alarm condition.

The 5620 SAM provides element and network management functions for 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices using the CLI and SNMP. When a function is not supported by the device, the function cannot be selected from the GUI or does not appear on the GUI.

7250 SAS, 7250 SAS-ES, 7250 SAS-ESA and Telco device workflow

Table 11-5 lists the high-level network and element management tasks performed using the 5620 SAM for 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco device NEs. You can use this workflow to:

- to install, configure, create, and manage 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco device end-user NEs and services
- determine which workflow functions meet your user needs, then perform those functions

Table 11-5 Information on how to install, configure, create, and manage 7210 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco device NEs and services

Procedure	See
View licensing information	Procedure 5-1
View 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco device support	7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco device support
To change the license key in a standalone 5620 SAM system	Procedure 5-4
To change the license key in a redundant 5620 SAM system	Procedure 5-5
To configure secure communication between a 5620 SAM main server and database	Procedure 5-18
To configure the device for 5620 SAM management	Procedure 12-2
In-band and out-of-band management procedures	Section 12.6
Equipment window overview	Section 16.1
To configure Telco and 7250 SAS uplink ports as network ports	Procedure 17-65
To configure 7250 SAS-ESA dry contact sensors	Procedure 17-78
To configure a 7250 SAS, 7250 SAS-ES and 7250 SAS-ESA CES module	Procedure 17-79
To configure a 7250 SAS, 7250 SAS-ES and 7250 SAS-ESA CES port	Procedure 17-80
To create a 7250 SAS, 7250 SAS-ES and 7250 SAS-ESA unstructured CES interface	Procedure 17-81
To create a 7250 SAS, 7250 SAS-ES and 7250 SAS-ESA structured CES interface	Procedure 17-82
To modify a 7250 SAS, 7250 SAS-ES and 7250 SAS-ESA CES interface	Procedure 17-83
To configure bridging on a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device	Procedure 28-50
To create a 7250 SAS-ES or 7250 SAS-ESA guarding LSP	Procedure 29-10
To create a 7250 SAS-ES or 7250 SAS-ESA dynamic LSP	Procedure 29-11
To configure a 7250 SAS-ES or 7250 SAS-ESA LSP	Procedure 29-12
To view 7250 SAS-ES and 7250 SAS-ESA dynamic bypass LSP information	Procedure 29-24

(1 of 2)

Procedure	See
7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco policies	7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco policies in this section
To configure a 7250 SAS and Telco node QoS level policy	Procedure 44-31
To configure a 7250 SAS and Telco ACL standard IP filter policy	Procedure 45-4
To configure a 7250 SAS and Telco ACL extended IP filter policy	Procedure 45-5
To configure a 7250 SAS and Telco ACL IGMP filter policy	Procedure 45-6
To configure a 7250 SAS and Telco ACL MAC filter policy	Procedure 45-7
7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch network management	7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch network management in this section
Workflow to create a VLAN service (7250 SAS and Telco)	Section 65.7

(2 of 2)

OmniSwitch support

The 5620 SAM supports several OmniSwitch series Enterprise LAN switches. Table 11-6 lists the supported types.

Table 11-6 5620 SAM OmniSwitch support

Family	Characteristics	AOS Version Supported	Chassis and cards
OS 6250	Layer 2+ Fast Ethernet Stackable LAN family of switches for both the enterprise (SME) and Ethernet (Metro) access segments.	Release 6.6.1 or later	Non-PoE chassis • OS 6250-24 • OS 6250-8M • OS 6250-24M • OS 6250-24MD PoE chassis • OS 6250-P24
OS 6400	Stackable layer 2+ gigabit Ethernet LAN switch available in 24 or 48-port variants. Up to eight switches can be linked to form a stack.	Release 6.3.3 or later	Non-PoE chassis • OS6400-24 • OS6400-48 PoE chassis • OS6400-P24 • OS6400-P48 Fiber chassis • OS6400-U24 • OS6400-U24D
OS 6850	Stackable layer 2/3 gigabit Ethernet fixed configuration switch available in 24 or 48-port variants. Up to eight switches can be linked to form a stack.	Release 6.3.1 or later	Non-PoE chassis • OS6850-24 • OS6850-24X • OS6850-48 • OS6850-48X • OS6850-U24X • OS6850-24L • OS6850-48L PoE chassis • OS6850-P24 • OS6850-P24X • OS6850-P48 • OS6850-P48X • OS6850-P24L • OS6850-P48L
OS 6855	Stackable layer 2/3 gigabit Ethernet switch specifically built for IP network deployments where environmental operating conditions are unusually demanding. The OS 6855 is available with up to 24 gigabit ports and four combo ports.	Release 6.3.2 or later Stackability only among OS6855-U24X chassis, Release 6.4.2	Fiber chassis • OS6855-U10 • OS6855-U24 • OS6855-U24X (stackable) Copper with Po E chassis • OS6855-14 • OS6855-24

(1 of 2)

Family	Characteristics	AOS Version Supported	Chassis and cards
OS 9600	A five-slot chassis supporting one CMM and four network interface modules. It offers a wide range of GigE and 10GigE interfaces and power-over-Ethernet to support IP telephones, WLAN access points and video cameras. The OmniSwitch 9600 supports a maximum of two load sharing power supplies.	Release 6.3.1 R2 or later	CMM cards • OS9600-CMM • OS9700-CMM • OS9800-CMM Network interface cards • 2-port 10GigE XFP • 6-port 10GigE XFP • 24-port GigE SFP • 24-port GigE (10/100/1000) RJ45 • 24-port GigE (10/100/1000) RJ45 w/PoE • 48-port GigE (10/100/1000) MRJ21 • 20-port Fast Ethernet (10/100 – SW upgradable to 10/100/1000) RJ45 and 2-port GigE (100/1000) SFP
OS 9700	A high-density ten-slot chassis with two slots for control and eight slots for network interfaces supporting an aggregation of up to 192 GigE ports or 48 10GigE ports. Designed for smart continuous switching operation, the two center slots are dedicated to CMMs allowing redundant configurations. The OmniSwitch 9700 supports a maximum of three power supplies.	Release 6.3.1 R2 or later	
OS 9800	A high performance 18-slot switch supporting 16 slots for Gigabit Ethernet and/or 10-Gigabit Ethernet network interface modules. An additional two slots are reserved for primary and redundant CMMs. The OmniSwitch 9800 supports a maximum of four power supplies.	Release 6.3.1 R2 or later	
OS 9700E	The OS 9700E is a high performance switch offering eight slots for Gigabit Ethernet and/or 10-gigabit Ethernet Network Interface (NI) modules. Additional two slots are reserved for primary and redundant Chassis Management Modules (CMMs).	Release 6.4.2 R1 or later	Network interface cards • OS9-GNI-C24E: 24-port 10/100/1000 with RJ-45 support • OS9-GNI-U24E: 24-port 1000base-X with SFP/MiniGBIC support • OS9-XNI-U2E: 2-port unpopulated 10-Gigabit Ethernet with XFP support
OS 9800E	The OS 9800E is a high performance switch offering 16 slots for Gigabit Ethernet and/or 10-Gigabit Ethernet Network Interface (NI) modules. An additional two slots are reserved for primary and redundant Chassis Management Modules (CMMs).		

(2 of 2)

Caution 1 — OmniSwitch NEs do not support automatic synchronization with the 5620 SAM database when you use the CLI to make configuration changes. To ensure that you are viewing accurate configuration information using the 5620 SAM, perform a database synchronization by clicking on the appropriate Resync button.

Caution 2 — OmniSwitch NEs do not send trap notification for all MIB changes on the NE. To ensure that you are viewing the most up to date configuration information using the 5620 SAM, you must perform a resynchronization of the NE by clicking on the appropriate Resync button.

Using WebView to manage an OmniSwitch

You can configure and manage an OmniSwitch using the WebView application, an Alcatel-Lucent web-based device management tool that resides in the OmniSwitch. The following web browsers support the WebView application:

- Internet Explorer 6.0 or later for Windows NT, 2000, XP, 2003
- Netscape 7.1 for Windows NT, 2000, XP
- Netscape 7.0 for Solaris SunOS 5.8

See the appropriate OmniSwitch *Switch Management Guide* for information about configuring and using the WebView application.

See Procedure 17-52 to start the WebView application from the 5620 SAM GUI.

OmniSwitch workflow

Table 11-7 lists the high-level network and element management tasks performed using the 5620 SAM for OmniSwitch NEs. You can use this workflow to:

- to install, configure, create, and manage OmniSwitch end-user NEs and services
- determine which workflow functions meet your user needs, then perform those functions

Table 11-7 Information on how to install, configure, create, and manage OmniSwitch NEs and services

Procedure	More information
View licensing information	Procedure 5-1
View OmniSwitch device support	OmniSwitch support
To change the license key in a standalone 5620 SAM system	Procedure 5-4
To change the license key in a redundant 5620 SAM system	Procedure 5-5
To enable debug configuration file loading for mirror services	Procedure 5-25
To configure secure communication between a 5620 SAM main server and database	Procedure 5-18
To create a default SMPv2 OmniSwitch user on a 5620 SAM system	Procedure 5-26
To enable OmniSwitch functionality before managing with the 5620 SAM	Procedure 12-3
Network element in-band and out-of-band management overview	Section 12.3
To create an OmniSwitch RADIUS or TACACS+ security policy	Procedure 18-11
To perform an immediate OmniSwitch software upgrade	Procedure 21-13
OmniSwitch LAG objects	OmniSwitch LAG objects

(1 of 3)

Procedure	More information
Equipment window overview	Section 16.1
To create and configure an OmniSwitch LAG	Procedure 17-25
To create and configure OmniSwitch dynamic LAG members	Procedure 17-26
To configure OmniSwitch PoE Ports	Procedure 17-38
To configure OmniSwitch stacks	Procedure 17-39
To configure an OmniSwitch CPU temperature threshold	Procedure 17-40
To configure OmniSwitch Ethernet ports	Procedure 17-62
To manage OmniSwitch running configuration	Procedure 17-49
To configure OmniSwitch Health Monitoring	Procedure 17-51
To start and stop a Webview or Secure Webview session on an OmniSwitch	Procedure 17-52
To configure an advanced loopback test on an OmniSwitch port	Procedure 17-57
To configure an OmniSwitch 6xxx or 9xxx routing instance	Procedure 27-2
To configure UDP relay/DHCP snooping on an OmniSwitch in routing instances	Procedure 27-3
To create an OmniSwitch L3 interface	Procedure 27-5
To configure an OmniSwitch L3 interface	Procedure 27-7
To configure an OmniSwitch static route	Procedure 27-18
To configure IGMP on an OmniSwitch	Procedure 28-37
OmniSwitch DHCP Relay and Snooping	Omniswitch DHCP relay and snooping
To configure bridging on an OmniSwitch	Procedure 28-51
To release a violated OmniSwitch LPS port	Procedure 28-52
Implementing QoS workflow on an OmniSwitch	Section 60.3
OmniSwitch QoS policies	Chapter 44
To configure an OmniSwitch QoS policy condition	Procedure 44-32
To configure an OmniSwitch QoS policy action	Procedure 44-33
To create an OmniSwitch QoS policy	Procedure 44-34
To configure an OmniSwitch Ethernet service UNI profile	Procedure 48-1
To configure an OmniSwitch Ethernet SAP profile	Procedure 48-2
OmniSwitch policies	OmniSwitch policies
7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch network management	7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch network management
Workflow to create a VPLS service on OS 9700E and OS 9800E NEs	Section 68.4
Workflow to create a standard VLAN service (OmniSwitch)	Section 65.8

(2 of 3)

Procedure	More information
Workflow to create a stacked VLAN service (OmniSwitch)	Section 65.9
Workflow to create an IP multicast VLAN service (OmniSwitch)	Section 65.10
To create an OmniSwitch stacked VLAN service	Procedure 65-6
To create an OmniSwitch IP multicast VLAN service	Procedure 65-7
To add a MEP to an OmniSwitch VLAN service access interface	Procedure 65-10
To configure IGMP on an OmniSwitch VLAN site	Procedure 65-11
OmniSwitch ping and traceroute	OmniSwitch ping and traceroute
Sample OmniSwitch ping and traceroute CLI scripts	Section 35.4
To create an OmniSwitch OAM CLI scripts	Procedure 35-34
To configure and run an OmniSwitch OAM ping	Procedure 35-35
To configure and run an OmniSwitch OAM traceroute	Procedure 35-36

(3 of 3)

7210 SAS-E support

The Alcatel-Lucent 7210 SAS-E is designed as a Carrier Ethernet customer edge device, which is owned and managed by the service provider. Using software based on the SR OS and managed by the 5620 SAM, the 7210 SAS-E extends Carrier Ethernet VPN services to the customer edge. The 7210 SAS-E can also be deployed as an aggregation device for smaller sites.

The 7210 SAS-E supports:

- 7210 SAS-E chassis:
  - integrated IOM and Ethernet ports
  - 12 x 100/1000 SFP Ethernet ports; and copper SFPs
  - 12 x 10/100/1000 TX Ethernet ports
- in-band and out-of-band management (out-of-band management is supported only on the 7210 SAS-E Release 2.0 R2 or later)
- Epipe and VPLS supported; IES supported only for in-band management
- Ethernet ports, access and uplink modes
- Ethernet Ring Protection (G.8032)
- LLDP
- OAM:
  - ICMP ping
  - DNS and ICMP trace
  - CFM and EFM
- static routes for in-band management
- static and dynamic LAGs

- QoS policies:
  - 7210 Access Ingress
  - 7210 Access Egress
  - 7210 Port Access Egress
  - 7210 Network
  - 7210 Network Queue
  - 7210 Queue Management
  - 7210 Slope
  - 7210 Port Scheduler
  - 7210 Remarking
- backup and restore
- software upgrade
- statistics collection
- alarm management
- egress port rate limiting
- frame-based accounting

7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], and 7210 SAS-X 24F 2XFP support

The 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], and 7210 SAS-X 24F 2XFP support are customer edge devices that address the Metro Ethernet services, managed WAN services, and service aggregation markets. Using software based on the SR OS and managed by the 5620 SAM, the 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], and 7210 SAS-X 24F 2XFP extend Carrier Ethernet VPN services to the customer edge. The 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], and 7210 SAS-X 24F 2XFP support:

- 24 x 10/100/1000 Ethernet SFP ports
- 4 x Channelized DS1/T1 CES MDA (not supported on the 7210 SAS-X 24F 2XFP)
- in-band and out-of-band management (out-of-band management is only supported on the 7210 SAS-M Release 2.0 R2 or later)
- egress port rate limiting
- frame-based accounting
- H-metering
- services:
  - VLL Epipe
  - VLL Cpipe (not supported on the 7210 SAS-X 24F 2XFP)
  - VPLS (ELAN)
  - spoke SDP binding
- Ethernet Ring Protection (G.8032) (not supported on the 7210 SAS-X 24F 2XFP)
- LLDP
- CESoP Cpipe for CES MDA (not supported on the 7210 SAS-X 24F 2XFP)
- 2-Port Gig Ethernet MDA with SyncE (not supported on the 7210 SAS-X 24F 2XFP)

- STM OAM: CRM, EFM, CPE Ping, LSP Ping, MAC Ping, SDP/Tunnel Ping, MTU Ping, VCCV Ping, ICMP Ping, SVC Ping, DNS, LSP Trace, MAC Trace, MAC Populate, MAC Purge, and ICMP Trace
- QoS policies:
  - 7210 Access Ingress
  - 7210 Access Egress
  - 7210 Port Access Egress
  - 7210 Network
  - 7210 Network Queue
  - 7210 Queue Management
  - 7210 Slope
  - 7210 Port Scheduler
  - 7210 Remarking
- discovery management
- configuration backup and restore
- policy audit
- remote CLI
- security management
- software upgrade
- span of control
- statistics collection and graphing
- alarm management
- routing:
  - static routes
  - ISIS
  - OSPF
- IP/MPLS:
  - T-LDP
  - RSVP

In addition to all of the functionality of the 7210 SAS-M 24F, the 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, and 7210 SAS-X 24F 2XFP support two 10 GigE ports.

7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], and 7210 SAS-X 24F 2XFP workflow

Table 11-8 lists the high-level network and element management tasks that can be performed using the 5620 SAM for 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], and 7210 SAS-X 24F 2XFP NEs. You can use the workflow to:

- install, configure, create, and manage OmniSwitch end-user NEs and services
- determine the workflow functions that meet your user needs, and perform the functions

Table 11-8 Information about how to install, configure, create, and manage 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], and 7210 SAS-X 24F 2XFP NEs and services

Procedure	More information
To view licensing information	Procedure 5-1
To view 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP,7210 SAS-M 24F 2XFP [ETR], and 7210 SAS-X 24F 2XFP device support	7210 SAS-E support and 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], and 7210 SAS-X 24F 2XFP support
To change the license key in a standalone 5620 SAM system	Procedure 5-4
To change the license key in a redundant 5620 SAM system	Procedure 5-5.
To configure secure communication between a 5620 SAM main server and database	Procedure 5-18.
To configure the device for 5620 SAM management.	Procedure 12-3
To change the system name	Procedure 5-19
7210 SAS-E In-band management workflow	Chapter 12
7210 SAS-E daughter cards	7210 SAS-E daughter cards
7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], and 7210 SAS-X 24F 2XFP, and 7210 SAS-X 24F 2XFP daughter cards	7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7210 SAS-X 24F 2XFP daughter cards
Equipment window overview	Section 16.1
To create a 7210 SAS split horizon group	Procedure 17-6
To enable frame-based accounting on a 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], or 7210 SAS-X 24F 2XFP	Procedure 17-7
To configure 7250 SAS-ESA or 7210 SAS-M 24F 2XFP [ETR] dry contact sensors	Procedure 17-78
7210 SAS QoS policies	7210 SAS QoS policies
To configure a 7210 SAS access ingress policy	Procedure 44-2
To configure a 7210 SAS access egress policy	Procedure 44-5
To configure a 7210 SAS port access egress policy	Procedure 44-4
To configure a 7210 SAS network policy	Procedure 44-7
To configure a 7210 SAS slope policy	Procedure 44-9
To configure a 7210 SAS network queue policy	Procedure 44-13
To configure a 7210 SAS queue management policy	Procedure 44-11
To configure a 7210 SAS port scheduler policy	Procedure 44-18
To configure a 7210 SAS remarking policy	Procedure 44-24
To create a VLL Epipe service on the 7210 SAS-E	Procedure 67-2

9500 MPR support

The Alcatel-Lucent 9500 MPR is a microwave digital radio that supports PDH and Ethernet to migrate from TDM to IP. The 9500 MPR provides a generic, modular IP platform for multiple network applications, such as 2G, 3G, HSDPA, and WiMAX to accommodate broadband services.

The 9500 MPR supports:

- 4 and 8-slot MSS shelves
- removable core-enhanced, radio modem, 32 x DS1 and 32 x E1, 16 x E1 ASAP Access (ETSI) card, 2 x DS3 (ANSI) card, 4+4 x Ethernet (EAS) (ANSI) card, and cooling fan cards
- ODUs

MSS-4 and MSS-8 shelves

Slots 1 and 2 are reserved for core-enhanced cards. Each shelf must have a core-enhanced card installed in slot 1 and may have an optional spare card installed in slot 2 to protect the main card.

The MSS-4 shelf supports cards in slots 3 and 4. The card slots can be used for unprotected radio modem or 32 x DS1 and 32 x E1 cards or a card in slot 3 can be protected by an identical card in slot 4.

The MSS-8 shelf supports six additional card slots. The slots support any combination of unprotected radio modem or 32 x DS1 and 32 xE1 cards, or a combination of protected and unprotected cards. Protected cards must be installed in slots 3, 5, or 7 and are protected by optional identical cards in slots 4, 6, and 8 respectively.

Core-enhanced card

The core-enhanced card in slot 1 provides:

- node management and control functions
- dc power
- a plug-in flash memory card to store node configuration and license data
- an Ethernet switch that implements all of the cross-connections between the radio modem or 32 x DS1 and 32 x E1 cards, between the Ethernet user ports, and between the Ethernet ports and the radio modem or 32 x DS1 and 32 xE1 cards
- four electrical Ethernet ports; port 4 can be used as an additional management port if required
- two SFP Ethernet ports; the ports are supported by the 5620 SAM when an SFP is installed

An optional identical core-enhanced card can be installed in card slot 2. The card provides protection if the card fails.

Core-B card

The Core-B card in slot 1provides:

- node management and control functions
- dc power
- a plug-in flash memory card to store node configuration and license data
- an Ethernet switch that implements all of the cross-connections between the radio modem or 32 x DS1 cards, between the Ethernet user ports, and between the Ethernet ports and the radio modem or 32 x DS1 cards
- four Gigabit Ethernet electrical interfaces and one Gigabit Ethernet optical interface (SFP)

An optional identical core-enhanced card can be installed in card slot 2. The card provides protection if the card fails.

Note — The Core-B card is supported on 9500 MPR for ANSI 1.2.0 only.

Radio modem card

The radio modem card:

- sends and receives standard Ethernet packets to and from the core-enhanced cards
- manages the radio frame generation and termination, the interface to and from the alternate radio transport card, and the cable interface functions to the ODU
- contains EPS and RPS logic
- generates internal dc power for the card

32xE1(ETSI) card and 32xDS1(ANSI) card

Two 32 port cards versions are available: the 32 x E1 ETSI standard based and the 32 x DS1 ANSI standard based cards.

- provides external interfaces for up to 32 E1or DS1 ports
- manages the encapsulation and reconstruction of PDH data for standard Ethernet packets
- sends and receives standard Ethernet packets to and from core-enhanced cards
- contains the switch for EPS core protection
- generates internal dc power

2 x DS3 (ANSI) card

Two DS3 ports are available.

- supports up to six units per shelf
- 1+1 EPS protection

4+4 x Ethernet (EAS) card

The EAS module is supported on card slots 3 and 4 only.This ANSI- based card supports 4 x Ethernet 10/100/1000-base T (traffic) and 4+4 x Ethernet (Access/MPT) connection interfaces. Each chassis allows for two EAS modules.

2+2 x Ethernet (EAS) card

The EAS module can be configured with two types of MPT radio ports: MPT-HC and MPT-MC. MPT-MCs can be configured on ports 1 and 2 only and cannot be involved in protection. MPT-HCs can be configured on any of the four ports and if the corresponding port on the consecutive slot has the same card with the same MPT type, then protection is applicable.

16 x E1 ASAP Access (ETSI) card

The 16 x E1 ASAP Access (ETSI) card enables the management of ATM services on the 9500 MPR, through collecting IMA traffic, terminating the IMA groups and encapsulating and extracting the ATM cells into and from ATM PW (pseudo-wire) packets towards the core board. ATM interfaces are established over PDH physical interfaces. ATM traffic is transported by the ATM PW service encapsulated into Ethernet frames. This card is supported for the ETSI 1.3.0 software loads.

ODU

The ODU is a microprocessor-controlled transceiver that interfaces the MSS with the microwave antenna. Each radio modem card connects to one ODU. A 1 + 0 radio modem protection scheme requires one radio modem card and one ODU for each radio direction. Two radio modem cards and two associated ODUs must be provisioned in each radio direction for the 1+1 protection scheme.

Using the 9500 MPR external element manager

You can start the 9500 MPR external element manager, NEtO, from the 5620 SAM GUI. See the 9500 MPR user documentation for information about installing and using the NEtO network element manager. See Procedure 17-53 for information about starting the external element manager from the 5620 SAM GUI.

Backup/Restore

When discovered, 9500 MPR NEs are automatically assigned to the default MPR Backup Policy and the MPR Read/Write Policy.

The MPR Read/Write Policy is a mediation policy that is automatically created and contains the default FTP authentication details which have to be updated accordingly based on the FTP login details required for backup/restore.

Bof save and CLI are not supported on 9500 MPR NEs. See Procedure 21-3 for information about creating a 9500 MPR backup policy.

9500 MPR workflow

Table 11-9 lists the high-level network and element management tasks performed using the 5620 SAM for 9500 MPR NEs. You can use this workflow to:

- to install, configure, create, and manage 9500 MPR end-user NEs and services
- determine which workflow functions meet your user needs, then perform those functions

Table 11-9 Information on how to install, configure, create, and manage 9500 MPR NEs and services

Procedure	More information
View licensing information	Procedure 5-1
View 9500 MPR device support	9500 MPR support
Enable 9500 MPR management by the 5620 SAM	Procedure 12-11
Enable initial set setup and view workflow of 9500 MPR In-band management	Section
To cross launch the 9400 AWY, MPT-sa, or MSS-1c J-USM manager	Procedure 12-6
View the workflow for a 9500 MPR software upgrade	Section 21.5
Create a 9500 MPR backup policy	Procedure 21-3
Perform an immediate 9500 MPR software upgrade	Procedure 21-14
Work with 9500 MPR shelf objects	Working with shelf objects
Work with 9500 MPR card and card slot objects	Working with card and card slot objects
Work with 9500 MPR physical links	Working with physical links
Equipment window overview	Section 16.1
Add 9500 MPR card protection	Procedure 17-28
Remove 9500 MPR card protection	Procedure 17-29
Add 9500 MPR port protection	Procedure 17-30
Remove 9500 MPR port protection	Procedure 17-31
Configure timing synchronization	Procedure 17-34
Configure 9500 MPR Ethernet ports	Procedure 17-63
To configure power source type on 2+2 x Ethernet (EAS) card slots for 9500 MPR (ETSI 2.1)	Procedure 17-64
Manage 9500 MPR running software	Procedure 17-50
Start the 9500 MPR external element manager (NEtO)	Procedure 17-53
Configure 9500 MPR E1 and DS1 ports	Procedure 17-66
Configure 9500 MPR DS3 ports	Procedure 17-67
Configure 9500 MPR radio modem ports	Procedure 17-68
To configure analog performance management on 9500 MPR radio modem ports	Procedure 17-69
To configure 9500 MPR port segregation	Procedure 17-70

(1 of 2)

Procedure	More information
To configure a loopback test on a 9500 MPR DS1, ES1 or radio modem port	Procedure 17-71
Configure VLAN groups and paths	Chapter 66
View a definition of a 9500 MPR Cpipe	9500 MPR Cpipe
Configure one or more 9500 MPR ATM QoS policies.	Procedure 44-30
View the workflow to create a 9500 MPR Cpipe service	Section 67.4
Create a 9500 MPR Epipe service (ANSI only)	Procedure 67-3
Create a 9500 MPR Apipe service (ETSI only)	Procedure 67-5
Create a 9500 MPR Cpipe service	Procedure 67-9
Fix a failed cross-connection in a 9500 MPR cpipe	Procedure 67-10
Create a 9500 MPR Dot1Q VLAN service (ETSI only)	Procedure 65-8
9500 MPR Error Recovery Mechanism	Procedure 34-10

(2 of 2)

Generic NE support

The 5620 SAM provides limited management support of generic NEs, which are non-Alcatel-Lucent devices, using generic NE profiles, alarm catalogues, and CLI scripts. A generic NE profile includes the following elements:

- the device MIB system object ID
- regular-expression strings that specify the format of prompts and commands
- the SNMP trap management configuration
- interfaces that can be specified as the endpoints of 5620 SAM physical links
- an optional alarm catalogue, which defines the alarms that the 5620 SAM raises in response to SNMP traps from the generic NE

Note 1 — By default, only the 5620 SAM admin user, or an operator with an assigned admin scope of command role, can manage generic NE profiles and alarm catalogues. A non-admin user requires the genericne scope of command role to manage generic NE profiles.

Note 2 — To create, modify, or delete a generic NE alarm catalogue or mapping, you require a trapmapper scope of command role with write, update, and execute permissions.

See chapter 12 for information about configuring a generic NE profile.

Generic NE device discovery and polling in the 5620 SAM are configured using the same methods that are used for an Alcatel-Lucent NE, but the 5620 SAM uses preconfigured scripts to manage and unmanage a generic NE. See chapter 10 for information about device discovery. See chapter 24 for information about creating CLI scripts using the 5620 SAM script manager.

The 5620 SAM displays generic NEs, but not generic NE interfaces, on the topology map and in the navigation tree.

Statistics support

The 5620 SAM supports the collection of a limited set of statistics counters from standard system, interface, and routing MIBs on generic NEs. These statistics are processed and presented in the same manner as statistics from other devices. You can view generic NE statistics on the Statistics tab of a generic NE interface properties form, retrieve them using the OSSI, and display them graphically using the 5620 SAM Statistics Plotter.

Note 1 — To collect or view generic NE statistics from routing MIBs, you require a valid 5650 CPAM license that has a third-party router quantity greater than zero.

Note 2 — If persistent SNMP indexes are not enabled on a generic NE, one or more generic NE interface indexes may change after a generic NE reboots. This can cause a mismatch between the statistics records collected before the reboot and the current interface indexes. The 5620 SAM takes no action to identify or correct such a mismatch.

Alarm support

By default, the 5620 SAM supports a limited number of standard system and interface SNMP traps for generic NEs. The 5620 SAM monitors SNMP reachability and interface status, and raises a standard alarm for each the following events:

- coldStart—The generic NE restarts.
- linkDown—An interface goes out of service.
- linkUp—An interface returns to service.

Note — When the 5620 SAM drops or fails to receive an SNMP trap from a generic NE, the trap is lost. The 5620 SAM is unable to request that a generic NE resend an SNMP trap.

You can configure the 5620 SAM to raise user-defined alarms in response to specific generic NE traps using alarm catalogues. An alarm catalogue is a set of trap-to-alarm mappings that can be associated with a generic NE profile. A generic NE profile can have at most one alarm catalogue, but each catalogue can contain up to 150 alarm mappings. When a mapping is administratively disabled, the 5620 SAM raises no alarm in response to an associated trap from a generic NE.

An alarm mapping can be static, which means that it maps to a specific alarm, or the mapping can use one or more transform functions that extend the mapping customization. A transform function defines conditions that enable the dynamic mapping of a trap to an alarm that is created using varbind values in an SNMP trap PDU. For example, you can use a transform function to assign a specific alarm name, severity, or probable cause to an alarm based on varbind values.

You can use a 5620 SAM GUI or OSS client to configure generic NE alarm catalogues and alarm mappings. The GUI supports the following methods:

- configuration forms—for object creation, modification, viewing, and deletion
  See chapter 12 for information about managing generic NE alarm catalogues using configuration forms.

- XML API script—for object creation and modification only
  A script template for alarm catalogue configuration is available at the following location below the 5620 SAM main server installation directory, typically /opt/5620sam/server on Solaris or C:\5620sam\server on Windows:
  install_dir/nms/sample/xmlapi/AlarmCatalogue-Template.txt

See the *5620 SAM Scripts and Templates Developer Guide* for information about using the Script Manager.

An OSS client can also retrieve a catalogue or a subset of the alarm mappings in a catalogue using the standard methods.

When the 5620 SAM receives a generic NE trap that is not one of the supported standard traps or a mapped trap in an alarm catalogue, the 5620 SAM drops the trap. When the 5620 SAM receives a high trap volume and must discard traps that it cannot process, it does not distinguish between standard and user-defined traps. To conserve system resources, Alcatel-Lucent recommends that you configure a generic NE to send only the required traps to the 5620 SAM.

Traps that map to user-defined alarms require extra processing by the 5620 SAM and are managed in a separate, resource-limited queue. When this queue fills, the 5620 SAM discards some of the traps and raises an alarm. You can monitor the queue length using the 5620 SAM Resource Manager.

Generic NE trap sequencing and throttling support are configurable in a generic NE profile. After the 5620 SAM finishes throttling traps from a generic NE or encounters a trap sequence error, it resynchronizes the discovered device MIBs.

12 — Device commissioning and management

12.1 Device commissioning overview

An Alcatel-Lucent device, Telco device, or generic NE requires commissioning preconfiguration before the 5620 SAM can manage it. When this preconfiguration is complete, the 5620 SAM can discover the device, as described in chapter 13.

Some devices, such as the 7210 SAS-E and 9500 MPR, require configuration in addition to device commissioning before the 5620 SAM can discover or manage them. See section 12.2 for information about device-specific management requirements.

Commissioning generic NEs for 5620 SAM management

The 5620 SAM uses configurable profiles and CLI configuration scripts to discover and manage generic NEs. You can use the same generic NE profile for multiple devices of the same type. Before the 5620 SAM can discover a generic NE using a discovery rule, the following conditions must be true:

- The device preconfiguration is complete.
- A 5620 SAM generic NE profile for the device exists.
- A 5620 SAM mediation policy is configured with a community string that matches the community string specified during the device preconfiguration.
- A discovery rule is configured to represent the device.

See chapter 13 for information about mediation policies and device discovery. See section 12.2 for information about configuring user-defined alarms for generic NE management.

Note 1 — By default, only the 5620 SAM admin user or an operator with an assigned admin scope of command role can manage generic NE profiles and alarm catalogs. A non-admin user requires an assigned generic NE scope of command role to manage generic NEs.

Note 2 — When multiple generic NE profiles contain possible matches for a system object ID, the profile that contains the system object ID with the longest or most specific match is chosen.

Note 3 — To create, modify, or delete a generic NE alarm catalog or mapping, you require a trapmapper scope of command role with write, update, and execute permissions.

12.2 Device management overview

The 5620 SAM supports in-band and out-of-band management of devices.

When you configure in-band management only, management traffic between the 5620 SAM and a device is transmitted through any port that is configured for network access, but not the management port. Using in-band management, the 5620 SAM sends management traffic to the system IP address of the device, or to an optional L3 management interface.

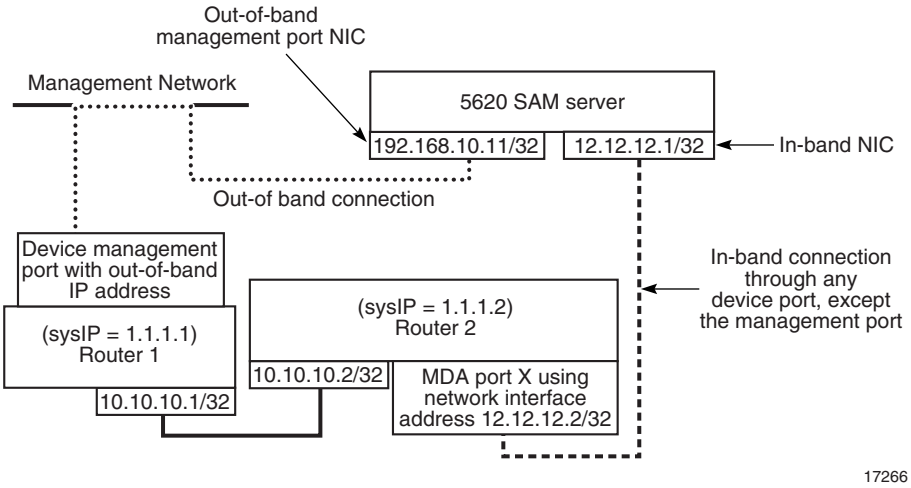
When you configure out-of-band management only, management traffic between the 5620 SAM and a device is transmitted through the management port of the device. Using out-of-band management, the 5620 SAM sends management traffic to the management IP address of the device.

When you configure a device for in-band and out-of-band management, one method provides redundancy for the other. If the IP addresses are the same, redundancy is not supported. Redundancy is not supported on the OmniSwitch.

Figure 12-1 shows an example of in-band and out-of-band management.

Note — To enable in-band management of a device, you must manually configure a second trap destination and trap log on the device.

Figure 12-1 Example of in-band and out-of-band management



The type of management is determined during device discovery. When the device is discovered using its management IP address, management is out of band. When the device is discovered using its system IP address or an L3 interface IP address, management is in band. In each case, a valid route to the device must exist. See chapter 13 for more information about the discovery process.

In Figure 12-1, there is an out-of-band management route that allows a ping from the 5620 SAM to the management IP address of router 1 (192.168.10.1/32). The in-band connection sends management packets to the system IP address on router 2 (12.12.12.2/32) on MDA port X.

Caution — Do not use the 5620 SAM to alter the configuration of the in-band port. If the port is shut down, network visibility is lost.

Some device types require configuration in addition to the SNMP configuration before they can be managed by the 5620 SAM. See the appropriate part of this section for device-specific management information.

Firewalls and management bandwidth

The ports between 5620 SAM components, and between the 5620 SAM system and the managed devices, must be open through firewalls to allow proper operation of the software. See the *5620 SAM Planning Guide* for more information about requirements for the following:

- firewalls and open ports
- communication bandwidth between 5620 SAM components
- communication bandwidth between the 5620 SAM and managed network

IPv6 management

The 5620 SAM supports device management using IPv6 for devices with IPv6 capabilities. The management protocol is established when the device is discovered. When a device is configured with an IPv6 address on its management port and/or system interface and the discovery rule is configured to discover IPv6 addresses, the 5620 SAM discovers and manages the device using IPv6. To change a device management protocol between IPv4 and IPv6, you must unmanage the device, create a new discovery rule specifying the new management protocol, and then rediscover the device.

Note — To manage 7750 SR, 7710 SR, or 7450 ESS devices using IPv6, the device must also be configured with an IPv4 address on the management port for out-of-band management, or an IPv4 address on the system interface for in-band management.

The 5620 SAM supports the configuration of IPv4 and IPv6 in-band and out-of-band management addresses on the same device.

Secure file transfers

The 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], 7210 SAS-X 24F 2XFP, 7450 ESS, and 7750 SR support secure file transfers using SSH2. When SSH2 is corectly configured and the secure file transfer type is configured in the SSH2 mediation policy for the device, the SCP is used to perform file transfers to and from the managed devices. See chapter 13 for more information about configuring SSH2.

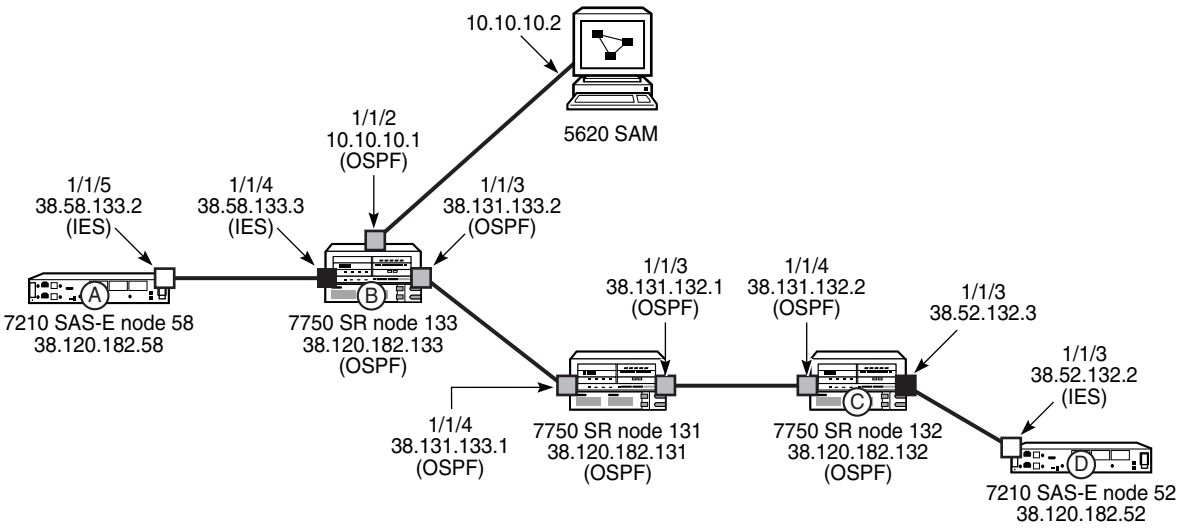
7210 SAS in-band and out-of-band management

The 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP [ETR], and 7210 SAS-X 24F 2XFP support in-band and out-of-band management. The 7210 SAS-E supports static routes, but does not support an IGP or SDPs. The example network shown in Figure 12-2 and the associated configuration steps describe the configuration required to enable 7210 SAS-E in-band management using static routes that are distributed to an IGP, which, in the example, is OSPF.

Note 1 — The 7210 SAS-E Release 2.0 R2 or later supports out-of-band management.

Note 2 — The 7210 SAS-M Release 2.0 R2 or later supports out-of-band management.

Figure 12-2 Example 7210 SAS-E in-band management network



Ⓐ static-route 10.10.10.0/24 next-hop 38.58.133.3, static-route 38.120.182.0/24 next-hop 38.58.133.3

Ⓑ static-route 38.120.182.58/32 next-hop 38.58.133.2, Distribute the static routes to OSPF

Ⓒ static-route 38.120.182.52/32 next-hop 38.52.132.2, Distribute the static routes to OSPF

Ⓓ static-route 10.10.10.0/24 next-hop 38.52.132.3, static-route 38.120.182.0/24 next-hop 38.52.132.3

Legend:
- Access Uplink port
- Access port
- Network port

20259

The following configuration steps are required to set up the example network:

1 Using the CLI, configure the SNMP security parameters on the devices that you need to discover. See Procedure 12-1 for more information.

2 Perform the following steps on node 133:

- Configure an interface on port 1/1/2 that connects to the 5620 SAM server interface.
- Configure an interface on port 1/1/3, which is connected to node 131.
- Create an L3 interface on port 1/1/4 by creating an IES.
- Create a static route to node 58.
- Create an ASBR OSPF (area 0.0.0.0) instance on the system and enable OSPF on the interfaces to node 131 and the 5620 SAM server.
- Create a routing policy to distribute the static route to OSPF.

3 Perform the following steps on node 131:

- Configure an L3 interface on port 1/1/4, which is connected to node 133.
- Configure an L3 interface on port 1/1/3, which is connected to node 132.
- Enable OSPF (area 0.0.0.0) on the system and the interfaces connected to nodes 133 and 132.

4 Perform the following steps on node 132:

- Create an L3 interface on port 1/1/4, which is connected to node 131.
- Create an L3 interface on port 1/1/3, which is connected to node 52.
- Create a static route to node 52.
- Create an ASBR OSPF (area 0.0.0.0) instance on the system and enable OSPF on the interface to node 131.
- Create a routing policy to distribute the static route to OSPF.

5 Perform the following steps on node 52:

- Create an IES L3 interface on port 1/1/3, which is an uplink port.
- Create static routes that direct traffic to the IES L3 interface.

6 Perform the following steps on node 58:

- Create a IES L3 interface on port 1/1/5, which is configured as an uplink port.
- Create static routes to direct traffic to the IES L3 interface.

7 Ensure that each 7210 SAS-E can ping the network interface IP address which is configured on the 5620 SAM main server.

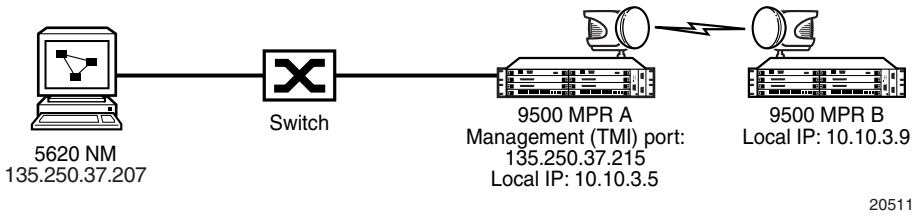
8 Ensure that the 5620 SAM main server can ping the system IP address of each 7210 SAS-E.

9 Configure an in-band polling policy using the 5620 SAM. See Procedure 12-9 for more information.

9500 MPR in-band management

To enable 9500 MPR in-band management, the 5620 SAM requires connectivity to the 9500 MPR NE, as shown in Figure 12-3 and described in the associated example configuration steps.

Figure 12-3 Example of 9500 MPR In-band management



Perform the following initial configuration on the 9500 MPR:

1 Ensure that the 9500 MPR A and 9500 MPR B NEs belong to the same OSPF area, and the radio links are bound to this OSPF area.

2 Ensure that the radio link between the 9500 MPRs is working by pinging the local IP addresses. In the network shown in Figure 12-3, 9500 MPR B should be able to ping the local IP address of 9500 MPR A.

3 Connect 9500 MPR A to the switch using the TMN port or port 4 of 9500 MPR A.

4 Configure the management port and local IP addresses on the 9500 MPRs; the addresses can be different or the same.

Perform the following network configuration:

1 Verify that you can ping the management port of 9500 MPR A from the 5620 SAM.

2 If the management and local IP addresses on 9500 MPR A are in different subnets, you must add a static route to the 5620 SAM server. Use the local IP address of 9500 MPR A as the destination and the management IP address of 9500 MPR A as the gateway.

3 Verify that you can ping the local IP address of 9500 MPR A from the 5620 SAM. If you cannot ping the local IP address of 9500 MPR A from the 5620 SAM, add a default route to 9500 MPR A. Use the management IP address of 9500 MPR A as the gateway.

4 Add a static route to the 5620 SAM using the local IP address of 9500 MPR B as the destination and the management IP address of 9500 MPR A as the gateway.

5 Verify that you can ping the management IP address of 9500 MPR A from 9500 MPR B. If the ping fails, add a default route to 9500 MPR B using the management IP address of 9500 MPR A as the destination and the local IP address of 9500 MPR A as the gateway.

6 Verify that you can ping the local IP address of 9500 MPR A and 9500 MPR B from the 5620 SAM server. The 5620 SAM should be able to discover and manage the 9500 MPRs after connectivity has been established between the 5620 SAM and the 9500 MPR nodes. See "9500 MPR support" for more information about 9500 MPR node discovery and management.

Note 1 — Port 4 can also be used for In-band management of 9500 MPR NEs over physical links similar to the setup below. You need to configure port 4 as TMN and also to configure it with an IP address. Ensure that all the NEs are reachable from the 5620 SAM server by configuring static routes or enabling OSPF. The setup is:

nge0_SAM_nge1-----MPRA ------(radio)------MPRB-----(Radio)-----MPRC_port#4 ---------port#4_MPRD

Note 2 — For ANSI, Release 2.2.0 or later, port 3 and port 5 can also be used by enabling the TMN In-band feature.

Configuring user-defined alarms for generic NEs

As part of a generic NE profile, you can map SNMP traps from generic NEs to user-defined 5620 SAM alarms in an alarm catalogue. A generic NE profile can be associated with only one alarm catalogue, but an alarm catalogue can contain up to 150 trap-to-alarm mappings.

A mapping is one of the following types:

- static—A specific SNMP trap is associated with a specific alarm.
- dynamic—The mapping includes one or more transform functions that define alarm properties based on values in SNMP trap PDUs.

Each mapping in a catalogue defines an alarm that the 5620 SAM raises or clears when it receives a specific SNMP trap. A mapping includes standard elements such as the trap OID, alarm type, probable cause, and severity, but can include the following optional elements:

- trap name
- self-clearing designation—specifies that the alarm clears when a specific clearing trap is received, and has the following requirements:
  - If the severity of the raising alarm is a static value, the clearing trap must have a static mapping in the same catalogue as the raising trap, and can be linked to only one raising trap
  - If the severity of the raising alarm is defined using a transform function, the transform function must include a raising value pair and a clearing value pair.
- FDN extension, which is an alarm-name extension that can include the following:
  - static text
  - scripting functions—expressions that specify the trap PDU values to include; these allow the same alarm type to be raised in response to different traps while uniquely identifying the trap origin in the alarm name
- additional text—used to provide information of value related to the trap event, for example, troubleshooting actions; the additional text consists of the trap OID by default, but can include the following:
  - static text
  - scripting functions—expressions that specify the trap PDU values to include; these are used to generate a more precise description of the alarm condition

Note — The FDN extension of a generic NE alarm is not appended to the Alarm Name field in the 5620 SAM GUI, but is included in the Additional Text field. To create a filter for generic NE alarms that have FDN extensions, you must filter on the Additional Text field.

A change to an alarm catalogue or to a mapping in a catalogue takes effect when you commit the change.

Transform functions

A transform function is an optional catalogue component that associates one or more values in an SNMP trap PDU with an alarm property such as the alarm name, probable cause, or severity. For example, you can create a transform function that assigns an alarm severity of Critical when the value in a specific varbind is 1, Major when the value is 2, and Minor when the value is 3.

When an alarm mapping includes one or more transform functions, the 5620 SAM can raise multiple alarms in response to the same SNMP trap. A trap value and the associated alarm property value are specified as a value pair in a transform function. You can also specify a default alarm property value that the 5620 SAM assigns to an alarm when a received value is not defined in a value pair.

A transform function defines the input value type, such as integer, and the output alarm property type, such as severity. You can modify these parameters only when the transform function does not contain a value pair and is not used by a mapping.

A transform function returns an empty string when a received value is not defined in a value pair and no default alarm property value is assigned. When the transform function defines the alarm name, probable cause, or severity, the 5620 SAM logs an error in response and does not raise an alarm.

12.3 Device commissioning and management workflow

1 Using a CLI, configure the SNMP parameters on the device. See Procedures 12-1 and 12-2.

2 Install and configure network interface cards on the 5620 SAM: one for in-band and one for out-of-band management networks.

3 Configure each device for in-band or out-of-band management, as required: in-band management traffic is transmitted using any network-configured port other than the management port. Out-of-band management traffic is transmitted using the device management port.

Note — You can discover devices using an in-band or an out-of-band connection. Ensure that each device in the network has routing enabled for the in-band and out-of-band addresses before you configure the discovery rules, as described in chapter 13.

4 If required, enable 5620 SAM in-band management of the device by manually configuring a second trap destination and trap log on the device.

5 Establish a route for in-band traffic, if required. For example, configure a static route or use OSPF.

6 Configure in-band or out-of band polling policies, as required. See Procedure 12-9.

12.4 Alcatel-Lucent and Telco device commissioning procedures

The following procedures describe how to configure the 5620 SAM to manage Alcatel-Lucent or Telco device.

Procedure 12-1 To commission a 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, 7705 SAR, 7710 SR, or 7750 SR for 5620 SAM management

See the appropriate device documentation for information about using a device CLI.

Caution — Do not apply an SNMP log filter to the 5620 SAM SNMP log. The 5620 SAM cannot manage an NE that has an SNMP log filter applied to the log used by the 5620 SAM, which is typically log ID 98.

1 Open a console window on the device.

2 Enter the following command at the prompt to configure the system address of the device:

configure router interface "system" address *xxx.xxx.xxx.xxx/mask* ↵

where <*xxx.xxx.xxx.xxx*> is the system IP address
mask is the bit mask

3 Enter the following command at the prompt to enable Telnet:

configure system security telnet-server ↵

4 Enter the following command at the prompt to enable FTP:

configure system security ftp-server ↵

5 If required, enter the following command at the prompt to enable SSH2:

configure system security ssh version 2 ↵

6 Enter the following command at the prompt to enable console, FTP, and SNMP access for the appropriate user account on the device:

configure system security user *user_account* access console ftp snmp ↵

where *user_account* is the appropriate user account for Telnet, FTP, and SNMP access, for example, admin

7 If required, enter the following command at the prompt to enable hash encryption for passwords and authentication keys during device configuration save or list operations:

configure system security hash-control read-version *read-version* write-version *write-version* ↵

where
read-version is the version of encryption accepted during read operations, for example, 1, 2, or all to indicate that both are accepted
write-version is the version of encryption used during write operations, for example, 1 or 2

Version 1 encryption uses a simple key algorithm that generates the same character string each time it hashes a specific password or authentication key.

Version 2 encryption uses a more complex key algorithm that generates a different character string each time it hashes a specific password or authentication key.

8 Enter the following commands in sequence at the prompt to set the time zone and time:

configure system time zone *time_zone* -*offset_from_UCT* ↵

admin set-time *YYYY/MM/DD hh:mm:ss* ↵

where
time_zone is the appropriate time zone, for example, EST
offset_from_UCT is the offset, in hours, from Universal Co-ordinated Time, also known as Greenwich Mean Time, for example, if you specify EST, *offset_from_UCT* is -5, as EST lags UCT by five hours
YYYY/MM/DD hh:mm:ss is the current local time

9 If required, perform one of the following to enable a time protocol.

a Enter the following command at the prompt to enable NTP:

configure system time ntp server-address *server_IP_address* ↵

where
server_IP_address is the IP address of the SNTP server

b Enter the following command at the prompt to enable SNTP:

configure system time sntp server-address *server_IP_address* ↵

where
server_IP_address is the IP address of the SNTP server

10 Enter the following commands in sequence at the prompt to enable the SNMPv2 engine and to configure an SNMP community:

configure system snmp no shutdown ↵

configure system snmp packet-size 9216 ↵

configure system security snmp community *community_name* rwa version both ↵

where *community_name* is the SNMPv2 community name

Note 1 — The command is used for the 5620 SAM write mediation policy. If you are using SNMPv2, you must use this mediation policy for read as well, or create another mediation policy that is also configured for rwa.

Note 2 — The SNMPv2 community string name rwa attributes must be enabled for the 5620 SAM to properly manage a node, even if the 5620 SAM is only used to monitor a network.

Note 3 — To configure SNMPv3 management on the device, see Procedure 13-1.

11 Enter the following commands in sequence at the prompt to ensure that the device uses persistent SNMP indexes:

bof persist on ↵

bof save ↵

12 Enter the following commands in sequence at the prompt to save the configuration changes and reboot the device:

admin save ↵

admin synchronize boot-env ↵

admin reboot now ↵

The device initializes with SNMP communication enabled.

13 Type the following to clear the log ID and trap group ID:

configure log ↵

log-id 98 ↵

shutdown ↵

exit ↵

no log-id 98 ↵

no snmp-trap-group 98 ↵

exit all ↵

14 Use a 5620 SAM client to discover the device and to verify that the device configuration allows management of the device, for example, by performing a device configuration backup. See chapter 13 for information about device discovery. See chapter 21 for information about performing device configuration backups.

15 Enter the following commands in sequence at the prompt to ensure that the SNMP trap configuration is correct:

configure log ↵

info ↵

The output should look similar to the following:

```
snmp-trap-group 98
description "5620sam"
trap-target "xxx.xxx.xxx.xxx:162" address
xxx.xxx.xxx.xxx snmpv2c notify-community "privatetrap98"
trap-target "yyy.yyy.yyy.yyy:162" address
yyy.yyy.yyy.yyy snmpv2c notify-community "privatetrap98"
```

```
 exit

 log-id 95

 from security

 to snmp 1024

 exit

snmp-trap-group 95

description "5620sam"

trap-target "xxx.xxx.xxx.xxx:162" address xxx.xxx.xxx.xxx snmpv2c
notify-community "privatetrap98"

trap-target "yyy.yyy.yyy.yyy:162" address  yyy.yyy.yyy.yyy
snmpv2c notify-community "privatetrap98"

exit
```

where

xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server in a standalone 5620 SAM configuration, or one of the two main servers in a redundant configuration

yyy.yyy.yyy.yyy is the IP address of the other 5620 SAM main server in a redundant 5620 SAM configuration, if present

Procedure 12-2 To commission a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device for 5620 SAM management

See the appropriate device documentation for more information about using the CLI.

Note — An uncommissioned Telco, 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA device is in Privileged, or enable, mode by default. After you configure an enable mode password for the device in step 6 of this procedure, enable mode is not the default. See the appropriate device documentation for more information about enable mode.

1 Open a console window on the device.

2 Enter the following command to enable further device configuration:

```
configure terminal ↵
```

3 Enter the following sequence of commands to set the host name and IP address for the managed device:

hostname *name* ↵

ip address *xxx.xxx.xxx.xxx/M* ↵

where
name is the host name
xxx.xxx.xxx.xxx is the IP address
M is the bit mask

Note — Ensure that each 7250 SAS-ES or 7250 SAS-ESA that is going to use in-band management can ping the network interface IP address configured on the 5620 SAM main server; also ensure that the 5620 SAM main server can ping the system IP address of each 7250 SAS-ES or 7250 SAS-ESA.

4 If you are configuring a 7250 SAS-ES or 7250 SAS-ESA, go to step 5. Otherwise, go to step 6.

5 For the 7250 SAS-ES and 7250 SAS-ESA, which support enhanced functionality such as OSPF and VPLS, you must configure a system interface, lo1, so that the 5620 SAM can discover or manage the devices. Enter the following sequence of commands to configure the lo1 system interface:

interface lo1 ↵

ip address *xxx.xxx.xxx.xxx*/32 ↵

where *xxx.xxx.xxx.xxx* is the IP address

6 Enter the following command to change the switch login password:

password *password password* ↵

where *password* is the new switch login password that is entered twice

7 Enter the following command to set the enable mode password:

enable password *password password* ↵

where *password* is the new enable mode password that is entered twice

8 By default, access ports on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices belong to a default VLAN. The port numbers may differ from those shown in the following examples, depending on which port is designated as the management port. Enter the appropriate sequence of commands to remove the device from the default VLAN.

a For a 7250 SAS, enter the following commands:

```
vlan ↵
config default ↵
remove ports 1/1/2-1/5/4 ↵
exit ↵
exit ↵
```

b For a 7250 SAS-ES or 7250 SAS-ESA,enter the following commands:

```
vlan ↵
config default ↵
remove ports 1/1/2-1/6/2 ↵
exit ↵
exit ↵
```

c For a Telco device, enter the following commands:

```
vlan ↵
config default ↵
remove 1/1/1-1/1/# ↵
exit ↵
exit ↵
```

where # is the number of ports on the card; for example, 24

9 Enter the following command to configure static routes from the device to the 5620 SAM network management domain:

ip route *xxx.xxx.xxx.xxx/M yyy.yyy.yyy.yyy*

where
xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server
M is the 5620 SAM main server subnet mask
yyy.yyy.yyy.yyy is the IP address of the gateway device used to reach the 5620 SAM main server

10 Perform one of the following to configure the required version of SNMP on the device:

a For SNMP v2c:

i Enter the following sequence of commands to configure the SNMP group and users:

```
snmp-server enable ↵

snmp-server view viewALL 1.3 included ↵

snmp-server group v2c_group v2c read viewALL write
viewALL notify viewALL ↵

snmp-server user v2c_user group v2c_group v2c ↵

snmp-server user v2c_usertrapXX group v2c_group v2c ↵
```

where
v2c_user is an SNMP user name; for example private. The name must match the SNMP Community String used by the 5620 SAM node discovery mediation policy.
v2c_group is an SNMP trap group name
v2c_usertrapXX is an SNMP trap user name. The name is comprised of the *v2c_user* name followed by trapXX, where XX is a number from 01 to 98. For example, if the *v2c_user* name is private, the *v2c_usertrapXX* name must be privatetrapXX. The name must match the SNMP trap user name used by the 5620 SAM node discovery mediation policy.

ii Enter the following sequence of commands to configure SNMP trap forwarding to the 5620 SAM:

```
snmp-server target-param Target v2c_usertrapXX v2c ↵

snmp-server target-addr name xxx.xxx.xxx.xxx port# Target
TRAP ↵

snmp-server notify all TRAP ↵
```

where
Target is a name specified for the SNMP target, for example Target_1
v3_usertrapXX is the user name created in step i above
name is the target name, for example sam
xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server
port# is the SNMP trap receiving port on the 5620 SAM main server; for example, the default of 98 for a standalone or primary main server, or 97 for a standby main server

b For SNMPv3:

i Configure an SNMPv3 user and group.

```
snmp-server enable ↵

snmp-server view viewALL 1.3 included ↵

snmp-server group v3_group v3 priv read viewALL write
viewALL notify viewALL ↵

snmp-server user v3_user group v3_group v3 priv privpass
auth md5 authpass↵

snmp-server user v3_usertrapXX group v3_group v3 priv
snmppass auth md5 ↵
```

where
v3_user is the SNMPv3 user name
v3_group is the name of the SNMPv3 trap group
privpass is the DES privacy encryption password
authpass is the MD5 authentication password
v3_usertrapXX is an SNMP trap user name. The name is comprised of the *v3_user* name followed by trapXX, where XX is a number from 01 to 98. For example, if the *v3_user* name is private, the *v3_usertrapXX* name must be privatetrapXX. The name must match the SNMP trap user name used by the 5620 SAM node discovery mediation policy.

ii Configure SNMPv3 trap forwarding to the 5620 SAM:

```
snmp-server target-param Target v3_usertrapXX v3 priv ↵

snmp-server target-addr name xxx.xxx.xxx.xxx port# Target
TRAP ↵

snmp-server notify all TRAP
```

where
Target is the target parameter name, for example Target_1
v3_usertrapXX is the SNMPv3 user name created in i above
name is the target name, for example SAM
xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server
port# is the SNMP trap-receiving port on the 5620 SAM main server

11 Perform one of the following to configure the STP for a device in a VLAN ring topology:

a Enter the following sequence of commands to configure RSTP:

```
protocol ↵

rapid-spanning-tree enable ↵

rapid-spanning-tree priority 4096 ↵
```

b Enter the following sequence of commands to configure MSTP:

```
protocol ↵

mstp enable ↵

mstp 0 priority 4096 ↵
```

Note — When you set the MSTP priority, ensure that the devices closest to the 7450 ESS are set with the lowest priority and use instance 0. This enables the STP on all ports. When ports are used for access as SAPs, STP should be disabled.

12 The 5620 SAM supports enhanced functionality such as MPLS LSPs, FRR, and VPLS on the 7250 SAS-ES and 7250 SAS-ESA.

See Table 12-1 to determine what protocol and interface configuration is supported on the 5620 SAM.

Table 12-1 5620 SAM protocol and interface configuration support for the 7250 SAS-ES and 7250 SAS-ESA

Protocols and Interfaces	Description	7250 SAS-ES 2.0	7250 SAS-ES and 7250 SAS-ESA 3.0
Create and configure L3 interfaces	Create L3 interfaces and configure interface properties	CLI	CLI
Configure LDP	Configure LDP on the NE Enter the LDP targeted peers for the NE	CLI	CLI
Configure OSPF	Configure OSPF on the NE, system interface, L3 interfaces, and specified networks	CLI	CLI
Configure OSPF-TE	Configure OSPF-TE on the NE	Not supported	CLI
Configure RSVP	Configure RSVP on the NE, system interface, and L3 interfaces Enable RSVP-TE extensions	CLI	CLI
Configure MPLS	Configure MPLS on the NE, system interface, and L3 interfaces	CLI	CLI
Create and configure MPLS interfaces	Create and configure MPLS interfaces and administrative groups	CLI for MPLS interfaces Administrative groups are not supported	CLI and 5620 SAM

After the devices are configured, perform the following for SNMP v2c.

- Configure a mediation policy that contains a community string user name that matches the one created using CLI, as described in Procedure 13-4.
- Create a discovery rule that represents the devices, and reference the newly created mediation policy, as described in Procedure 13-5.

After the devices are configured, perform the following for SNMPv3.

- Create SNMPv3 users from the 5620 SAM GUI using the NE user configuration manager. See Procedure 18-6 for more information about NE user configuration. Ensure that the following are configured.
  - Give the user SNMP access by enabling the snmp check box.
  - Enter the same User Name as the user name that was created using CLI; for example, *v3_user*
  - On the SNMPv3 tab, select MD5 as the authentication protocol and DES as the privacy protocol.
  - Type the appropriate plain-text ASCII password used as the MD5 authentication key and DES privacy key; for example, *snmppass*.

- Create a new SNMPv3 mediation policy, as described in Procedure 13-4. Ensure that the following are configured:
  - Security Model is SNMP v3 USM
  - SNMP User Name is the same as the user name created using CLI, which is also the name of the NE user configuration created to use SNMPv3.
- Create a discovery rule that represents the devices, and reference the newly created mediation policy, as described in Procedure 13-5.

Procedure 12-3 To commission an OmniSwitch for 5620 SAM management

See the appropriate OmniSwitch documentation for more information about the CLI command syntax and SNMP.

Note 1 — The 5620 SAM cannot discover an OmniSwitch that is configured with the factory default settings.

Note 2 — You must use a direct console port connection to access an OmniSwitch for the first time. All other management methods such as SNMP, Telnet, FTP, and HTTP, are disabled until you enable them.

1 Open a console window using a direct console port connection to the OmniSwitch.

2 Create a Loopback0 interface and assign an IP address to the interface by entering the following at the prompt:

`ip interface Loopback0 address` ***`xxx.xxx.xxx.xxx`*** ↵

where
xxx.xxx.xxx.xxx is the IP address of the interface

Note 1 — Loopback0 is the name assigned to an IP interface to identify an address that is used for network management purposes. The Loopback0 interface is not bound to any VLAN, therefore it always remains operationally active.

Note 2 — The Loopback0 interface name is case-sensitive. Ensure that you enter the name exactly as shown.

3 Enable SNMP sessions on the switch by entering the following at the prompt:

`aaa authentication snmp local` ↵

4 Enable FTP, Telnet, HTTP, or SSH sessions, if required, by entering the following at the prompt:

`aaa authentication ftp local` ↵

`aaa authentication telnet local` ↵

`aaa authentication http local` ↵

`aaa authentication ssh local` ↵

5 Perform one of the following to configure the required version of SNMP on the switch and the 5620 SAM:

The OmniSwitch default user, admin, does not have SNMP access. Before the 5620 SAM can discover an OmniSwitch, you must create at least one user on the switch with SNMP access.

a For SNMP v2c:

i Configure an SNMP v2 user by entering the following at the prompt:

`user user_name password password no auth` ↵

where
user_name is a username that corresponds to an SNMP v2 user that the 5620 SAM can identify; Alcatel-Lucent recommends that you use the name sam, which is the 5620 SAM default name
password is a password associated with the username; the password is between 8 and 47 characters

Note — If you need to use a different SNMPv2 default user name, use Procedure 5-26 to create an SNMPv2 default user name on the 5620 SAM.

ii Configure SNMP v2 trap forwarding to the 5620 SAM by entering the following at the prompt:

`snmp station xxx.xxx.xxx.xxx v2 user_name` ↵

where
xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server
user_name is the username that you created in step i

Trap forwarding configuration occurs automatically when the 5620 SAM discovers a switch and uses the default SNMP v2 user name sam or the user name configured in Procedure 5-26.

iii Configure an SNMP security level that allows the switch to accept all SNMP queries by entering the following at the prompt:

`snmp security no security` ↵

iv Configure an SNMP v2 community string by entering the following at the prompt:

`snmp community map community_string user user_name` ↵

where
community_string is the name of an SNMP v2 community string that the 5620 SAM can identify
user_name is the SNMP v2 username created in step i

v Create a mediation security policy on the 5620 SAM that uses a community string that matches the string created in step iv. See Procedure 13-4 for information about creating a mediation security policy.

vi Create a discovery rule on the 5620 SAM to discover the switch and reference the policy created in step v. See Procedure 13-5 for information about creating a discovery rule.

b For SNMP v3:

If you need to discover an OmniSwitch using SNMP v3 you must create an SNMP v3 user on the switch that matches an SNMP v3 user defined on the 5620 SAM.

i Configure an SNMP v3 user on the switch by entering the following at the prompt:

user *user_name* password *password* *security_level* ↵

where
user_name is a username that matches an SNMP v3 USM username configured on the 5620 SAM
password is a password associated with the username; the password is between 8 and 47 characters. The password is the plain text ASCII MD5/SHA authentication key and DES privacy key.
security_level is MD5, MD5 + DES, SHA, or SHA + DES

ii Configure SNMP v3 trap forwarding to the 5620 SAM by entering the following at the prompt:

snmp station *xxx.xxx.xxx.xxx* v3 *user_name* ↵

where
xxx.xxx.xxx.xxx is the IP address of the 5620 SAM main server
user_name is the username created in step i

Trap forwarding occurs automatically when the 5620 SAM discovers a node with a username that matches the SNMP v3 USM username specified in the 5620 SAM mediation policy.

iii Configure the SNMP v3 switch security option that you need by entering the following at the prompt:

snmp security *security_option* ↵

where *security_option* is one of the security options described in Table 12-2

Table 12-2 SNMP security options

Option	Description
no security	All SNMP queries are accepted.
authentication set	Includes: • SNPM v1 and v2 Gets • Non-authenticated v3 Gets and Get-Nexts • Authenticated v3 Sets, Gets, and Get-Nexts • Encrypted v3 Sets, Gets, and Get-Nexts

(1 of 2)

Option	Description
authentication all	Includes: • Authenticated v3 Sets, Gets, and Get-Nexts • Encrypted v3 Sets, Gets, and Get-Nexts
privacy set	Includes: • Authenticated v3 Gets and Get-Nexts • Encrypted v3 Sets, Gets, and Get-Nexts
privacy all (default)	Includes: • Encrypted v3 Sets, Gets, and Get-Nexts
traps only	Includes: • All SNMP requests are rejected

(2 of 2)

iv Create an SNMP v3 user on the 5620 SAM using the NE User Configuration manager. See Procedure 18-6 for information about NE user configuration.

- Enable SNMP to give the SNMP v3 user SNMP access.
- Choose a username that matches the name created on the switch in step i.
- Choose the same SNMP v3 authentication protocol, privacy protocol, and password that is configured on the switch.

v Create an SNMP v3 mediation security policy. See Procedure 13-4 for information about configuring a mediation security policy.

- Choose the SNMP v3 (USM) security model option.
- Choose a username that matches the name created on the switch in step i.

vi Create a discovery rule that uses the mediation security policy created in step v. See Procedure 13-5 for information about creating discovery rules.

6 Use a 5620 SAM client to discover the switch and to verify that the switch configuration allows you to manage the switch.

12.5 Generic NE commissioning procedures

The following procedures describe how to configure the 5620 SAM to manage one or more generic NEs.

Procedure 12-4 To prepare a generic NE for 5620 SAM management using a generic NE profile

Perform this procedure to prepare a non-Alcatel-Lucent device for 5620 SAM discovery and management. See chapter 15 for more information about device management.

Note — For light weight generic NE management (9400 AWY, MSS-1c, and MPT-sa), see Procedure 12-5 .

1 Open a console window on the device. See the appropriate device documentation for information about using the device CLI.

2 Perform the following preconfigurations.

i Enable FTP.

ii Enable Telnet.

iii Enable the SNMP engine.

iv Configure at least one SNMPv1, SNMPv2c, or SNMPv3 community.

v Set the SNMP PDU size to 9216.

vi Enable persistent SNMP indexes.

3 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

4 Click on the Create button and choose Create Generic NE Profile. The Generic NE Profile (Create) form opens.

5 Configure the parameters:

- ID
- Auto-Assign ID
- Generic NE Type
- Generic NE Category
- Sys Object ID
- Description
- Default Element Manager URL
- Chassis MAC Object ID
- Default External EMS
- CLI Supported

Note — You cannot modify the Generic NE Type parameter after the generic NE profile is created; you must delete the generic NE profile and create a profile using the new Generic NE Type parameter value.

6 Click on the CLI Profile tab button and configure the parameters:

- Command Prompt
- Max Number Of Sessions
- Telnet Port
- Pre Login Prompt
- Write Login Prompt
- Write Password Prompt
- Read Login Prompt
- Read Password Prompt
- Error Indicator
- Disable Paging Command
- Reset Command
- Login Timeout (seconds)
- Execution Command Timeout (seconds)
- Login Prompt Optional
- Idle Session Warning Message

7 Configure the following parameters if a login confirmation prompt appears:

- Enable Confirm Prompt
- Prompt
- Answer

The Prompt and Answer parameters are configurable when the Enable Confirm Prompt parameter is selected.

8 Configure the following parameters for a second level of login security, if required:

- Enable Second Login
- Enable Login Command
- Enable Login Prompt

The Enable Login Command and Enable Login Prompt parameters are configurable when the Enable Second Login parameter is selected.

9 Click on the Interface Types tab button to configure an interface for the generic NE.

10 Click on the Add button. The Select Generic NE Interface Type form opens.

11 Configure the filter criteria and click on the Search button. The form displays a list of interface types.

12 Select one or more interface types in the list and click on the OK button. The Select Generic NE Interface Type form closes and the selected interface types are listed on the Generic NE Profile (Create) form.

13 Click on the Routing MIBs tab button. The Generic NE Profile form is displayed.

Note — The Routing MIBs tab button is dimmed if you do not have a valid 5650 CPAM license that has a third-party router quantity greater than zero. See the *5650 CPAM User Guide* for information about 5650 CPAM licenses.

14 Click on the Add button. The Select Generic NE Routing MIB window is displayed.

15 Click on the Search button. A list of the supported Routing MIBs is displayed.

16 Select one or more of the Routing MIBs in the list and click on the OK button. The Select Generic NE Routing MIB window closes. The Generic NE Profile form is displayed.

Note — You must not configure the Routing MIBS and apply the configuration to the Generic NE profile before you configure the interface types. See steps 9 to 12. If you configure the Routing MIBs in the wrong order, you must perform a full node resync and specify the 'ignore time stamp' instruction.

17 Click on the OK button. The Generic NE Profile form reappears with the new generic NE profile.

18 Click on the Apply button.

Note — After you have discovered the NE using the generic NE profile in 5620 SAM, you can use the Routing tree to navigate to and view the discovered routing objects.

19 Click on the Trap Configuration tab button.

Caution — The 5620 SAM assumes that the trap log name on a generic NE is the same as the trap log name on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, and 7750 SR. Some generic NEs may not support the use of a trap log name that matches the name used by the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, and 7750 SR. If this is the case for a generic NE that you need to manage using the 5620 SAM, you may not be able to use the Trap Restoration Logs on the generic NE.

20 Configure the parameters:

- Supports Trap Sequence Number
- Supports Trap Restoration Logs
- Maximum Trap Gap
- Full Node Resync on Max Trap Gap
- Minimum Time Interval Between Full Node Resyncs (seconds)

Caution — The 5620 SAM supports trap sequencing only for devices that increment the trap ID value by 1. Do not enable the Supports Trap Sequence Number parameter if the generic NE increments the trap ID value by anything other than 1.

21 Click on the Select button beside the Script ID parameter in the Trap Configuration Script panel. The Select Script - Generic NE Profile form opens.

The script chosen in this step enables trap forwarding to the 5620 SAM. The 5620 SAM runs this script on the generic NE when it tries to manage the generic NE.

Note 1 — A 5620 SAM CLI script to configure the GNE trap destination must already exist before you can select it for use in the generic NE profile. See the *5620 SAM Scripts and Templates Developer Guide* for information on creating CLI scripts.

Note 2 — If the 5620 SAM system is a redundant deployment, ensure that both 5620 SAM main servers are specified in the trap configuration script as SNMP trap destinations to be added.

22 Select a script in the list and click on the OK button. The Select Script - Generic NE Profile form closes and the script identification is displayed on the Generic NE Profile (Edit) form.

23 Click on the Select button beside the Script ID parameter in the Trap De-Configuration Script panel. The Select Script - Generic NE Profile form opens.

The script chosen in this step disables trap forwarding to the 5620 SAM. The 5620 SAM runs this script on the generic NE when it tries to unmanage the generic NE.

Note — If the 5620 SAM system is a redundant deployment, ensure that both 5620 SAM main servers are specified in the trap de-configuration script as SNMP trap destinations to be removed.

24 Select a script in the list and click on the OK button. The Select Script - Generic NE Profile form closes and the script identification is displayed on the Generic NE Profile (Edit) form.

25 Click on the Select button beside the Catalogue Name parameter in the Alarm Catalogue panel. The Select Alarm Catalogue - Generic NE Profile form opens.

26 Select an alarm catalogue in the list and click on the OK button. The Select Alarm Catalogue - Generic NE Profile form closes and the catalogue name is displayed on the Generic NE Profile (Edit) form.

27 Click on the OK button. A dialog box appears.

28 Click on the Yes button. The Generic NE Profile (Edit) form closes.

29 Close the Generic NE Manager form.

Procedure 12-5 To prepare a light weight (9400 AWY, MSS-1c, and MPT-sa) generic NE for 5620 SAM management using a generic NE profile

Perform this procedure to prepare a light weight (9400 AWY, MSS-1c, and MPT-sa) device for 5620 SAM discovery and management. See chapter 15 for more information about device management.

1 Ensure that the SystemGneProfilesNames= flag is set to “AWY”, “MSS1c” or “MPTSA” in the nms-server.xml file for light weight generic NE management of 9400 AWY, MSS-1c, or MPT-sa.

Note 1 — The SAM IP must be registered with any NEs that are to be managed as light weight generic NEs.

Note 2 — To create the profile of light weight managed NEs, the user does not have to enter any parameters such as SysObject ID . To include an NE type, the config file "read" option can be used. After completion, the respective profile will appear as the default profile in the 5620 SAM.

i Go to directory /opt/5620sam/server/nms/config

ii Open the nms-server.xml file.

iii Go to the line systemGNEProfile=“ ”

iv Edit as systemGNEProfile=“MPTSA” or systemGNEProfile=“MSS1c” or systemGNEProfile=“9400AWY” or systemGNEProfile=“MPTSA, MSS1c, 9400AWY”

v Save and exit the file.

vi Go to path /opt/5620sam/server/nms/bin

vii Execute the following command: ./nmsserver.bash read_config

viii Manage the NEs with SNMP v2 community string as “SNMP-trap” for trap access mediation policy, and keep the default setting for read-write access policy.

ix Observe that a new group has been created in the Equipment Network tree and that all related generic NEs are located under this group.

2 Auto-populate the alarms catalogue.

i Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

ii Choose Generic NE Profile (Generic NE) in the object drop-down list and click on the Search button. A list of generic NE profiles is displayed.

iii Select the created generic NE profile in the list and click on the Properties button. The Generic NE Profile (Edit) form opens with the General tab displayed.

iv Click on “Populate Alarm Catalogue”. The respective Alarm catalogue is created.

v Click on the Trap Configuration tab button. Attach the Alarm catalogue to the respective profile.

vi Click on the Interface tab button. Add each of the respective interfaces or all interfaces to get the traps. All alarms should now be visible in your 5620 SAM client.

3 Cross launch the NEtO for a generic NE.

Note — To cross launch a 9400 AWY NE, keep the NEtO software directory in your 5620 SAM client and remove any space in the NEtO directory description. The description format must be: C:\9500SAM\8.0\NEtOETSI\multiversion2.1\NEtO_MultiVersion\NEtO

i Specify the directory name in the External EMS field under GNE properties for GNE cross launch.

ii Right-click on the GNE and choose External Element Manager from the contextual menu. Observe that NEtO is launched.

Procedure 12-6 To cross launch the 9400 AWY, MPT-sa, or MSS-1c J-USM manager

Perform this procedure to enable the cross launch of a Java-based EMS/craft terminal.

1 Perform Procedure 12-4 to discover the 9400 AWY, MPT-sa, or MSS-1c GNE.

2 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

3 Right-click on the 9400 AWY, MPT-sa, or MSS-1c GNE in the Equipment view and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

4 Configure the External EMS parameter.

5 Click on the Launch External EMS button to launch the Java based J-USM manager.

Note — The profile value of the External EMS parameter (if specified) is passed to the J-USM manager.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 12-7 To modify a generic NE profile

Perform this procedure to change the parameters in an existing generic NE profile.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Profile (Generic NE) in the object drop-down list and click on the Search button. A list of generic NE profiles is displayed.

3 Select a generic NE profile in the list and click on the Properties button. The Generic NE Profile (Edit) form opens with the General tab displayed.

The following tabs contain configurable parameters:

- General—contains parameters that identify the generic NE type
- CLI Profile—contains parameters that define the console window prompts and commands
- Trap Configuration—contains parameters that define the SNMP trap management configuration
- Interface Types—allows the association of multiple types of interfaces with the generic NE profile. A generic NE interface is selectable as the endpoint of a 5620 SAM physical link.

4 Modify the parameters for the generic NE profile, as required.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Generic NE Profile (Edit) form closes.

7 Close the Generic NE Manager form.

8 If you modify the list of interfaces on the Interface Types tab, perform the following steps.

Caution — If you modify the list of interfaces on the Interface Types tab, you must resynchronize the entire generic NE without comparing timestamps to ensure that the 5620 SAM database is correctly updated with the new interface information.

i Right-click on the generic NE in the 5620 SAM topology map and choose Resync from the contextual menu. The Resync Site(s) form opens with the Resync Options panel displayed.

ii Click on the Next button. The Force Resync panel is displayed.

iii Select the Ignore Timestamps parameter.

iv Click on the Finish button. The 5620 SAM resynchronizes the generic NE.

v Close the Resync Site(s) form.

Procedure 12-8 To delete a generic NE profile

Note 1 — You cannot delete a generic NE profile that is associated with a managed generic NE. You must unmanage the generic NEs associated with a generic NE profile before you can delete the profile.

Note 2 — You cannot delete a generic NE profile when a generic NE associated with the profile is a target of a CLI script. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

1 Unmanage and delete the generic NEs that are managed using the generic NE profile. See chapter 13 for more information.

2 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

3 Choose Generic NE Profile (Generic NE) in the object drop-down list and click on the Search button. A list of generic NE profiles is displayed.

4 Select a profile in the list and click on the Delete button. A dialog box appears.

5 Click on the Yes button. The 5620 SAM deletes the generic NE profile.

6 Close the Generic NE Manager form.

12.6 Device management procedures

The following procedures describe how to configure device management.

Procedure 12-9 To configure polling policies

Perform this procedure to configure the 5620 SAM to use in-band, out-of-band, or in-band and out-of-band polling at the intervals specified in a mediation policy. See chapter 13 for information about configuring mediation policies.

1 Choose Equipment or Routing from the drop-down menu on the navigation tree.

2 Open the Network icon. The managed devices are displayed.

3 Click on an icon that represents a managed device.

4 Right-click and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

5 Record the system IP address and the management IP address. Configure the Location and OLC State parameters, if required.

6 Click on the Polling tab button and perform one of the following:

a Configure the following parameters on the General tab if you are configuring a 7750 SR, 7450 ESS, 7710 SR or 7705 SAR:

i Specify whether scheduled polling is enabled or disabled using the Scheduled Polling parameter. Scheduled polling is configured using the Mediation configuration form. See Procedure 13-4 for more information.

ii Configure the Redundant Synchronization Mode parameter.

iii Verify that the Persistent SNMP Indices parameter is set to true to ensure persistent SNMP indices are used.

iv Configure the parameters:

- Primary DNS
- Secondary DNS
- Tertiary DNS
- DNS Domain
- Separate LI Administration
- LI Local Save Allowed

Note 1 — To configure LI parameters, you need LI privileges.

Note 2 — To view LI configuration information, you need LI privileges. Right-click on a discovered device in the navigation tree and choose Properties from the contextual menu, and click on the LI Configuration Status tab button.

v View the read-only parameters to determine the current polling status:

- Resync Status indicates whether the last polling interval was successfully completed.
- Last Resync Start Time and Last Resync End Time indicate the start and finish of the last polling interval.

vi Click on the Management tab button.

vii On the In Band panel, configure the parameters for an L3 management interface, if required:

- L3 Management Interface
- Enable L3 Management Interface

viii On the Management Preference panel, configure the following parameters:

- Active Management IP
- Auto Revert to Preferred
- Management IP Selection

Note — The Auto Revert to Preferred parameter is configurable when the Management IP Selection parameter is set to Out Of Band Preferred or In Band Preferred.

ix On the Notifications Preferred panel, configure the following parameters:

- Primary Route Preference
- Secondary Route Preference

x Go to step 7.

b If you are configuring a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA perform the following:

i Specify whether scheduled polling is enabled or disabled using the Scheduled Polling parameter. Scheduled polling is configured using the Mediation configuration form. See Procedure 13-4 for more information.

ii View the read-only parameters to determine the current polling status:

- Resync Status indicates whether the last polling interval was successfully completed.
- Last Resync Start Time and Last Resync End Time indicate the start and finish of the last polling interval.

iii Go to step 7.

c Configure the following parameters on the General tab if you are configuring a 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], or 7210 SAS-X24F2XFP:

i Specify whether scheduled polling is enabled or disabled using the Scheduled Polling parameter. Scheduled polling is configured using the Mediation configuration form. See Procedure 13-4 for more information.

ii Verify that the Persistent SNMP Indices parameter is set to true to ensure that persistent SNMP indices are used.

iii Configure the parameters in the Bof Configuration panel, if required:

- Primary DNS
- Secondary DNS
- Tertiary DNS
- DNS Domain

iv View the read-only parameters to determine the current polling status:

- Resync Status indicates whether the last polling interval was successfully completed.
- Last Resync Start Time and Last Resync End Time indicate the start and finish of the last polling interval.

v Click on the Management tab button.

vi On the In Band panel, configure the parameters:

- L3 Management Interface
- Enable L3 Management Interface

vii On the Management Preference panel, configure the parameters:

- Active Management IP
- Auto Revert to Preferred
- Management IP Selection

Note 1 — The Active Management IP, Auto Revert to Preferred, and Management IP Selection parameters are only configurable on the 7210 SAS-E Release 2.0 R2 or later, and the 7210 SAS-M Release 2.0 R2 or later.

Note 2 — The Auto Revert to Preferred parameter is configurable when the Management IP Selection parameter is set to Out Of Band Preferred or In Band Preferred.

viii On the Notifications Preferred panel, configure the following parameters:

- Primary Route Preference
- Secondary Route Preference

ix You can configure two uplinks in the BOF for port redundancy. If the image path and configuration file path are local, you do not need to configure the IP address and routing information for uplink A and uplink B. You can optionally obtain IP parameters using DHCP when you configure a value of 0 for the uplink port IP address. The DHCP server should be configured to provide the IP address and the default gateway information that is used to reach the server where the image and configuration files are stored.

x Click on the 7210 BOF tab button and on the Select button in the Uplink A panel to choose an uplink port. The Select Port - Uplink Bof Configuration search form opens.

xi Choose a port from the list and click on the OK button. The Select Port - Uplink Bof Configuration search form closes and the port name appears in the Uplink A panel.

xii Configure the following parameters in the Uplink A panel:

- IP Address
- Mask
- VLAN ID

xiii Click on the Select button in the Uplink B panel to choose an uplink port. The Select Port - Uplink Bof Configuration search form opens.

xiv Choose a port from the list and click on the OK button. The Select Port - Uplink Bof Configuration search form closes and the port name appears in the Uplink B panel.

xv Configure the following parameters in the Uplink B panel:

- IP Address
- Mask
- VLAN ID

xvi Click on the Uplink Routes tab button and on the Add button. The Uplink Route Configuration (Create) form opens.

xvii Configure the following parameters:

- Uplink
- Route Destination
- Mask
- Next Hop

xviii Click on the Apply button if you need to add more than one uplink route or the OK button if you only need to add one route. A dialog box appears.

xix Click on OK to save your configuration.

xx Repeat steps xvii to xix to add another uplink route. You can add up to ten routes for each uplink.

d Configure the Scheduled Polling parameter if you are configuring a 9500 MPR. Scheduled polling is configured using the Mediation configuration form. See Procedure 13-4 for more information.

View the read-only parameters to determine the current polling status:

- Resync Status indicates whether the last polling interval was successfully completed.
- Last Resync Start Time and Last Resync End Time indicate the start and finish of the last polling interval.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button to confirm the action. The Network Element (Edit) form closes.

Procedure 12-10 To edit polling policy settings for multiple managed devices

You can use the list of managed devices from the Discovery Manager Resync Status tab to modify polling settings for a device or devices; for example, when you want to enable or disable polling on numerous managed devices.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens.

2 Click on the Resync Status tab button.

3 Select a device or devices from the list.

4 Click on the Properties button. When you choose multiple devices, the Network Element (Multiple Instances) (Edit) form opens.

You can only configure those parameters that are common to all devices selected from the list.

5 Click on the Polling tab button.

6 Enable or disable polling using the Scheduled Polling parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button to confirm the action. The Network Element (Edit) form closes.

Procedure 12-11 To enable 5620 SAM management of a 9500 MPR

Perform this procedure to enable the 5620 SAM to manage the 9500 MPR and to allow NEtO sessions to be opened using the 5620 SAM GUI.

Note 1 — The 5620 SAM can manage a 9500 MPR using the dedicated TMN port or port 4 on the core card. If you use port 4 on the core card, the card status must be TMN.

Note 2 — The local IP address must match the TMN interface address. You can use NEtO to configure the required IP addresses.

You must first install the NEtO software on a 5620 SAM client station and modify the client configuration. See the 9500 MPR user documentation for more information about how to install and use the NEtO software. See Procedure 17-53 for information about how to start NEtO from the 5620 SAM GUI.

Note 1 — The 5620 SAM server and NEtO cannot be run on the same machine. The 5620 SAM Client and NEtO (not the 5620 SAM Server) must be on the same machine.

Note 2 — Before attempting to run an x-launch from the 5620 SAM, it is advisable to check whether NEtO can be opened on a standalone basis from the 5620 SAM client machine. To perform this check, go to the NEtO install directory and execute NEtO.exe, ensuring that the craft terminal launches.

1 Log in to a 5620 SAM client station.

2 Perform Procedure 13-5 to create a discovery rule for the device.

3 Discover a 9500 MPR NE and verify that the 5620 SAM can manage the device.

Warning — As the 9500 MPR NE has a default local IP address of 10.0.1.2, in order to ensure the NE is discovered by the 5620 SAM, the operator must reconfigure the IP address so that it is unique.

Note — Upon discovery of a 9500 MPR NE, 5620 SAM will auto-create and auto-assign a trap access policy using the "SNMP-trap" community string.

4 Open one of the following files using a plain-text editor.

- on a Windows client:
  Navigate to the path *install_dir*\nms\thirdparty\config and open the file named Alcatel-MPR-9500_1.1.0 in Wordpad or Notepad, where *install_dir* is the client installation location, typically C:\5620sam\client.
- on a Solaris client:
  Navigate to the path *install_dir*/nms/thirdparty/config/ and open the file named Alcatel-MPR-9500_1.1.0, where *install_dir* is the client installation location, typically /opt/5620sam/client.

5 Edit the NEtO directory path in the variable *install_dir =${path}*

- For example for a Windows client, the paths could be:
- *install_dir=D:\\NEtO*
- *install_dir=C://9500MPR//MPRE_CT_V01.22.01*, or
- *install_dir=D:\\NM\\SAM\\NEtO_Multiversion\\NEtO*

- For example for a Solaris client, the path could be *install_dir=/tmp/neto*.

6 Save and close the file.

7 Select the equipment view of the navigation tree on the 5620 SAM GUI. Right-click on a 9500 MPR NE, and select External Element Manager from the menu.

8 Verify that the NEtO software launches.

Procedure 12-12 To create a generic NE alarm catalogue

Perform this procedure to create an alarm catalogue for use with a generic NE profile.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Click on the Create button and choose Create Generic NE Alarm Catalogue. The Generic NE Alarm Catalogue (Create) form opens.

3 Configure the parameters:

- Catalogue Name
- Description
- Version

4 Perform the following steps to create a transform function for the catalogue, if required.

i Click on the Transform Functions tab button.

ii Click on the Create button. The Generic NE Alarm Transform Function (Create) form opens.

iii Configure the parameters:

- Transform Function Name
- Out Value Type
- Specify Default Out Value

iv If you enable the Specify Default Out Value parameter, click on the Select button beside the Default Out Value parameter. The Select Property form opens. Otherwise, go to step vi.

v Select a value in the list and click on the OK button. The Select Property form closes, and the value is displayed on the Generic NE Alarm Transform Function (Create) form.

vi Click on the Pairs tab button.

vii Click on the Add button. The Pair (Create) form opens.

viii Configure the In Value parameter.

ix Click on the Select button beside the Out Value parameter. The Select Property form opens.

x Select a value in the list and click on the OK button. The value is displayed on the Pair (Create) form.

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The Pair (Create) form closes, and the value pair is listed on the Generic NE Alarm Transform Function (Create) form.

xiii Repeat steps 4 vii to xii to add another value pair, if required.

xiv Click on the OK button. A dialog box appears.

xv Click on the OK button. The Generic NE Alarm Transform Function (Create) form closes, and the transform function is listed on the Generic NE Alarm Catalogue (Edit) form.

xvi Repeat steps 4 ii to xv to create another transform function, if required.

xvii Click on the Apply button. A dialog box appears.

xviii Click on the OK button.

5 Click on the Mappings tab button.

6 Click on the Create button to create a raising alarm mapping. The Generic NE Alarm Mapping (Create) form opens.

7 Configure the following parameters:

- Trap OID
- Trap Name
- Administrative State
- FDN Extension
- Additional Text
- Use Default Additional Text

8 Perform one of the following using the parameters in the Alarm Name panel.

a Specify a static alarm name by configuring the Alarm Name parameter.

b Specify a dynamic alarm name. Perform the following steps.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

9 Perform one of the following using the parameters in the Probable Cause panel.

a Specify a static probable cause. Perform the following steps.

i Click on the Select button beside the Probable Cause parameter. The Select Property form opens with a list of probable causes displayed.

ii Select a probable cause in the list and click on the OK button. The probable cause is displayed on the Generic NE Alarm Mapping (Create) form.

b Specify a dynamic probable cause. Perform the following steps.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

10 Perform one of the following using the parameters in the Severity panel.

a Specify a static severity by configuring the Severity parameter.

b Specify a dynamic severity. Perform the following steps.

Note — When you specify the use of a transform function for the alarm severity, the Mapping Type changes to Raising/Clearing. You cannot create a clearing mapping for this type of mapping; you must use a transform function to clear an alarm when the alarm severity is defined using a transform function.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The Generic NE Alarm Mapping (Create) form closes, and the new alarm mapping is listed on the Generic NE Alarm Catalogue (Create) form.

13 Repeat steps 6 to 12 to create an additional raising alarm mapping, if required.

14 If you do not need to create a clearing alarm mapping, go to step 24.

15 To create a clearing alarm mapping, select a raising alarm mapping in the list and click on the Create Clearing button. The Generic NE Alarm Mapping (Create) form opens.

Note 1 — A raising alarm mapping is indicated by the word Raising in the Mapping Type list column.

Note 2 — You can create a clearing alarm mapping only when the corresponding raising alarm is in the same alarm catalogue.

Note 3 — You can associate a clearing alarm mapping with only one raising alarm mapping.

Note 4 — You cannot create a clearing mapping for a mapping that uses a transform function to define the alarm severity; you must use a transform function to clear an alarm when the alarm severity is defined using a transform function.

16 Configure the parameters:

- Trap OID
- Trap Name
- Administrative State
- FDN Extension
- Additional Text
- Use Default Additional Text

Note 1 — A static clearing alarm mapping inherits the following values from the associated raising alarm:

- Alarm Name
  This value must match the raising alarm value.
- Probable Cause
  This value must match the raising alarm value.
- FDN Extension
  The resulting text string must match the text string generated by the raising mapping.
- Additional Text
  The resulting text string must match the text string generated by the raising mapping.

See Procedure 12-14 for information about modifying the Alarm Name or Probable Cause value.

Note 2 — The explicit FDN Extension and Additional Text values can differ from the values in the raising mapping, but the generated text strings must match. For example, if the object name is in varbind 2 of the raising trap and in varbind 3 of the clearing trap, the parameter values name different varbinds but the script output is identical.

Note 3 — The alarm severity in a clearing alarm mapping is set to Cleared and cannot be changed.

17 Perform the following steps to specify a dynamic alarm name, if required, using the parameters in the Alarm Name panel.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

18 Perform the following steps to specify a dynamic probable cause, if required, using the parameters in the Probable Cause panel.

i Select the Specify Transform Function parameter.

ii Click on the Select button beside the Varbind Transform Function parameter. The Select Transform Function form opens.

iii Select a transform function in the list and click on the OK button. The Select Transform Function form closes, and the transform function name is displayed on the Generic NE Alarm Mapping (Create) form.

iv Configure the Varbind Position parameter.

19 Click on the OK button. A dialog box appears.

20 Click on the OK button. The Generic NE Alarm Mapping (Create) form closes, and the new alarm mapping is listed on the Generic NE Alarm Catalogue (Create) form.

21 Repeat steps 15 to 20 to create and additional clearing alarm mapping, if required.

22 Click on the OK button. A dialog box appears.

23 Click on the OK button. The Generic NE Alarm Mapping (Edit) form closes.

24 Click on the OK button. A dialog box appears.

25 Click on the Yes button. The Generic NE Alarm Catalogue (Edit) form closes.

26 Close the Generic NE Manager form.

Procedure 12-13 To add an alarm mapping to a generic NE alarm catalogue

Note — A modification to a generic NE alarm catalogue takes effect when you commit the change.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Alarm Catalogue (Trap to Alarm Mapper) in the object drop-down list and click on the Search button. A list of generic NE alarm catalogues is displayed.

3 Select an alarm catalogue in the list and click on the Properties button. The Generic NE Alarm Catalogue (Edit) form opens with the General tab displayed.

4 Configure the Description and Version parameters, if required.

5 Perform steps 4 to 26 in Procedure 12-12.

Procedure 12-14 To modify or delete a generic NE alarm mapping

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Alarm Catalogue (Trap to Alarm Mapper) in the object drop-down list and click on the Search button. A list of generic NE alarm catalogues is displayed.

3 Select an alarm catalogue in the list and click on the Properties button. The Generic NE Alarm Catalogue (Edit) form opens with the General tab displayed.

4 Click on the Mappings tab button.

5 Perform one of the following.

a Modify the mapping. Perform the following steps.

Note — A modification to a generic NE alarm mapping takes effect immediately after you commit the change.

i Select a mapping in the list and click on the Properties button.The Generic NE Alarm Mapping (Edit) form opens.

Note — To change the Alarm Name value in a raising alarm mapping and in the associated clearing alarm mapping, you must do one of the following:

- Configure the parameter in each mapping simultaneously by selecting both mappings before you click on the Properties button.
- Configure the parameter in one mapping at a time and commit the changes to the catalogue only after both mappings are modified.

ii Configure the following parameters:

- Trap Name
- Administrative State
- Alarm Name
- Severity
- FDN Extension
- Additional Text
- Use Default Additional Text

iii Click on the Select button beside the Probable Cause parameter. The Select Property - Generic NE Alarm Mapping form opens with a list of probable causes displayed.

iv Select a probable cause in the list and click on the OK button. The probable cause is displayed on the Generic NE Alarm Mapping form.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Generic NE Alarm Mapping (Create) form closes.

b Delete the mapping. Perform the following steps.

Note — When you delete a generic NE raising alarm mapping, the associated clearing mapping is also deleted.

i Select a mapping in the list and click on the Delete button. A dialog box appears.

ii Click on the OK button. The 5620 SAM deletes the generic NE alarm mapping.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Generic NE Alarm Catalogue (Edit) form closes, and the Generic NE Manager form reappears.

8 Close the Generic NE Manager form.

Procedure 12-15 To delete a generic NE alarm catalogue

Note 1 — You cannot delete an alarm catalogue that is associated with a generic NE profile. You must remove the alarm catalogue from each associated generic NE profile before you can delete the catalogue.

Note 2 — When you delete a generic NE alarm catalogue, you delete the alarm mappings that the catalogue contains.

1 Choose Administration→Generic NE Manager from the 5620 SAM main menu. The Generic NE Manager form opens.

2 Choose Generic NE Alarm Catalogue (Trap to Alarm Mapper) in the object drop-down list and click on the Search button. A list of generic NE alarm catalogues is displayed.

3 Select an alarm catalogue in the list and click on the Properties button. The Generic NE Alarm Catalogue (Edit) form opens with the General tab displayed.

4 Click on the Generic NE Profiles tab button. The tab lists the generic NE profiles to which the alarm catalogue is assigned.

5 If no profiles are listed, go to step 8.

6 Perform the following steps to remove a profile association.

i Select a profile in the list and click on the Properties button. The Generic NE Profile (Edit) form opens with the General tab displayed.

ii Click on the Trap Configuration tab button.

iii Click on the Clear button in the Alarm Catalogue panel. The Catalogue Name value is removed from the form.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button. The Generic NE Profile (Edit) form closes, and the Generic NE Alarm Catalogue (Edit) form reappears.

7 Repeat step 6 for each listed profile.

8 Close the Generic NE Alarm Catalogue (Edit) form. The Generic NE Manager form reappears.

9 Select the alarm catalogue in the list and click on the Delete button. A dialog box appears.

10 Click on the Yes button. The 5620 SAM deletes the generic NE alarm catalogue.

11 Close the Generic NE Manager form.

13 — Device discovery

13.1 Device discovery overview

The 5620 SAM simplifies network provisioning by discovering NEs and reconciling their properties with the contents of the 5620 SAM database.

The 5620 SAM discovers NEs using SNMP. During the discovery process, the 5620 SAM scans the network for devices according to user-specified IP addresses or IP address ranges. When the IP address used to discover a device is the system IP address, also called the system ID, management is considered in-band. When the IP address used to discover the device is the management IP address of the device management port, management is considered out-of-band. See chapter 12 for more information about in-band and out-of-band management.

After the 5620 SAM discovers a device, it sets the device state to Managed and adds the device properties to the 5620 SAM database. To discover one or more devices, you use the 5620 SAM Discovery Manager to create discovery rules and scan the network as specified by the rules.

Discovery rules contain rule elements that specify which devices or subnets are to be included in or excluded from the discovery process. A discovery rule can contain multiple rule elements. For example, you can configure one rule element to discover a subnet and another to exclude specific IP addresses from the subnet.

Note — The 5620 SAM does not attempt to discover tests or test suites that are configured locally on an NE, for example, using a CLI.

SNMP management

Simple Network Management Protocol, or SNMP, is an application-layer protocol that provides a message format to facilitate communication between SNMP managers and agents. SNMP provides a standard framework for NE monitoring and management from a central location.

An SNMP manager controls and monitors the activities of network hosts that use SNMP. An SNMP manager uses a get operation to obtain a value from an SNMP agent, and uses a set operation to store a value in the agent. The manager uses definitions from a management information base, or MIB, to perform operations on the managed device, for example, retrieving data values, replying to requests, and processing SNMP notifications called traps.

SNMPv1 and SNMPv2c provide no security, authentication, or encryption. Without authentication, an unauthorized user is able to perform SNMP network management functions and eavesdrop on management information as it passes from one system to another.

SNMPv3 requires that an authentication and encryption method such as SSH is assigned to each user for validation by the NE. SNMPv3 authentication and encryption enable an NE to validate the system that issues an SNMP message and to determine whether another system has tampered with the message.

For information about device-specific SNMP support, see the SNMP chapter of the appropriate *System Management Guide* for the device. For information about SSH security, see section 13.3.

IPv6 discovery

The 5620 SAM supports the discovery of devices that use IPv6 in-band or out-of-band management IP addresses. In order for the 5620 SAM to discover and manage a device that uses IPv6, the device must have an IPv6 address on the management port, system interface, or both. The 5620 SAM main server must also be given an IPv6 address during installation.

Note — To manage 7750 SR, 7710 SR, or 7450 ESS devices using IPv6, the device must also be configured with an IPv4 address on the management port for out-of-band management, or an IPv4 address on the system interface for in-band management.

The IP version that the 5620 SAM uses to discover a device is specified in each discovery rule. If the 5620 SAM discovers both IPv4 and IPv6 addresses on the system interface of a device, it discovers the device using the address that corresponds to the IP version specified in the discovery rule.

Discovery and SNMP packet size

Each 5620 SAM-managed device must be configured to send SNMP packets of up to 9216 bytes in size. You must ensure that each device between the managed devices and the 5620 SAM can handle an MTU size of 9216 bytes, or is configured to forward fragmented SNMP packets.

Consider the following:

- When an intermediate network device receives SNMP traffic, it must be able to process packets of up to 9216 bytes in size. If this exceeds the MTU size of the intermediate device, and the device cannot forward fragmented packets, the packets may be dropped and device discovery may fail.
- Verify that large packets can travel from the managed devices to the 5620 SAM by using CLI to ping the IP address of the 5620 SAM main server using a large packet. See the *5620 SAM Troubleshooting Guide* server troubleshooting chapter for more information about using traceroute and ping to verify packet transport.

Unmanaging or deleting devices

Using the 5620 SAM to unmanage a device excludes the device from the managed network, but a reference to the device remains in the 5620 SAM discovery system. The unmanage function may be used for unusual conditions such as when the 5620 SAM requires a complete refresh of NE data because of data corruption. Unmanaging a device results in a loss of management data for the selected device, which includes, but is not limited to, the following:

- object names and descriptions
- statistics
- alarms
- physical links
- policies
- script results
- scheduled activities
- NE backups

Deleting a device results in the complete loss of management data for the device and completely removes the device from the managed network.

Caution — If you use the 5670 RAM to process 5620 SAM statistics, unmanaging or deleting an NE results in the loss of all historical 5670 RAM AA statistics for the device.

13.2 Mediation and SNMP MIBs

A 5620 SAM mediation policy defines the interval at which the 5620 SAM polls NEs for SNMP MIB configuration changes. You can use the Mediation and MIB Entry Policy forms to view the information in an SNMP MIB. See Procedure 13-4 for more information.

You can use the 5620 SAM client GUI to list the contents of the device MIBs that the current 5620 SAM system supports. The list includes the following information:

- the MIB name
- the MIB version; the 5620 SAM software may support multiple MIB versions
- the OID of a MIB entry
- the MIB entry name
- the 5620 SAM polling interval for a MIB or MIB entry

See Procedure 13-20 for information about listing and saving SNMP MIB information.

13.3 SSH security

SSH is a protocol that provides secure file transfer and file system access between the 5620 SAM, and managed NEs. SSH version 2, or SSH2, is enabled by default on the following device types:

- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7250 SAS
- 7250 SAS-ES
- 7250 SAS-ESA
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR

SSH2 supports the use of public/private encryption-key pairs to perform authentication based on public key cryptography. A public/private key pair is generated on an NE. The private key is stored locally on the NE, and the public key is specific to SSH2 clients and persists in the 5620 SAM for future communication with the SSH2 server on the NE. The public key is used to verify that the client is connecting to the correct SSH2 server.

An SSH2 server identifies itself to a client by sending a message that is signed with the private key of the server. The 5620 SAM uses the public key of the SSH2 server to authenticate the identity of the server.

SSH2 host key management

An NE sends an SSH2 host key on the first attempt of the 5620 SAM to make an SSH2 connection. The 5620 SAM automatically accepts the public key fingerprint and stores it locally. After the first connection, the local copy of the fingerprint is used for server authentication during subsequent sessions.

If a different host key is sent by the same NE in a subsequent session, the connection is rejected and the 5620 SAM raises an alarm. If the user verifies that the host key of the SSH2 NE has been changed in a legitimate manner, for example, when the SSH server is rebooted and host key persistence is not configured, the user can manually accept the key by removing the mismatched host key entry from the SSH2 known host manager of the 5620 SAM. This removes the SSH2 fingerprint from the 5620 SAM database. Connections are then accepted from the NE until the SSH server is again rebooted.

Note — By default, SSH host keys do not persist in the 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X24F2XFP, 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR.

Host keys always persist in the 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA.

Alcatel-Lucent recommends that you configure the host key persistence on an SSH2 NE to retain the public key fingerprint across reboots. If public key persistence is not enabled, a 5620 SAM operator must manually accept a new key and remove an alarm each time a connection attempt is made after the NE reboots.

SSH2 and NE CLI sessions

When SSH2 for CLI sessions is enabled in the mediation policy of an SSH2-capable device, SSH2 instead of Telnet is used for each CLI session. The following devices support SSH2 CLI sessions:

- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7250 SAS
- 7250 SAS-ES
- 7250 SAS-ESA
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR
- generic NE

SSH1 is used only in SSH CLI sessions on NEs that do not support SSH2.

SSH2 and script management

When SSH2 for CLI sessions is enabled in the mediation policy of an SSH2-capable device, SSH2 is used instead of Telnet for each script execution session. The following devices support the use of SSH2 for management using the 5620 SAM Script Manager:

- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7250 SAS
- 7250 SAS-ES
- 7250 SAS-ESA
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR
- generic NE

SSH1 is used only in SSH CLI sessions on NEs that do not support SSH2.

SSH2 and secure file transfers

When secure file transfers are specified in the mediation policy of an SSH2-capable device, SCP is used instead of FTP for backups, restores, software upgrades, and statistics collection. The following devices support the use of SSH2 for secure file transfers:

- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR

SSH and device management

The 5620 SAM supports the management of 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA devices using CLI. When the mediation policy for a device is configured to use SSH2, secure CLI communication is used to manage the device. Table 13-1 lists different SSH protocols and the compatibility of each with different device types.

Table 13-1 SSH2 and NE compatibility

Protocol	7210 SAS-M 24F 7210 SAS-M 24F 2XFP 7210 SAS-M 24F 2XFP ETR 7210 SAS-X 24F 2XFP 7450 ESS 7705 SAR 7710 SR 7750 SR	7250 SAS 7250 SAS-ES 7250 SAS-ESA	Generic NE
SSH2	✓	✓	✓
SCP	✓		
Device management using SSH2		✓	

Note — SSH2 communication with a device may be slower to establish than other types of communication because of the encryption and authentication computations that are required.

13.4 Server resource management

The 5620 SAM supports the grouping of NEs by network function for increased SNMP mediation efficiency.

Resource allocation is automatically configured during 5620 SAM installation and network discovery based on the available system resources, and the numbers and types of NEs that are to be managed. The resource group to which an NE belongs is initially determined by the device type. The following are the 5620 SAM NE resource groups and the default device assignments:

- global—for 5620 SAM tasks that are not associated with NEs
- default—for NEs that do not belong to a specific resource group
- core—for 7450 ESS and 7750 SR devices
- middle—for 7210 SAS-E, 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7210 SAS-X 24F 2XFP, 7710 SR, and 7705 SAR devices
- edge—for 7250 SAS, Telco, and similar devices
- GNE—for other network devices

The 5620 SAM logs the system load of each resource group at regular intervals. An Alcatel-Lucent support representative can monitor system resource usage, determine whether the current resource allocation is appropriate, and reconfigure resource management, if required.

Caution — Only a qualified Alcatel-Lucent support representative can assess or configure 5620 SAM server resource management. Contact Alcatel-Lucent technical support for more information.

13.5 SNMP event notification policies

To reduce the 5620 SAM processing load associated with SNMP events, you can configure a policy that specifies which SNMP traps the 5620 SAM processes. An event notification policy acts as a filter that enables or disables the processing of specific SNMP traps for a specific NE type and version.

A 5620 SAM operator with an admin or operations scope of command role and write access permission to the policy package can create an event notification policy using the Mediation form. The 5620 SAM assigns a default event notification policy to an NE during initial device discovery. A 5620 SAM operator can create and apply a policy that specifies which traps to process and which to ignore. 5620 SAM processing is enabled for all supported traps in the default policy. See Procedure 13-6 for more information about configuring an event notification policy.

The following conditions apply to event notification policies:

- After an NE upgrade, the 5620 SAM processes the new traps generated by the upgraded NE. A 5620 SAM administrator must ensure that the event notification policies that are in effect before an NE upgrade are correctly configured, and must modify them after the upgrade to silenced new traps, if required.
- 5620 SAM software upgrades do not affect existing event notification policies.

Caution — The 5620 SAM relies on certain SNMP notifications to verify network management activities. Before you configure an event notification policy, consult an Alcatel-Lucent support representative to ensure that you do not disable the processing of traps that are vital to 5620 SAM operation.

SNMP statistics that include the number of ignored traps for an NE are available from the Statistics tab of the NE properties form.

13.6 Workflow for device discovery

The following workflow lists the high-level steps required to discover network devices.

1 Using a CLI, commission the devices that you want to discover. See chapter 12 for more information.

2 Using a CLI, ensure that each device you want to discover and manage using SNMPv3 has a unique engine ID. See Procedure 13-1 for more information.

3 Create generic NE profiles for non-Alcatel-Lucent devices, if required, as described in chapter 12.

4 Perform the following steps to configure SSH2 security, if required.

i Enable SSH2 on the device. See Procedure 13-2 for more information.

ii Configure and start an SSH server on the device. See the appropriate device documentation for SSH configuration information.

Note — A 7705 SAR may become temporarily unreachable after you enable SSH and start the SSH server on the device.

iii If the device supports SSH2 host key persistence, use Telnet to enable this function on the device. See Procedure 13-3 for more information.

5 Create a mediation policy. If you want to use SSH2 for mediation, ensure that you enable SSH2 for CLI sessions and secure file transfers.See Procedure 13-4 for more information.

Note — If you specify the use of SNMPv3 in the policy, you must enable SSH2 in the policy.

6 Discover devices.

i Create one or more discovery rules, as required. See Procedure 13-5 for more information.

Note — If you want to use SSH2, specify the created SSH2 mediation policy for read and write access in the discovery rule.

ii Verify the discovery, management, and synchronization statuses of each device specified in the discovery rules.

7 Create event notification policies, as required. See Procedure 13-6 for more information.

8 Assign event notification policies to NEs, as required. See Procedure 13-7 for more information.

9 Manage device discovery, as required, by performing one or more of the following using the procedures in this chapter.

- Edit discovery rules and rule elements. See Procedure 13-8 for more information.
- Enable or disable discovery rules. See Procedure 13-9 for more information.
- Delete discovery rules. See Procedure 13-10 for more information.
- Rescan the network using a discovery rule. See Procedure 13-11 for more information.
- Manage, unmanage, or delete managed devices. See Procedures 13-12, 13-13, and 13-14 for more information.
- Synchronize NEs with the 5620 SAM database. See Procedure 13-15 for more information.
- Monitor the acceptance and rejection of SSH2 host keys using the 5620 SAM SSH2 Known Host Key Manager. See Procedure 13-16 and 13-17 for more information.
- Switch from non-secure mediation to secure mediation for one or more devices. See Procedures 13-18 and 13-19 for more information.

13.7 Device discovery procedures

Use the following procedures to configure device discovery and mediation.

Procedure 13-1 To configure SNMPv3 on a device

Perform this procedure to enable SNMPv3 on a device. SNMPv3 provides user-based security. The access granted is restricted to the scope of the configured users and groups.

If you are configuring an NE for LI, you must create a second access group. See step 2 in Procedure 31-3 for more information about creating an LI user and access group.

1 Open a CLI session on the device.

2 Enter the following commands in the order shown to create a read-write-notify group for general SNMP mediation on the managed device:

```
configure system security snmp ↵

access group "snmpv3_groupname" security-model usm security-level
privacy read "iso" write "iso" notify "iso" ↵
```

where
snmpv3_groupname is the name that is being assigned to the SNMP group

3 If mediation of VPRN objects is required, enter the following command to create a read-write-notify group for this purpose on the managed device:

access group "*snmpv3_groupname*" security-model usm security-level privacy context vprn prefix read "vprn-view" write "vprn-view" notify "iso" ↵

where
snmpv3_groupname is the name that is being assigned to the SNMP group

4 Enter the following command to exit SNMP group configuration.

exit ↵

5 Enter the following command to obtain the SNMP engine ID of the device.

show system info ↵

The SNMP engine ID is displayed as SNMP Engine ID.

6 Generate an MD5 or SHA authentication key, and DES privacy keys, using the password2key utility on a 5620 SAM client or server station.

- MD5 and SHA authentication keys are used to create an encrypted authentication password for users.
- DES privacy keys are used to encrypt the entire SNMP packet, for additional security.

Note — The length of a generated key is determined by the authentication method. MD5 keys are 32-character strings. SHA keys are 40-character strings.

i Log in to the 5620 SAM client or server station.

Note 1 — If you are using the password2key utility on a Solaris 5620 SAM server station, you must log in as the samadmin user.

Note 2 — If you are using the password2key utility on a 5620 SAM client station, you must log in as a local administrator or as the user that installed the client.

ii Open a console window.

iii Navigate to the *install_directory*/nms/bin directory

where *install_directory* is the 5620 SAM installation location, typically /opt/5620sam/server or /opt/5620sam/client on Solaris, or C:\5620sam\server or C:\5620sam\client on Windows

iv Run the password2key utility (in nmsclient.bat or nmsclient.bash) to create an MD5 or SHA authentication key.

nmsclient.bat password2key *method password engine_ID* ↵

where
method is the type of encryption algorithm used to generate the authentication key, either MD5 or SHA
password is the ASCII password string used to generate the authentication key for the SNMPv3 user, for example, yoga
engine_ID is the SNMP engine ID obtained in step 5

The SHA authentication key generated from this example is 60210e3d2bfa7e02682262df9c5de400b9c3322b.

v Run the password2key utility (in nmsclient.bat or nmsclient.bash) to create an MD5 or SHA DES privacy key.

nmsclient.bat password2key *method password engine_ID* ↵

where
method is the type of encryption algorithm used to generate the DES privacy key, either MD5 or SHA
password is the ASCII password string used to generate the DES privacy key, for example, happy
engine_ID is the SNMP engine ID obtained in step 5

The DES privacy key generated from this example is 4088f4ef966b8d1ebe54b8d841a5f76806c374ec.

vi If your security model requires unique keys for each managed device, repeat steps 6iv and 6v for each set of keys to be generated.

vii Store the generated keys.

7 Using the keys generated in step 6, create an SNMPv3 user on the managed device.

i Enter the following sequence of commands at the prompt:

```
configure system security user snmpv3_username ↵

access snmp ↵

snmp ↵

authentication method authentication_key privacy des-key
DES_privacy_key ↵

group snmpv3_groupname ↵

exit all ↵
```

where
snmpv3_username is the name being assigned to the SNMPv3 user
snmpv3_groupname is the name of the new SNMP user group
method is sha or md5, depending on the authentication method used
authentication_key is the SHA or MD5 authentication key generated in step 6
DES_privacy_key is the DES privacy key generated in step 6

Note — A DES privacy key is 32 characters long. If SHA encryption, which produces a 40-character key, is used to generate the DES privacy key in step 6, you must provide only the first 32 characters of the key, as shown in the following example that uses the key values from step 6:

```
authentication sha
60210e3d2bfa7e02682262df9c5de400b9c3322b privacy des
4088f4ef966b8d1ebe54b8d841a5f768 ↵
```

ii Enter the following command at the prompt to save the configuration changes.

```
admin save ↵
```

The device is now ready to be managed using SNMPv3. To enable device management by the 5620 SAM, you must do the following:

- Create an SNMPv3 user using the 5620 SAM NE user configuration manager. See chapter 18 for information about creating and configuring NE users. You must specify the following for each user:
  - Give the user SNMP access.
  - Enter the same User Name as the user name created earlier in this procedure.
  - On the SNMPv3 tab, select SHA as the authentication protocol and DES as the privacy protocol.
  - Type the appropriate ASCII password used to generate the MD5 or SHA authentication key, and DES privacy key, in step 6; for example, yoga and happy.
- Create a new SNMPv3 mediation security policy, as described in Procedure 13-4. Specify the following:
  - the SNMPv3 USM security model
  - the SNMP user name created earlier in this procedure
- Create one or more discovery rules that use the new SNMPv3 mediation policy.

8 Close the CLI session.

Procedure 13-2 To verify that SSH2 is enabled on a device

Perform this procedure to verify that SSH2 is enabled on a device, and to enable SSH2 on the device, if required. See section 13.3 for a list of devices that support SSH2.

Note — If the device is a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA, you cannot use this procedure to enable SSH2. You must see the device documentation for information about enabling SSH2.

1 Open a CLI session on the device.

2 Run the following CLI command to see whether SSH2 is enabled:

```
show system security ssh ↵
```

3 If required, enter the following command at the prompt to enable SSH2:

```
configure system security ssh version 2 ↵
```

4 Close the CLI session.

Procedure 13-3 To enable host key persistence on the SSH2 server of a device

Perform this procedure to enable the persistence of the server host key on a 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP, 7210 SAS-M 24F 2XFP ETR, 7450 ESS, 7750 SR, 7705 SAR, or 7710 SR. Host key persistence is always enabled on the 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA. For other devices, see the user documentation for information about configuring SSH2 host key persistence.

1 Open a CLI session on the device.

2 Enter the following at the prompt to disable the SSH server:

```
configure system security ssh server-shutdown ↵
```

3 Enter the following at the prompt to enable host key persistence:

```
configure system security ssh preserve-key ↵
```

4 Enter the following at the prompt to enable the SSH server:

```
configure system security ssh no server-shutdown ↵
```

5 Enter the following at the prompt to verify that the preserve-key function is enabled on the server:

```
show system security ssh ↵
```

6 Close the CLI session.

Procedure 13-4 To configure NE mediation

Perform this procedure to configure the 5620 SAM to poll network elements at regular rates and intervals. To configure LI mediation, see Procedure 31-5.

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Configure the parameters:

- Polling Synchronization Time
- Polling Admin State
- Discovery Rule Scan Interval

Note — Polling and scanning use system resources, and can increase the amount of management traffic. Consider your network needs and network management domain capabilities when setting these parameters.

3 Configure MIB polling intervals for different managed devices, as required.

i Click on the MIB Entry Policies tab button.

A list of MIBs appears, organized by the product name of the device that supports the MIB.

ii Configure the search filter and click on the Search button. The Mediation (Edit) form displays the MIB entry policies that match the search criteria.

iii Select one or more MIBs from the list.

iv Click on the Properties button.

The MIB Entry Policy (Edit) form opens.

v Configure the parameters:

- Polling Interval
- Administrative State
- Number of Varbind per PDU

Caution — Changing the Number of Varbind per PDU parameter value may affect the time required for subsequent NE resynchronizations and degrade 5620 SAM server performance. Do not configure the parameter without contacting Alcatel-Lucent technical support.

vi Click on the OK button.

vii Confirm the action.

The MIB Entry Policy (Edit) form closes and the Mediation (Edit) form reappears.

viii Click on the Apply button to save the changes, if required.

4 Use the Ping tab to define how the management IP addresses of devices are checked using a ping. Each managed device may provide one or more of the following three IP addresses, each of which can be scheduled to be pinged, as configured during discovery rule creation:

- the system IP address, called an in-band management interface
- the management IP address on the management port, called an out-of-band management interface
- the IP address of the standby Control card, also called a CPM

Note — When the device does not have one or two of the IP addresses, for example, there is no CPM IP address, ensure that you create a ping policy that does not have its schedule enabled. This allows the assignment of an inactive ping policy during discovery configuration. See Procedure 13-5 for more information.

i Click on the Ping tab button.

Note — 5620 SAM ping policies use a TCP ping, not an ICMP ping.

ii Click on the Add button to create a new ping policy, or click on the Properties button to change an existing ping policy.

The ManagementPingPolicy (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- Policy ID
- Displayed Name
- Ping Command Timeout (seconds)
- Schedule Enabled

  You must enable scheduling for the default ping policy to be performed. When scheduling is not enabled, and a managed device is not reachable, management connection alarms may not be raised.
- Ping Interval (minutes)
- Ping Interval (seconds)

The destination interface of the ping is determined during the creation of discovery rules for devices. You can also perform an unscheduled ping from the Managed State tab of the Discovery Manager configuration form. See Procedure 13-5 for more information.

iv Click on the Apply button to save the changes.

You can view management connection alarms from the network element properties form of the managed device that was pinged. For example, from the Discovery Manager form, click on the Resync Status tab button. Choose a device from the list and click on the Properties button. From the network element properties form, click on the Faults tab button to view the alarms.

5 Create or modify a statistics MIB policy to determine how often the 5620 SAM polls the managed device MIBs for statistics. See the *5620 SAM Statistics Management Guide* for more information.

6 Click on the Mediation Security tab button.

i Click on the Add button to create a new SNMP mediation security policy, or select an existing policy and click on the Properties button to modify the policy. The MediationPolicy form opens.

Note 1 — Each 7250 SAS or Telco device requires a separate mediation policy unless the user names and passwords, which are often the SNMP community strings, match exactly.

Note 2 — To configure SNMPv3 security, you must preconfigure the 5620 SAM server and the managed devices. See Procedure 13-1 for more information.

ii Configure the general mediation parameters:

- Policy ID
- Auto-Assign ID
- Displayed Name
- Security Model
- Timeout (milliseconds)
- Retry
- Community String

Note — The Community String value must match the community string value on the managed device.

iii Configure the parameters in the CLI and File Transfer panels:

- Communication Protocol
- User Name
- User Password

  You must also enter the User Password parameter value in the Confirm Password parameter field.
- File Transfer Type

Note 1 — If you choose Secure as the File Transfer Type parameter value, you must set the Communication Protocol parameter to SSH2.

Note 2 — To configure SSH2 you must enable SSH2 and host key persistence on the SSH server of the device. See section 13.3 for more information about configuring SSH2.

Note 3 — If you choose SSH2 as the Communication Protocol, the User Name and User Password parameters must be the user name and password for the SSH server.

Note 4 — You must also enter the User Password value in the Confirm Password field.

7 If you choose SSH2 as the Communication Protocol value in step 6 iii, configure the SSH2 Server Port parameter.

8 Perform one of the following.

a If you choose FTP as the File Transfer Type value in step 6 iii, configure the parameters in the FTP panel:

- User Name
- User Password
  You must also enter the User Password parameter value in the Confirm Password parameter field.
- Connect Timeout (sec)
- Read Timeout (sec)

b If you choose Secure as the File Transfer Type value in step 6 iii, configure the parameters in the Secure FTP panel:

- Connect Timeout (sec)
- Read Timeout (sec)

See chapter 12 for information about enabling FTP access for a device user account.

9 If you set the Security Model parameter to SNMPv3 (USM), assign a user profile that is configured with the SNMPv3 authentication and privacy parameters, as described in Procedure 13-1.

i Click on the Select button to view a list of configured users. The Select Site User For SNMP Access form opens.

ii Select a user from the list and click on the OK button. The user name is displayed on the Mediation Security form.

iii Click on the Properties button to open the configuration form for the user and view or modify the SNMPv3 security settings, if required.

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The Mediation Policy form closes and the Mediation (Edit) form reappears.

12 Close the Mediation (Edit) form.

Procedure 13-5 To discover devices

Perform this procedure to complete the following tasks:

- Create discovery rules
- Ping the managed devices to test connectivity
- Locate managed devices on a topology map
- Discover devices by scanning the network according to discovery rules

- Set discovered devices in a managed state
- Resynchronize NEs and the 5620 SAM database
- Check the discovery, management, and synchronization status of a device

Note 1 — SNMP parameters must be correctly specified using CLI on the managed devices. Contact your Alcatel-Lucent support representative or see chapter 12 for more information about using CLI to commission devices before managing them.

Note 2 — Ensure that in-band and out-of-band management are correctly configured to discover devices, as described in chapter 12.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens with the Discovery Rules tab displayed.

2 Configure a discovery rule.

i Click on the Add button to create a new discovery rule. The Create Discovery Rule - Specify General Attributes form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Description
- Administrative State

  When you set the administrative state to Up, the network is scanned according to the discovery rule when the discovery rule is saved. The network is also scanned according to the discovery rule as specified by the Discovery Rule Scan Interval parameter in the Mediation (Edit) form. When you set the administrative state to Down, the network is not scanned as specified by these conditions.
- OLC State
- Management Protocol

iii Click on the select button beside the Group Name parameter. The Select Discovery Group - TopologyDiscoveryRule window opens with a list of Topology Groups.

iv Choose a Topology Group from the list.

v Click on the OK button. The Create Discovery Rule form refreshes with the Topology Group information displayed.

Note — If the selected Topology Group reaches the maximum element limit, any additional discovered NEs are automatically added to the Discovered Group.

vi Click the Next button. The Create Discovery Rule - Add Rule Elements form opens.

vii Click on the Add button to add a new rule element. The TopologyDiscoveryRuleElement form opens.

viii Configure the parameters:

- IP Address
- Mask Bits
- Usage

Note — Ensure that you track the IP addresses used to discover devices. When the IP address used to discover the device is the system IP address (also known as the system ID) or the L3 management interface address, management is in band. When the IP address used to discover the device is the management IP address of the device management port, management is out of band.

ix Click on the OK button. The TopologyDiscoveryRuleElement form closes and the Create Discovery Rule - Add Rule Elements form reappears.

The discovery rule is saved. When you click on the Apply button in the Discovery Manager form in step 3, the network is scanned according to the new or modified discovery rule.

x Confirm the action.

xi Add more rule elements, as required by performing substeps vii to ix.

xii Click on the Next button. The Create Discovery Rule - Configure Mediation Security form opens.

xiii Specify the mediation policies for read access, write access, and SNMP trap access. Mediation policies are created or modified using the Mediation form, as described in Procedure 13-4.

Click on the Select button if you want to specify mediation security policies specific to the discovery rule. The Configure Mediation Security form opens.

You can:

- Select an existing mediation security policy from the list and click on the OK button.
- Select an existing mediation security policy and click on the Properties button. The MediationPolicy (Edit) form opens.
- Configure the parameters, as described in step 6 in Procedure 13-4 and click on the OK button to save the changes.

If you do not specify a policy, the default policy is applied. Go to step xiv.

xiv Click on the Next button. The Create Discovery Rule - Configure Management Ping Policy form opens.

xv Specify the management ping policies for each of the following management IP addresses, if required:

- the management IP address on the management port, called an out-of-band management interface
- the system IP address, called an in-band management interface
- the IP address of the standby Control card, also called a CPM

Note — Management ping policies are created using the Mediation configuration form. These are the policies applied during discovery rule creation. You must apply a ping policy even to interfaces that do not exist.

For example, if there is no standby CPM or out-of-band management IP address, specify a ping policy that has the Schedule Enabled parameter set to disabled for the nonexistent management and standby CPM interfaces. In this example, a ping policy with the Schedule Enabled parameter enabled is required for the in-band interface that does exist. See Procedure 13-4 for more information about creating ping policies.

xvi Click on the Select button for each ping policy ID parameter. The Configure Management Ping Policy list form opens.

xvii Choose a ping policy from the list. When there is no interface, choose a ping policy that has its Schedule Enabled parameter set to disabled.

xviii Click on the OK button. The ping policy ID appears in the Policy ID parameter.

You can view management connection alarms from the network element properties form of the managed device that was pinged. For example, from the Discovery Manager form, click on the Resync Status tab button. Choose a device from the list and click on the Properties button. From the network element properties form, click on the Faults tab button to view the alarms.

xix Click on the Next button. The Create Discovery Rule - Configure MIB Statistics Policy form opens with the default MIB statistics policy displayed.

xx Click on the Select button to choose a different MIB statistics policy, if required. The Configure MIB Statistics Policy form opens. Select a MIB statistics policy in the list and click on the OK button.

xxi Click on the Next button. The Create Discovery Rule - Add Discovered Routers to Span(s) form opens.

xxii Click on the Add button to specify a span of control for the new network element contained in the discovery rule. If you do not specify a span, the default span is applied.

Note — New routers added to a span from a discovery rule are added explicitly to the span.

When a discovered NE group is part of a user-defined span, new routers that are discovered from the discovery rule are automatically added to the span.

xxiii Click on the Next button. The Create Discovery Rule - Configure Backup Policy form opens.

xxiv Click on the Select button to choose a different backup policy, if required. The Select Backup Policy - Topology Discovery Rule form opens. Select a backup policy in the list and click on the OK button.

xxv Click on the Finish button. The Create Discovery Rule form closes and a dialog box appears.

xxvi Click on the OK button to close the dialog box. The Discovery Manager form reappears.

3 Save the discovery rule, and discover devices by scanning the network as specified by the discovery rule.

i Click on the Discovery Rules tab button on the Discovery Manager form.

ii Click on the Apply button.

New or modified discovery rules are saved. The 5620 SAM discovers devices by scanning the network as specified by the discovery rules. After a device is discovered, the 5620 SAM server sets the device in a managed state and adds the device elements to the 5620 SAM database.

Discovery rules that are disabled or shut down are not applied.

4 Verify that the device is discovered and is managed by the 5620 SAM by clicking on the Managed State tab button on the Discovery Manager form. A list of managed devices opens.

The management state of the device is displayed in the Site State column. Managed is the default state. If the device is unmanaged, select the device from the list and click on the Manage button.

5 From the Managed State tab, you can also perform management IP address pings to ensure connectivity to all managed devices. Do not ping devices without an interface.

6 From the Managed State tab, you can locate the device in a topology map.

i Click on one or multiple managed devices in the list.

ii Click on the Navigate button. A drop-down menu opens that lists the map view options.

iii Select an option. The *topology_view* (Navigate) window appears showing the selected network objects.

Note — Only managed devices located outside the discovery group can be located. If the selected managed devices do not all belong to the same group on the map, then only the managed devices of one of the groups is located. Unmanaged devices cannot be located.

7 Verify that the device configuration has been reconciled with the 5620 SAM database contents by clicking on the Resync Status tab button.

The status is displayed in the Resync Status column.

- Full Resync Done indicates that the 5620 SAM resynchronized with all or a subset of the MIB entry tables for an NE.
- Partial Resync Done indicates that the 5620 SAM resynchronized with a subset of the MIB entry tables for an NE.
- Full Resync Failed indicates that the attempt of the 5620 SAM to resynchronize with all MIB entry tables for an NE failed.

  A failed status does not indicate that the SNMP agent on the managed device is not reachable. If the agent is unreachable, an SnmpReachabilityProblem alarm is raised against the managed device. When the agent becomes reachable, the alarm is cleared.
- Partial Resync Failed indicates that the attempt of the 5620 SAM to resynchronize with a subset of the MIB entry tables for an NE failed.
- Requested indicates that the resynchronization request has entered the request queue.

To initiate manual device reconciliation, select one or more devices in the list and click on the Resync button.

If the reconciliation fails:

- View faults that are associated with a device by double-clicking on the device in the Discovery Manager form and clicking on the Faults tab button in the form that opens.
- Check your SNMP security parameters on a device using the CLI.
- Check your 5620 SAM mediation settings by choosing Administration→Mediation from the 5620 SAM main menu.

Devices that have been successfully discovered appear in the 5620 SAM navigation tree and the Equipment Window form.

8 From the Resync Status tab, you can locate the device in a topology map.

i Click on one or multiple resynchronized devices in the list.

ii Click on the Navigate button. A drop-down menu opens that lists the map view options.

iii Select an option. The *topology_view* (Navigate) window appears showing the selected network objects.

Note — Only devices located outside the discovery group can be located. If the selected devices do not all belong to the same group on the map, then only the devices of one of the groups is located.

9 Close the Discovery Manager form.

Procedure 13-6 To configure an event notification policy

Perform this procedure to configure how the 5620 SAM processes specific SNMP traps from specific NE types and releases.

Caution — The 5620 SAM relies on certain SNMP notifications to verify network management activities. Before you configure an event notification policy, consult an Alcatel-Lucent support representative to ensure that you do not disable the processing of traps that are vital to 5620 SAM operation.

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens.

2 Click on the Event Notification Policies tab button.

3 Perform one of the following.

a Create a policy.

i Click on the Add button. The Event Notification Policy (Create) form opens.

ii Configure the parameters:

- Auto-Assign ID
- Policy ID
- Displayed Name
- Description
- Network Element Type

After the Network Element Type parameter is configured, the form expands to display the Product and Version panels.

iii Click on the Select button in the Version panel to choose the version of NE to which the policy is to apply. The Select Version - Event Notification Policy form opens with a list of available versions displayed.

iv Select a version and click on the OK button. The Select Version - Event Notification Policy form closes and the version information is displayed on the Event Notification Policy (Create) form.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Mediation (Edit) form reappears with the new policy in the list.

vii Click on the Apply button. A dialog box appears.

viii Click on the Yes button.

ix Select the new policy in the list and click on the Properties button. The Event Notification Policy (Edit) form opens.

b Modify a policy.

i Click on the Displayed Name column heading to sort the existing policies by device type and version.

ii Drag the Displayed Name column boundary to display the device type and release information.

iii Scroll through the list to locate the policy for the required device type and version using the information in the Displayed Name column.

iv Select the required policy and click on the Properties button. The Event Notification Policy (Edit) form opens.

v Configure the parameters:

- Displayed Name
- Description

4 Click on the Notification Policies tab button. A list of SNMP traps is displayed.

5 Click on a column header, for example, MIB Name or MIB Entry Name, to sort the list alphabetically.

6 Select an SNMP trap entry in the list and click on the Properties button. The MIB Entry Policy - trappolicy (Edit) form opens.

7 Configure the Administrative State parameter.

Note — You cannot configure the Administrative State parameter in a default event notification policy. A default policy is indicated by a check mark beside the Default Policy indicator on the General tab of the Event Notification Policy (Edit) form.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The MIB Entry Policy - trappolicy (Edit) form closes.

10 Repeat steps 6 to 9 to configure the processing of an additional SNMP trap by the 5620 SAM.

11 Close the Event Notification Policy (Edit) form.

12 Close the Mediation (Edit) form.

Procedure 13-7 To assign an event notification policy to an NE

Caution — The 5620 SAM relies on certain SNMP notifications to verify network management activities. Before you assign an event notification policy to an NE, consult an Alcatel-Lucent support representative to ensure that you do not disable the processing of traps that are vital to 5620 SAM operation.

1 Right-click on an NE icon in the navigation tree and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

2 Click on the Polling tab button.

3 Click on the Clear button in the Assigned Event Notification Policy panel. The Select button in the panel is enabled.

4 Click on the Select button in the Assigned Event Notification Policy panel to choose an event notification policy. The Select Event Notification Policy - Network Element form opens with a list of appropriate event notification policies for the device displayed.

5 Select a policy in the list and click on the OK button. The Select Event Notification Policy - Network Element form closes and the new policy identifier is displayed on the Network Element (Edit) form.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Network Element (Edit) form closes and the policy is applied.

Procedure 13-8 To edit a discovery rule

Edit discovery rules when new devices are added to the network.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Select a discovery rule from the list.

3 Click on the Properties button.

The appropriate TopologyDiscoveryRule (Edit) form opens.

4 Configure the parameters, as required. For example, to remove a rule element:

i Click on the Rule Elements tab button.

ii Select the rule from the list.

iii Click on the Delete button.

iv Confirm the action.

5 Click on the OK button to close the TopologyDiscoveryRule (Edit) form.

6 Perform steps 3 to 7 in Procedure 13-5.

7 Close the Discovery Manager form.

Procedure 13-9 To enable or disable a discovery rule

When a discovery rule is enabled, the network is scanned according to the discovery rule when the discovery rule is saved or rescanned. The network is also scanned according to the discovery rule as specified by the Discovery Rule Scan Interval parameter in the Mediation form. If your discovery rule is disabled, the network is not scanned as specified by these conditions.

1 Choose Administration→Discovery Manager from the main menu. The Discovery Manager form opens.

2 Select a discovery rule from the list.

3 Enable or disable the discovery rule.

   a Click on the Turn Up button to enable the discovery rule.

   b Click on the Shut Down button to disable the discovery rule.

Procedure 13-10 To delete a discovery rule

When you delete a discovery rule, only the rule is removed; the devices discovered using the rule are not removed from the 5620 SAM.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Select a discovery rule in the list.

3 Click on the Delete button. A dialog box appears.

4 Click on the OK button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Discovery Manager form closes.

Procedure 13-11 To rescan the network according to a discovery rule

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Select one or more discovery rules from the list.

3 Click on the Rescan button.

4 Click Yes to confirm the action.

The 5620 SAM scans the network as specified by the discovery rules and discovers devices. After a device is discovered, the 5620 SAM server sets the device in a managed state and adds the NE properties to the 5620 SAM database.

5 Perform steps 4 and 7 in Procedure 13-5 to verify that the device has been successfully discovered.

Procedure 13-12 To manage or unmanage a device

Warning — Unmanaging a device results in a loss of management data for the selected device. See section 13.1 for more information.

If you use the 5670 RAM to process 5620 SAM statistics, unmanaging an NE results in the loss of all historical 5670 RAM AA statistics for the device.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Click on the Managed State tab button.

3 Select a device in the list.

4 Click on the Manage or Unmanage button, as required. A Confirm message appears.

5 View the information and click Yes to confirm the action.

The device becomes managed or unmanaged by the 5620 SAM.

Procedure 13-13 To specify which management address the 5620 SAM uses to remanage a device

Perform this procedure to specify which management IP address is saved for a device when the device is set to an unmanaged state. You can configure the 5620 SAM to save the original management IP address or the most recently used management IP address for a device.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Click on the Managed State tab button.

3 Choose a device from the list.

4 Click on the Properties button. The Node Discovery Control (Edit) form opens with the General tab displayed.

5 Configure the Use Original Management IP parameter.

6 Click on the OK button. A dialog box appears.

7 Click Yes to confirm the action.

Procedure 13-14 To delete a device

Warning — Deleting a device results in a loss of management data and completely removes the device from the managed network. See section 13.1 for more information.

If you use the 5670 RAM to process 5620 SAM statistics, deleting an NE results in the loss of all historical 5670 RAM AA statistics for the device.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Click on the Managed State tab button.

3 Select a device in the list.

4 If the device is managed, click on the Unmanage button and wait for the state to change to Unmanaged, otherwise, go to step 5.

5 Click on the Delete button. A Confirm message appears.

6 View the information and click Yes to confirm the action.

The device is deleted by the 5620 SAM.

Procedure 13-15 To partially or fully resynchronize NEs with the 5620 SAM database

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens.

2 Click on the Resync Status tab button.

3 Select a device or devices from the list.

4 Click on the Resync button. The Resync Site(s) form opens.

5 Choose a resynchronization option.

- **a** Select Resync All MIB Entries to resync all MIBs for the device or devices and click on the Next button. The Force Resync form opens. Go to step 6.
- **b** Select Choose MIB Entries to resync some MIBs for the device.
  - **i** Click on the Next button.

    The Choose MIB Entries form opens.
  - **ii** Choose one or more MIB entries from the list.
  - **iii** Click on the Next button. The Force Resync form opens.

6 Select the Ignore Timestamps parameter to unconditionally resynchronize with the network device. When you do not ignore timestamps, MIBs are not resynchronized if the last change timestamp is unchanged.

7 Click on the Finish button. A message indicates when the resynchronization is successful.

8 Perform step 7 in Procedure 13-5 to verify that the device properties have been added to the 5620 SAM database.

9 Close the Discovery Manager form.

Procedure 13-16 To view the active and mismatched host keys

1 Open the SSH2 known host key manager by performing one of the following.

- **a** Choose Administration→Security→SSH2 Known Host Key from the 5620 SAM main menu.
- **b** Perform the following steps.
  - **i** Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.
  - **ii** Click on the Managed State tab button. A list of managed devices appears.
  - **iii** Select a device in the list and click on the Properties button. The Node Discovery Control (Edit) form opens.

iv Click on the Mediation Security tab button.

v Click on the SSH2 Known Host Key button.

The SSH2 Known Host Key Manager form opens.

2 Configure the filter criteria. A list of active and mismatched host keys appears.

3 Click on the Close button to close the SSH2 Known Host Key Manager form and the open parent forms, as required.

Procedure 13-17 To manually accept a mismatched host key

Perform this procedure to manually accept a host key that has been rejected by the 5620 SAM client so that a connection to the SSH server can be established. Before you accept a mismatched host key, verify the validity of the connection to the SSH server.

1 Open the SSH2 Known Host Key Manager by performing one of the following.

a Choose Administration→Security→SSH2 Known Host Key Manager from the 5620 SAM main menu.

b Perform the following steps.

i Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.

ii Click on the Managed State tab button. A list of managed devices appears.

iii Select a device in the list and click on the Properties button. The Node Discovery Control (Edit) form opens.

iv Click on the Mediation Security tab button.

v Click on the SSH2 Known Host Key button.

The SSH2 Known Host Key Manager filter form opens.

2 Choose Mismatch SSH2 Host Key as a match criterion using the drop-down list in the SSH2 Server Status column header.

3 Click on the Search button. A list of mismatched host keys is displayed.

4 Select the required host key entry.

5 Verify with the device administrator that the key fingerprint is the host key of the required device.

6 Click on the Delete button to delete the mismatched host key. The mismatched host key is deleted and a connection to the SSH server can be established.

Note — You can only remove the mismatched host key entry using the SSH2 Known Host Key Manager form. Deleting a Host Key Mismatch alarm from the dynamic alarm list does not remove the host key from the SSH2 Host Key Manager and 5620 SAM database.

7 Close the SSH2 Known Host Key Manager form.

8 Close the Node Discovery Control (Edit) form, if it is open.

9 Close the Discovery Manager (Edit) form, if it is open.

Procedure 13-18 To change from SNMPv2c management of a device to SNMPv3 management

1 Unmanage and delete the device.

- **i** Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.
- **ii** On the Discovery Manager (Edit) form, select the device from the list that you want to manage using SNMPv3 and then click on the Unmanage button.
- **iii** When the device shows a Site State of Not Managed, click on the Delete button.
- **iv** Click OK on the Discovery Manager (Edit) form.

2 Perform Procedure 13-1 to create SNMPv3 groups and users on the device, and to create a discovery rule with an SNMPv3 mediation security policy.

Note — You can modify the existing discovery rule with an SNMPv3 mediation security policy. However, you must create a new discovery rule for the deleted device if not all devices discovered by the same rule are changed to SNMPv3 management.

3 Rediscover the device.

- **i** Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form appears.
- **ii** Click on the Discovery Rules tab button.
- **iii** Select the discovery rule that was created in step 2 to discover the deleted device.
- **iv** Click on the Rescan button.
- **v** Click OK on the Discovery Manager (Edit) form.

Procedure 13-19 To switch from non-secure to secure mediation

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Click on the Mediation Security tab button. You can create a mediation policy as described in Procedure 13-4, or modify the default mediation policy to use SSH2. Perform one of the following.

   a Click on the Add button to create a new mediation policy. The Mediation Policy (Create) form opens with the General tab displayed.

   b Choose the default policy from the list, and click on Edit. The Mediation Policy (Edit) form opens with the General tab displayed.

3 Configure the following parameters using the prescribed values:

- SSH2 as the Communication Protocol
- The SSH2 server user name and password as the User Name and User Password
- Secure as the File Transfer Type

Note — When the File Transfer Type is set to Secure, the Communication Protocol, User Name, and User Password parameters must be configured with the SSH2 information.

- The port that the NE uses for SSH2 communication as the SSH2 Server Port

4 Configure the remaining parameters on the form.

5 Click on the OK button. A dialog box appears.

6 Click on the OK button. The Mediation Policy form closes.

7 Click on the OK button. The Mediation (Edit) form closes.

8 Perform steps 1 to 3 of Procedure 13-5 to create a new discovery rule that uses the new SSH2 mediation policy as the read-access mediation policy and the write-access mediation policy.

9 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.

10 Click on the Managed State tab button. A list of managed devices appears.

11 Choose the device from the list that you want to use SSH2 for CLI sessions and secure file transfers.

12 Click on the Properties button.

13 Click on the Mediation Security tab button.

14 Choose the newly created SSH2 mediation policy as the read access mediation policy.

Note — You can also change the mediation policy for a discovery rule by performing step 14 and choosing a discovery rule from the Discovery Rules tab.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The Discovery Manager (Edit) form closes.

Procedure 13-20 To list and save SNMP MIB information

Perform this procedure to list and save SNMP MIB information, which may be of use for purposes such as the following:

- to maintain a record of the SNMP MIBs that the 5620 SAM supports
- to compare SNMP MIB support between 5620 SAM releases
- to identify the polling interval for a MIB entry

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Click on the MIB Entry Policies tab button.

3 Configure the search filter and click on the OK button. The Mediation (Edit) form displays the MIB entry policies that match the search criteria.

4 To view the polling interval for a MIB entry, perform the following steps.

i select the MIB entry and click on the Properties button. The MIB Entry Policy (Edit) form opens with the General tab displayed.

ii View the polling interval setting in the Configuration panel.

iii Close the MIB Entry Policy (Edit) form.

5 If required, sort the list according to the contents of a column by clicking on the column header.

6 If required, perform the following steps to save the listed information to a file.

i Right-click on a column header and choose Save to File. the Save As form opens.

ii Use the form to specify the file that is to contain the saved information.

iii Click on the Save button. The information is saved to the specified file.

7 Close the Mediation (Edit) form.

14 — Device CLI sessions

14.1 Device CLI sessions overview

You can perform most NE management functions using the 5620 SAM client GUI. Functions such as the following, however, require CLI access to a managed NE:

- validating GUI configuration actions
- configuring items that the GUI cannot, such as LI user access
- troubleshooting using device debug files

The 5620 SAM client GUI provides CLI access to the managed NEs from the main menu and from NE contextual menus in topology maps and navigation trees.

Note 1 — When you use a CLI to change security parameters on anNE, the changes may not be synchronized with the 5620 SAM and subsequently not displayed in the GUI. For security reasons, the 5620 SAM cannot retrieve parameters such as passwords from an NE. To ensure that the security parameters are synchronized, you must use the client GUI to change the values.

Note 2 — A CLI script that is configured for an OmniSwitch NE can fail if it contains one or more of the following characters:

- ~
- !
- @
- $
- %
- &

Scope of command roles and user permissions on the cli package control CLI command access on an NE. The user permissions are set when security is configured on the NE locally or by using 5620 SAM configuration forms. See chapter 18 for more information about setting NE access privileges.

vi editor support

On the 7750 SR, 7450 ESS, and 7710 SR, Release 8.0 or later, you can use the vi editor to modify local files. For example, after you use the 5620 SAM script manager to create a CLI script, you can use a 5620 SAM CLI session to monitor the script execution on an NE, then use vi to modify the script. The vi editor is available in 5620 SAM Telnet and SSH sessions. It supports the standard vi navigation keys as well as the cursor keys, sometimes called the arrow keys. See the appropriate device documentation for information about the supported vi commands and functions for a specific device.

See the appropriate device documentation for information about the device CLI command structure and usage. See the *5620 SAM Scripts and Templates Developer Guide* for more information about using the 5620 SAM script manager to create CLI scripts.

14.2 Workflow to use a 5620 SAM CLI

1 Ensure that the user logged in to the 5620 SAM client GUI has console access account privileges to the managed devices.

2 Ensure that the Telnet server is started on the managed devices.

3 Ensure that SSH2 is properly configured on the managed devices, if required.

4 Open a CLI session and log in to the managed device.

5 Configure the device, view device information, and modify files, as required.

6 Close the CLI session.

14.3 CLI procedures

The following procedures describe how to open CLI sessions using the 5620 SAM and configure the CLI console preferences.

Procedure 14-1 To open a device CLI session using the 5620 SAM

Perform this procedure to open a Telnet or SSH session on a managed device using the 5620 SAM client GUI.

1 Perform one of the following.

a Use the 5620 SAM navigation tree; perform the following steps.

i Choose Equipment from the view selector.

ii Right-click on a device icon.

iii Choose NE Sessions→*option* from the contextual menu

where *option* is Telnet Session or SSH Session

The Telnet Session or SSH Session window opens.

Note 1 — The managed device must be configured for Telnet access. See the appropriate device documentation for information about configuring Telnet access to the device.

Note 2 — SSH2 is used in SSH sessions by default on the 7450 ESS, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7750 SR, 7250 SAS, and generic NEs. Ensure that SSH2 is properly configured on such a device and that an SSH2 mediation policy is specified in the device discovery rule. See chapter 13 for more information about configuring SSH2 security.

b Use the 5620 SAM main menu; perform the following steps.

i Choose one of the following main menu options:

- Tools→NE Sessions→Telnet Session
- Tools→NE Sessions→SSH Session

The Telnet Session or SSH Session window opens.

ii Perform one of the following to specify an NE as the CLI session target.

- Type the management IP address of the NE beside the dimmed Connect button.
- Select an IP address from the drop-down menu.
- Click on the Select button to search for the NE.

The Connect button is enabled.

iii Click on the Connect button.

c Use the Manage Equipment form; perform the following steps.

i Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

ii Configure the filter criteria and click on the Search button.

iii Select an NE in the list.

iv Click on the NE Sessions button and choose Telnet Session or SSH Session. The Telnet Session or SSH Session window opens.

d Use a service topology map; perform the following steps.

i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

The appropriate management list form opens.

ii Configure the filter criteria and click on the Search button.

iii Select a service in the list.

iv Click on the Topology View button. A dialog box appears.

v Click on the Yes button. A service topology map opens.

vi Right-click on an NE in the map and choose NE Sessions→Telnet Session or NE Sessions→SSH Session. The Telnet Session or SSH Session window opens.

e Use the Physical Topology map; perform the following steps.

i If the Physical Topology map is not open, choose Application→Physical Topology from the 5620 SAM main menu. The Physical Topology map opens.

ii Right-click on an NE in the map and choose NE Sessions→Telnet Session or NE Sessions→SSH Session. The Telnet Session or SSH Session window opens.

2 Enter the login credentials. You can use the CLI as specified by your user account permissions.

3 Perform NE management tasks, as required.

4 Click on the Disconnect button to close the CLI session.

Note — When you disconnect from a CLI session, the session window remains open to facilitate the opening of a subsequent CLI session.

5 Perform one of the following.

a Open a new CLI session; perform the following steps.

i Perform one of the following to specify an NE as the CLI session target.

- Type the management IP address of an NE beside the dimmed Connect button.
- Select an IP address from the drop-down menu.
- Click on the Select button to search for an NE.

The Connect button is enabled.

ii Click on the Connect button.

b Close the Telnet Session or SSH Session window.

Procedure 14-2 To configure the 5620 SAM CLI console preferences

Perform this procedure to customize the 5620 SAM CLI window settings. You can specify the following:

- the console text style and appearance
- the size of the scrolling buffer
- whether to save the session output to a file

1 Open a CLI session, as described in Procedure 14-1.

2 Right-click in the CLI window and choose Configure from the contextual menu. The Terminal Configuration form opens.

3 Configure the parameters:

- Minimum number of scrolling lines
- Font Name
- Font Size
- Bold
- Italic
- Foreground color
- Background color
- Send Console To a File
- Append to file
- Log File Location

Note — When the Send Console To a File parameter is enabled and the Append to file parameter is disabled, the log file is overwritten each time a new CLI session starts.

4 Click on the OK button. The Terminal Configuration form closes. The current and subsequent CLI sessions use the new settings.

15 — Equipment management

15.1 Equipment management overview

This chapter covers general equipment management information. The 5620 SAM equipment management interface consists of:

- a main menu
- contextual menus
- a navigation tree
- managed objects
- an equipment window
- property forms to configure object parameters

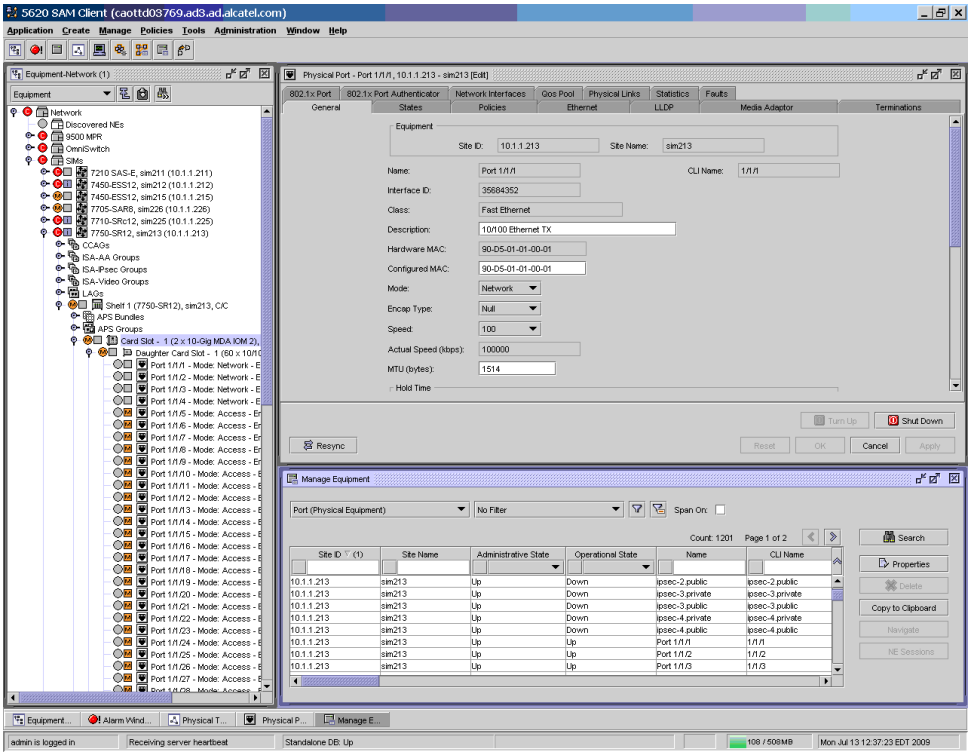
The 5620 SAM is used to create, configure, and manage a device with the various children objects required to be part of a network. Equipment such as the routers, which are at the top of the hierarchy, have properties that are configured using the CLI and discovered when the 5620 SAM discovery process is run.

After the device is discovered, you use properties forms to configure specific parameters for the child objects of the discovered device. The properties forms are opened from the contextual menus available for each created object in the equipment view of the navigation tree or from the equipment window display tab after you choose an object and click a Properties button, a Create button, or when you double-click an object.

Figure 15-1 shows the 5620 SAM GUI used to manage equipment.

- The navigation tree on the left side has the Equipment view chosen and a daughter card from shelf 1, and card slot 1 is expanded to show the available ports.
- The equipment window form on the right side displays the shelf and associated equipment parameters for the managed device under various tabs.
- The physical port configuration form is open for port 1/1/1 on the left side of the working panel. The form displays parameter information under each tab that can be configured for the managed equipment from the General tab.

Figure 15-1 GUI with equipment management drawings and forms



The 5620 SAM allows you to create and manage the following objects in the equipment view of the navigation tree:

- network — which contains the routers, devices, and topology groups
- router, device, and topology group — the next level in the hierarchy
- CCAG, LAG, IGH, ISA-AA Group, ISA-IPSEC Group, ISA-LNS Group, ISA-NAT Group, ISA-Video Group, and Shelf — which are at the third highest level in the hierarchy
- card — the highest level under the shelf, considered the parent object
- daughter card — a child object of the card object
- bundles — to group DS0 channels that physically reside on the same MDA
- port — automatically created under each daughter card, a child object of the daughter card
- channel, sub-channel, and timeslot — child objects of the port

15.2 Working with objects

Objects in the 5620 SAM are considered to have parent/child relationships that are contained within a hierarchy. For example, a card in a card slot is the parent object of a daughter card. The behavior of each object is defined using parameters that are specific to the function required. Those parameters can be managed to suit the needs of the service required. Objects are created and managed using the properties forms found in the contextual menus of the equipment view and in the forms of the equipment window.

The network is the top object in the navigation tree. The device object is the discovered device at the top of the hierarchy in the navigation tree, directly below the network icon. The following children objects of the router are created automatically in the navigation tree after the device is discovered.

- CCAG
- ISA-IPSEC Group
- ISA-AA Group
- ISA-LNS Group
- ISA-NAT Group
- ISA-Video Group
- LAG
- IGH
- Shelf
- Card Slot
- Card Slot A for the CPM and switch fabric
- Card Slot B for the redundant CPM and switch fabric

The following objects must be created using property forms or create forms from the contextual menus of the equipment view or the ring group view, or the equipment window.

- topology groups
- individual CCAGs with VSM-CCA members
- individual ISA-IPSEC Groups with ISA IPsec MDA members
- individual ISA-AA Groups with ISA-AA MDA members and ISA-AA partitions
- individual ISA-LNS Groups with ISA broadband applications MDA members
- individual ISA-NAT Groups with ISA broadband applications MDA members
- individual ISA-Video Groups with ISA-Video MDA members
- individual LAGs with subgroups of LAG member ports
- IGH members
- cards
- ring groups
- daughter cards

  Ports are automatically created when the daughter card is created.
- channels

Configuring an object is accomplished in two steps. First the object must exist or be created, second, the object parameters are modified. The following procedure is used to create objects using the navigation tree.

Procedure 15-1 To create an object

1 Right-click on an empty object in the navigation tree or in the Display tab of the equipment window to open the contextual menu.

2 Choose Properties or, when available, Create <*objectname*>.

The properties form or the create form, as applicable, opens.

3 Configure the parameters as required.

Certain object parameters are available for configuration. Configuring these parameters creates the object, however, after the object is created you may need to edit it using properties or equipment window forms.

15.3 Working with network objects

The network icon in the navigation tree is the parent object of all managed devices. When you expand the network icon, all managed devices are shown as children of the network parent.

15.4 Working with topology group objects

The topology group icons in the navigation tree represent logical topology groups. Initially, a topology group object is created by choosing Create→Equipment→Group from the 5620 SAM main menu. A Group (Create) form opens. Additional topology groups can be created using the Copy button on the topology group properties form.

The Discovered NEs topology group is created by default and contains the discovered devices. You can create new topology groups and move devices to them using the topology maps.

Although there is no limit to the number of topology groups, Alcatel-Lucent recommends a maximum of 10 000 topology groups per system for optimal performance. Each topology group can contain a maximum of 500 objects. Network elements and immediate child groups are considered objects in a topology group. A bracketed number is displayed beside the name of each topology group in the navigation tree. This number indicates the current number of objects in the group.

See chapter 4 for information about configuring topology group objects and managing topology groups using maps.

15.5 Working with device objects

The device icons in the navigation tree represent device objects. Most of the configured properties for this object are inherited from the device. The Properties contextual menu option from the navigation tree allows you to configure or modify parameters for the object. These parameters are found on the respective tab buttons of the properties form and include the following:

- General
- Polling
- Protocols
- Load Balancing
- PAE Site
- Groups
- SAS Agent
- Faults

See chapter 17 for information about configuring device objects. See chapter 12 for in-band and out-of-band management using parameters on the Polling tab.

Multiple device support

The 5620 SAM supports the following devices:

- 7705 SAR
- 7750 SR
- 7750 SR-c4
- 7750 SR-c12
- 7710 SR
- 7450 ESS
- 7250 SAS
- 7250 SAS-ES
- 7250 SAS-ESA
- Telco
- 9500 MPR
- OS 6250M
- OS 6250SME
- OS 6400
- OS 6850
- OS 6855
- OS 9600
- OS 9700
- OS 9700E
- OS 9800
- OS 9800E
- 7210 SAS-E
- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP [ETR]
- 7210 SAS-X 24F 2XFP
- generic NEs

See chapter 11 for more information about the supported device types.

15.6 Working with CCAG objects

CCAGs are navigation tree objects located below device icons. CCAGs are configured manually using the CCAG object navigation tree menu and subsequent forms. For proper CCAG configuration, a VSM-CCA card must be present in the NE. In the navigation tree, a VSM-CCA card can be opened to show its ports. The ports are indicated by VSM Port x/y/z, which shows port type and the ID of the port.

You must configure the following in the CCAG configuration forms:

- General properties such as CCAG ID, Description, CCA Rate Enabled, CCA Rate, Access Adapt QoS, and Administrative State
- CCAG MDA Members which are compatible ports that can belong to a CCAG.

When you create a CCAG, the 5620 SAM creates virtual paths to be used as interconnections to bind services together. Two unidirectional paths are created: Alpha and Beta. For each path, three virtual ports are created: one for SAP-SAP connections, one for SAP-NET connections, and one for NET-SAP connections. The last two virtual ports are used to bind a service and a network interface together.

A maximum of eight cards can be added to a CCAG, with a maximum of eight CCAGs per NE.

15.7 Working with ISA-AA groups and ISA-AA partitions

ISA-AA groups are created to provide redundancy for application assurance capabilities when multiple ISA-AA MDAs are installed on an NE. ISA-AA redundancy protects against card failure and minimizes service interruption during maintenance or protocol signature upgrades. When you create or delete an ISA-AA group, a default AA group policy is automatically created or deleted under the ISA-AA group.

You must configure the following on the ISA-AA groups configuration form:

- General properties, such as Group Number, Description, Operation Upon Failure, and Administrative State
- ISA-AA Group members
- ISA-AA Group diverted forwarding classes

An ISA-AA group can contain up to seven member ISA-AA MDAs, with up to seven ISA-AA groups per NE. Each group can contain up to seven primary members and one backup member.

ISA-AA groups are supported on the 7750 SR-7, 7750 SR-12, 7450 ESS-6, 7450 ESS-7 and 7450 ESS-12, Release 7.0 or later.

The 5620 SAM supports ISA-AA partitions. Each partition is an object with its own AA policy. You can partition an AA group into AA policy partitions with one partition for each VPN-specific AA service. The partition support VPN-specific custom protocols, applications, application group definitions, policy definitions and reporting. Each partition policy can be divided into multiple application QoS policies using ASOs. Multiple ISA-AA groups are used to scale the number of VPN-specific AA policies.

See chapter 73 for information about ISA-AA partitions, AA groups, and AA policies. See Procedure 17-17 for information about how to create and configure ISA-AA partitions.

15.8 Working with ISA-IPSEC groups

ISA-IPSEC groups are created to provide redundancy for IP security tunneling and encryption functions when multiple ISA-IPSEC MDAs are installed on an NE. ISA-IPSEC redundancy protects against card failure and minimizes service interruption during maintenance or protocol signature upgrades.

You must configure the following in the ISA-IPSEC groups configuration form:

- General properties, such as Group Number, Description, and Administrative State
- ISA-IPsec Group members

Up to two cards can be added to an ISA-IPSEC group, with up to four ISA-IPSEC groups per NE. Each group can contain one primary and one backup member. One member is the active member.

15.9 Working with ISA-LNS groups

The 5620 SAM supports the creation and configuration of ISA-LNS groups. ISA-LNS groups provide LNS PPP session termination on 7750 SR NEs. You can assign an ISA-LNS group to a tunnel group profile or a tunnel profile. When an operational L2TP tunnel is established, peers that are associated with the ISA-LNS group are automatically created. Session traffic is automatically balanced across the available active ISA broadband application MDAs in the group. You can add ISA broadband application MDAs to an ISA-LNS group, and up to four ISA-LNS groups on each NE. See Procedure 17-19 for information about how to create and configure an ISA-LNS group.

You must configure the following on the ISA-LNS groups configuration form:

- General properties, such as Group Number, Description, and Administrative State
- ISA-LNS Group members

Note — ISA broadband application MDAs can be configured only on IOM3-XP modules in a Release 8.0 or later 7750 SR -7 or 7750 SR-12.

15.10 Working with ISA-NAT groups

An ISA-NAT group provides a redundant NAT function for routing instances using ISA Broadband Applications MDAs. An ISA-NAT group can contain up to six MDAs in a warm redundancy configuration. At least one member MDA must be in the active role for an ISA-NAT group to be operational. See chapter 17 for information about creating and configuring ISA-NAT groups. See chapter 27 for information about configuring the NAT function on a routing instance. See the NE documentation for more information about NAT deployment.

Note 1 — You can install an ISA-NAT Broadband Applications MDA in an IOM3-XP module.

Note 2 — The same ISA Broadband Applications MDA can belong to an ISA-NAT group and an ISA-LNS group.

Note 3 — ISA-NAT is supported on a Release 8.0 or later 7750 SR-7 or 7750 SR-12 in chassis mode B or higher. See chapter 15 for information about chassis modes.

15.11 Working with ISA-Video groups

ISA-Video groups are created to provide packet buffering and packet processing in support of the IPTV video features.

When configured in the router, video ISAs are logically grouped into video groups. An ISA-Video group allows more than one video ISA to be treated as a single logical entity for a specific application, where the system performs a load-balancing function when it assigns tasks to a member of the group.

ISA-Video groups provide a redundancy mechanism to guard against hardware failure within a group. ISA-Video groups pool the processing capacity of all the group members and increase the application throughput because of the increased packet processing capability of the group.

You must configure the following on the ISA-Video groups configuration form:

- General parameters
- ISA-Video Group members

You can add up to four MDAs to an ISA-Video group, and up to four ISA-Video groups on each NE. All members of an ISA-Video group are primary members.

Note — If the parameter ad Insert server is enabled, only one MDA can be added to an ISA-Video group.

15.12 Working with LAG objects

LAGs are navigation tree objects located below the device icon. LAGs are configured manually using the configuration forms available when you choose Create LAG from the LAG object navigation tree contextual menu.

The following minimum configuration is required to enable LACP.

- Enable LACP at either end of the LAG group.
- Set one end of the LAG group as LACP active.

You must configure the following in the LAG configuration forms:

- General properties, such as LAG description, configured address, encapsulation type, and administrative state
- Link aggregation group parameters, such as port threshold, port threshold action, and dynamic cost
- LACP parameters, such as LACP mode, LACP transmit interval, actor administration key, LACP transmission standby, and LACP selection criteria
- LAG members, which are the compatible ports that can belong to a LAG

Because all ports can have their own MAC address, when ports are part of a LAG, the LAG must have an MAC address.

The port configuration of the first port added to the LAG is used to compare with subsequently added ports. If a discrepancy is found with a newly added port, that port is not added to the LAG. Only ports configured in network mode can belong to LAGs.

Up to 16 ports can be added to or removed from a LAG on IOM 3 and IMM cards in chassis mode D. Otherwise, up to only eight ports can be added to or removed from a LAG. All ports added to a LAG must have the same parameter settings.

Only ports belonging to one LAG subgroup are considered eligible members of a LAG and can be selected as active links.

OmniSwitch LAG objects

OmniSwitches support the following types of LAGs:

- static
- dynamic

When you create a static LAG you can manually add ports that you want to be members of the LAG.

Ports that you select to be members of a dynamic LAG are first placed into an Unassigned Dynamic LAG Members group. The OmniSwitch uses LACP to dynamically assign ports from an Unassigned Dynamic LAG Members group to the appropriate LAG. When a port is assigned to a dynamic LAG it is removed from the Unassigned Dynamic LAG Members group.

You can create VLANs, 802.1Q framing, configure QoS conditions, and other networking features on LAGs because the switch's software treats these virtual links like physical links.

OmniSwitches support:

- up to 32 LAGs on an OS 6250, OS 6400, OS 6850, or OS 6855 OmniSwitch or stack of OmniSwitches
- up to 128 LAGs on an OS 9600, OS 9700, OS 9800 OmniSwitch, Release 6.3.4 or later and on an OS 9700E, or OS 9800E, Release 6.4.2 or later
- 2, 4, or 8 Ethernet links in a LAG
- access or network LAGs

15.13 Working with IGH objects

IGHs are navigation tree objects located below the device icon. IGHs are configured manually using the configuration forms available when you choose Create IGH from the IGH object navigation tree contextual menu.

You create an IGH to group together IP links and POS links so that if a configured number of links go out of service for any reason, the remaining links in the IGH go out of service too. This causes the routing protocols to re-converge to switch from the primary path to an alternate path.

The following requirements and restrictions apply to IGHs.

- IGHs are supported only on network links.
- IGHs are supported only on SONET/TDM interfaces with PPP auto encapsulation.

- A port or channel needs to be bound to a router interface after the member is added to an IGH.
- You can assign a port to only one IGH.

15.14 Working with shelf objects

Shelf objects represent the hardware that is configured on a shelf. When you choose the shelf object in the navigation tree and click on Properties in the contextual menu, you can view the states and conditions of the shelf including:

- general information
- fan tray state and speed
- power supply tray statuses
- LED statuses
- card slots
- hardware environment information
- timing
- statistics
- dry contacts
- faults
- port segregation
- software control module
- software bank information
- cross connects

See Procedure 17-68 for information on configuring 9500 MPR port segregation.

Chassis modes

The chassis mode of a device indicates the minimum IOM or IMM card type that is initialized by the device and determines the scaling numbers and features that are available to the system. The chassis mode can be configured on the following device types:

- 7450 ESS-4, 7450 ESS-6, 7450 ESS-7 and 7450 ESS-12
- 7450 ESS-6v
- 7750 SR-7 and 7750 SR-12

See the appropriate device Release Notice for scaling information.

Tables 15-1 and 15-2 list the chassis modes that you can configure on each IOM and IMM card type for the supported devices.

Table 15-1 Chassis modes and 7750 SR IOM and IMM card compatibility

Card	Chassis mode	NE release
2 x 10-Gig MDA IOM	A	All supported releases
2 x 10-Gig MDA IOM Card, B	A and B	
2 x 10-Gig MDA IOM 2	A, B, and C	
2 x XP MDA IOM 3	A, B, C, and D	6.1 or later

(1 of 2)

Card	Chassis mode	NE release
4-Port 10 GE XFP IMM	A, B, C, and D	6.1 or later
8-Port 10 GE XFP IMM		
48-Port GIGE SFP IMM		
48-Port GIGE TX IMM		
12-Port 10GE SFP IMM		8.0 R5 or later
1-Port 100GE CFM IMM		

(2 of 2)

Table 15-2 Chassis modes and 7450 ESS IOM card compatibility

Card	Chassis mode	7450 ESS-7, 7450 ESS-12, and 7450 ESS-4	7450 ESS-6	7450 ESS-6v
2 x 10-Gig MDA IOM	A	All supported releases	All supported releases	All supported releases
2 x 10-Gig MDA IOM Card, B	A and B			
2 x 10-Gig MDA Oversubscribed IOM	A and B			
2 x XP MDA IOM 3	A and B	6.1 or later	6.1 or later	6.1 or later
	D	7.0 or later	7.0 or later	7.0 or later

Timing synchronization

Timing synchronization parameters can be configured on 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, 7750 SR-c4 and 7750 SR-c12 shelves that contain the following daughter cards:

- 10 Gigabit Ethernet with 2- and 4-port configurations
- 10/100/1000 Ethernet SFP with 20 ports
- 10 Gigabit Ethernet XFP with 4-, 8-, and 48-port configurations
- 10-port Gigabit Ethernet SFP HA
- 16 x Channelized DS1/E1 ASAP
- 16 x Channelized DS1/E1 ASAP v2
- 8-port Ethernet
- 8-port Ethernet v2
- 4-port OC3/STM1 ASAP SFP

See Procedure 17-34 for more information about configuring timing synchronization.

15.15 Working with card and card slot objects

When you click on the plus sign beside the shelf object, all the card slots contained in the shelf appear in the navigation tree. They can appear as empty card slots when a card is not provisioned for the slot. Card slot objects for the OmniSwitch OS 6250, OS 6400, OS 6850, and OS 6855 appear automatically when a physical device exists because the entire OmniSwitch device is represented by a card slot object (there are no daughter cards associated with these devices). Card slots can be configured with CMM or Ethernet card types for the OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E devices, but there are no daughter cards associated with these devices.

When the 5620 SAM discovers a 7705 SAR-F, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, or 7210 SAS-E, the integrated IOM and daughter card objects appear automatically in the navigation tree.

Card slot objects for the 9500 MPR can be configured for plug-in cards; there are no daughter cards associated with this device.

Choose Configure Card from the contextual menu of the object and assign a supported card type for the slot. The Assigned Card Type parameter lists the card types can be assigned to the card slots.

Some card types can be pre-provisioned in a slot before the card is installed in the chassis. A card and daughter card must be provisioned before a port can be configured.

When a card is first configured, the administrative state can be down. The resource is not operationally up until the card is equipped and the administrative state is up. A card can only be provisioned in a slot that is vacant, and no other card can be provisioned (configured) for that specific slot.

To reconfigure a slot position, delete the card currently in the slot and configure the new card type added to the slot. A card can only be provisioned in a slot when the card type is allowed in the slot.

Note — You can also reconfigure a slot position by changing the chassis mode. The chassis mode determines the minimum card requirements. See section 15.14 for more information about chassis modes.

For example, if a 2 x 10-Gig MDA IOM 2 card is installed in the chassis that is running in chassis mode B, the card behaves as a 2 x 10-Gig MDA IOM Card, B. You can upgrade the chassis mode to C to make the IOM card behave as a 2 x 10-Gig MDA IOM 2 card.

Card provisioning and chassis modes

The behavior of the installed card depends on the chassis mode that has been configured on the device. Table 15-3 describes the behavior of the provisioned (configured) card types and installed cards in each chassis mode.

Table 15-3 Behavior of installed IOM cards

Provisioned card type	Installed card type	Behavior
2 x 10-Gig MDA IOM	2 x 10-Gig MDA IOM	The IOM card appears and behaves at the scaling limits of the 2 x 10-Gig MDA IOM.
	2 x 10-Gig MDA IOM Card, B	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM. The 2 x 10-Gig MDA IOM Card, B is fully backward-compatible with the 10-Gig MDA IOM.
	2 x 10-Gig MDA IOM 2	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM. The 2 x 10-Gig MDA IOM 2 is fully backward-compatible with the 10-Gig MDA IOM.
	2 x XP MDA IOM 3 (1)	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM. The 2 x XP MDA IOM is fully backward-compatible with the 10-Gig MDA IOM.
2 x 10-Gig MDA IOM Card, B	2 x 10-Gig MDA IOM	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM Card, B	The IOM card appears and behaves at the scaling limits of the 2 x 10-Gig MDA IOM Card, B.
	2 x 10-Gig MDA IOM 2	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM Card, B. The 2 x 10-Gig MDA IOM 2 is fully backward-compatible with the 10-Gig MDA IOM Card, B.
	2 x XP MDA IOM 3 (1)	The IOM card appears and behaves as a 2 x 10-Gig MDA IOM Card, B. The 2 x XP MDA IOM 3 is fully backward-compatible with the 10-Gig MDA IOM Card, B.
2 x 10-Gig MDA IOM 2	2 x 10-Gig MDA IOM	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM Card, B	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM 2	The behavior of the card depends on the operational chassis mode: • 2 x 10-Gig MDA IOM in chassis mode A • 2 x 10-Gig MDA IOM Card, B in chassis mode B • 2 x 10-Gig MDA IOM 2 in chassis mode C and D
	2 x XP MDA IOM 3 (1)	The behavior of the card depends on the operational chassis mode: • 2 x 10-Gig MDA IOM in chassis mode A • 2 x 10-Gig MDA IOM Card, B in chassis mode B • 2 x 10-Gig MDA IOM 2 in chassis mode C and D

(1 of 2)

Provisioned card type	Installed card type	Behavior
2 x XP MDA IOM 3 card [(1)]	2 x 10-Gig MDA IOM	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM Card, B	The IOM card fails because the minimum card requirements are not met.
	2 x 10-Gig MDA IOM 2	The IOM card fails because the minimum card requirements are not met.
	2 x XP MDA IOM 3 [(1)]	The behavior of the card depends on the operational chassis mode: • 2 x 10-Gig MDA IOM in chassis mode A • 2 x 10-Gig MDA IOM Card, B in chassis mode B • 2 x 10-Gig MDA IOM 2 in chassis mode C • 2 x XP MDA IOM 3 in chassis mode D

(2 of 2)

Note
(1) Also applies to any IMM

15.16 Working with daughter card objects

After the card is created in the card slot you can create and configure MDAs, also known as daughter card objects, in the daughter card slot that appears when you click on the plus sign beside the card object. The daughter card slots in the card appear in the navigation tree. They appear as empty daughter card slots when a daughter card is not provisioned for the slot. When a daughter card is provisioned for the slot, it is identified. See chapter 17 for information about how to create and configure daughter cards using the 5620 SAM.

Each 5620 SAM license key allows a specific number of MDA cards of each node type to be managed. You can purchase additional MDA management capacity as required. MDA cards fall into two licensing categories: premium and standard. Generally, all non high performance MDA cards are considered standard. All IMM, High Speed MDA (HSMDA) and Extended Performance (XP) MDA cards are considered premium.

Note 1 — When the 5620 SAM has discovered the number of premium MDAs allowed by the license key, the 5620 SAM can no longer discover 7210 SAS-M, 7210 SAS-X, 7710 SR, and 7450 ESS devices.

Note 2 — Upgrading the 5620 SAM to a new major release may require adjustment to the license keys to avoid license keys warnings with exception MDA cards. See the appropriate 5620 SAM Release Description for information about which exception MDA cards have been downgraded.

7705 SAR auxiliary alarm daughter cards

The 7705 SAR supports an auxiliary alarm daughter card. This is a unique card type, intended to interface with real-time systems. The following inputs and outputs are available:

- 24 digital inputs can connect to dry contacts of security sensors, HVAC systems, and telecom systems.
- Two analog inputs support a voltage range of 0 to 75 Volts, with up to four configurable thresholds for alarms/events per port. These inputs can be used for battery DC voltage monitoring.
- Eight dry-contact relay outputs can interface to external audible, visual, or telecom equipment. Normally Open (NO) and Normally Closed (NC) contact pins are available.

The inputs and outputs are listed on the Ports tab of the daughter card slot Properties form, in the same manner as ports on a dataplane daughter card.Each input or output has configurable parameters. The Name parameter for each input and output must be unique throughout a particular node.

7705 SAR six port E&M daughter cards

The 7705 SAR supports the six port E&M daughter card. Configuration of ports and channels on this daughter card is similar to the 16 port DS1/E1 ASAP daughter card. You create a channel under each port, and a channel group under each channel.

The following configuration restrictions and limitations also apply to ports and channels on the six port E&M daughter card:

- Maximum of one channel per port
- Maximum of one channel group per channel
- Channel groups must be Access mode with CEM encapsulation type
- Channel group MTU is not configurable

CESoPSN Cpipe is the only service type to which channel groups on this daughter card are assignable as SAPs.

7705 SAR-F daughter cards

The 7705 SAR-F integrates 8-port Ethernet v3 and 16-port DS1/E1 v2 ASAP MDA functionality on a single chassis. When the 5620 SAM discovers a 7705 SAR-F the integrated MDAs are automatically configured and displayed in the equipment tree.

7210 SAS-E daughter cards

The 7210 SAS-E supports an integrated 2 x 12-Gig IOM card on a single chassis. The equipment navigation tree displays a card slot with one daughter card that contains 12 x 100/1000 Ethernet SFP ports and 12 x 10/100/1000 Ethernet ports. When the 5620 SAM discovers a 7210 SAS-E, the integrated IOM and daughter card are automatically configured and displayed in the equipment tree.

7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7210 SAS-X 24F 2XFP daughter cards

The 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7210 SAS-X 24F 2XFP support an integrated 2 x 12-Gig IOM card on a single chassis. The equipment navigation tree displays card slot 1 with a daughter card that contains 24 x 10/100/1000 Ethernet SFP ports. When the 5620 SAM discovers a 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], or 7210 SAS-X 24F 2XFP, the integrated IOM and daughter card are automatically configured and displayed in the equipment tree.

IMM daughter cards

The IMM card integrates IOM 3 and high bandwidth MDA functionality on a single card that fits into existing IOM slots. When you configure the IMM the integrated MDAs are automatically configured. The 5620 SAM equipment tree displays the IMM with two daughter cards, each having half of the total number of ports supported by the IMM.

Each daughter card object contains a number of ports that are specific to the type of service required. The port objects are created automatically under the daughter card but they must be configured based on the function served by the port; for example, as an access interface for a VPRN service.

You can associate policies to daughter cards. Network buffer policies are used to create and edit QoS buffer pool resources on egress network ports, channels, and ingress ports. Ingress and egress network ports and channels have a dedicated buffer pool for egress queuing. The ingress and egress network traffic is handled by a buffer pool at the ingress and a buffer pool at the egress.

You can also configure multicast path management on an IMM daughter card. See chapter 46 for more information.

15.17 Working with port and channel objects

The types of ports available depend on the daughter cards that are configured in the chassis. For some OmniSwitch devices, the ports that are available depend on the chassis type, for others the type of card that is configured for the card slot. Ethernet ports cannot be channelized. SONET/SDH and TDM ports can be channelized. The following types of ports are supported:

- Fast Ethernet (10/100/1000 Base-T)
- Gigabit Ethernet (1000Base-T)
- 10 Gigabit Ethernet (10000Base-T)
- 10 Gigabit Ethernet (10GBase-T)
- Ethernet combo
- PoE
- OC-3/STM-1, OC-12/STM-4, OC-48/STM-16, and OC-192/STM-64 SONET/SDH
- channelized OC-3 and DS3/E3
- channelized ASAP OC-3/STM-1, OC-12/STM-4, DS1/E1, and DS3/E3

The port syntax for most devices that support daughter cards is card slot/daughtercard/port. For example, Port 1/1/1 represents port 1 of daughter card 1 in slot 1. The port syntax for the OmniSwitch is card slot/port. In every case, ports are created automatically when the daughter card is created. You must select one port object at a time and configure the properties of the port for the service that you need the port to provide. The properties vary depending on whether the port type is one of the Ethernet ports, SONET/SDH ports, or TDM ports. Channel objects are created on SONET/SDH or TDM ports for any type of channelization on the port whether it is a clear channel application or a sub-channel application.

Use the properties forms available from the contextual menus in the navigation tree or the equipment window to configure port and channel parameters. You can configure the port mode as network, access, or hybrid.

- Network ports pass network-level traffic.
- Access ports are customer-facing and pass service-level traffic.
- Hybrid ports can pass network-level and access-level traffic.

Note — By default, a port is in Network mode.

Clear channel ports (OC-192/OC-48c/OC-12c/OC-3c) are either network or access ports. Channelized ports (CHOC-12/CHOC-3c/ DS3/E3) are always in access mode, however, the ASAP CHOC-3 supports both access and network modes. The ASAP DS1/E1 ports support:

- access mode for ATM/IMA and TDM
- network mode for PPP/MLPPP

Network ports are used in the service provider transport or infrastructure network, such as an IP/MPLS-enabled backbone network or uplink ports for rings using L2 Ethernet switches, such as the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco. A port that is in network mode can be assigned an IP address and host an L3 interface that can perform IP routing functions.

Note — The number of network interfaces that you can configure on one port is increased considerably in Release 8.0 and later NEs to support hybrid port applications. See the appropriate device documentation for specific interface configuration limits.

Access ports are associated with a SAP, a subscriber, and a service to provide connectivity. Access ports and channels are configured with encapsulation values to differentiate the service on the port or channel. When a port is access mode, one or more services can be configured on the port. A channelized port that is to act as an endpoint must be in access mode. You can convert access ports to hybrid ports and migrate any existing SAPs. See Procedure 15-2 for more information.

Hybrid ports are ports that can host SAPs and network interfaces simultaneously. This enables a customer to use one uplink port for enterprise and end-user traffic. A hybrid port preserves the existing network and access port functionality, and uses the same QoS, scheduler, and port scheduler resources as other ports, but requires the configuration of weight values that allocate buffer percentages to the access and network traffic on the port.

The 5620 SAM supports hybrid mode configuration for Ethernet ports on Release 8.0 or later of the 7450 ESS, and 7750 SR-7, and 7750 SR-12 in any chassis mode.

Note — The 7450 ESS-1 and 7750 SR-1 do not support hybrid port mode.

You can configure a hybrid port on an Ethernet MDA in an IOM-3XP, or on a CMA in an IOM-XP. The 7750 SR supports hybrid port configuration on an IMM in addition to an IOM-3XP.

Note — Hybrid port configuration is not supported on an HSMDA or a VSM MDA.

A hybrid port supports dot1q and QinQ encapsulation, but does not support null encapsulation, in order to accommodate single-SAP operation. The available VLAN tags are shared among the VLAN SAPs and VLAN network IP interfaces. When you create a SAP or L3 interface on a hybrid port, the outer VLAN tag must not be in use by another SAP or L3 interface on the port.

By default, the MTU of a hybrid port is set to the larger of the network and access MTUs to accommodate the creation of L3 interfaces and SAPs.

Note 1 — A hybrid port can participate in a single-chassis LAG.

Note 2 — A hybrid port cannot participate in an MC-LAG or MC ring.

See the appropriate device documentation for more information about hybrid ports.

When working with a TDM port, you must specify the Line Buildout as either short or long. That is, for a DS3 port the Line Buildout parameter must be configured. If the TDM port is in the context of a SONET STS-1 sub-channel, for example, the DS3 channel is built on the STS-1 channel of a SONET port, the line buildout parameter is not required.

At the connection termination points, you are required to configure the Encap Type as required, the MTU size as required, and the configured MAC address as required when configuring the port or channel.

Policies can be added or deleted as required using the equipment window.

You can associate policies to ingress and egress access and network ports. Buffer policies are used to create and edit QoS buffer pool resources on network ports, access ports, and access channels. Egress network ports, access ports, and access channels have a dedicated buffer pool for queuing. The traffic is handled by a single buffer pool, one at the ingress, and one at the egress.

You can configure the amount of egress buffer space to be allocated to the port or channel. By default, all egress buffers are allocated fairly among the egress ports and channels based on their relative egress bandwidth.

The egress buffers for egress network ports and channels are put into per-port or per-channel egress buffer pools and are used by the egress network forwarding class queues on that port or channel. The ingress buffers allocated to network ports and channels are summed into a single pool and are used by the ingress network forwarding class queues (defined by the network ingress buffer policy).

The egress and ingress buffers allocated to access ports and channels are put into an egress buffer pool and ingress buffer pool for the port or channel. The access buffer pools are used by egress and ingress service queues created by the SAP-egress and SAP-ingress policies in use by services on the port or channel.

Changing the size of an egress buffer pool should be carefully planned. By default, there are no free buffers to increase the size of a pool. In order to increase a pool on one port or channel, the same amount of buffers must be freed from other egress buffer pools on the same daughter card.

Procedure 15-2 To migrate SAPs from access mode to hybrid mode

Perform this procedure on Ethernet or SC-LAG access ports that contain SAPs.

Note — Save the device configuration before you perform this procedure. See the appropriate NE documentation for more information.

1. Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.
2. Right-click on an Ethernet port or SC-LAG port in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.
3. Change the Mode parameter from Access to Hybrid. A dialog box opens.
4. Click on the Yes button.

   A warning message window opens stating that you must perform an admin save.
5. Perform Procedure 21-4 in response to the warning message.
6. Select the I understand the implications of this action check box and click on the Yes button. The SAP Migration Result window displays information about the number of SAPs migrated.
7. Click on the OK button to close the windows.

Digital diagnostics monitoring

The 5620 SAM displays the following digital diagnostics monitoring data and alarm and warning information for ports on SFPs and XFPs optical modular transceivers:

- temperature
- supply voltage (SFP)

- TX bias
- TX output power
- RX received optical power
- external calibration

The transceiver is programmed with warning and alarm thresholds for low and high conditions that can generate system events. The thresholds for SFPs and XFPs are programmed by the transceiver manufacturer. The 5620 SAM raises an alarm when these thresholds are exceeded.

You can view digital diagnostics monitoring information from the DDM tab on the property form of supported ports. The External Calibration tab is available if the ports on SFPs and XFPs optical modular transceivers support the external calibration functionality.

Tagged and untagged VLAN ports

Consider the following when you create VLANs on CLE devices, such as 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch devices.

- You must configure the 7250 SAS and Telco uplink ports in network mode, to allow a physical connection, which is called the uplink, to the network device that feeds the traffic ring, such as a 7450 ESS.
- The 5620 SAM supports tagged and untagged ports as VLAN access ports.

Table 15-4 describes the behavior when ingress tagged or untagged traffic enters and then exits a VLAN.

Table 15-4 Tagged and untagged traffic behavior

Ingress traffic configuration	Ingress VLAN port configuration	Action	Egress VLAN port configuration and action
Untagged	Untagged	The VLAN allows the traffic and passes it based on the default VLAN ID. The MAC address of the destination is learned.	If the egress VLAN port is untagged, the traffic remains untagged.
			If the egress VLAN port is tagged, a tag is added to the traffic.
	Tagged		If the egress VLAN port is untagged, the traffic remains untagged.
			If the egress VLAN port is tagged, a tag is added to the traffic.

(1 of 2)

Ingress traffic configuration	Ingress VLAN port configuration	Action	Egress VLAN port configuration and action
Tagged	Untagged	The VLAN allows the traffic if the tag matches the default VLAN ID. The MAC address of the destination is learned. If the tag does not match the default VLAN ID, the traffic is dropped.	If the egress VLAN port is untagged, the tag of the traffic is removed. If the egress VLAN port is tagged, the traffic remains tagged.
	Tagged	The VLAN allows the traffic: • if the tag matches the default VLAN ID • if the tag matches another VLAN ID The MAC address of the destination is learned. If the tag does not meet either condition, the traffic is dropped.	If the egress VLAN port is untagged, the tag of the traffic is removed. If the egress VLAN port is tagged, the traffic remains tagged.

(2 of 2)

Figures 15-2 and 15-3 show how tagged and untagged traffic is handled on the devices, based on the VLAN ID.

Figure 15-2 Untagged traffic and VLANs

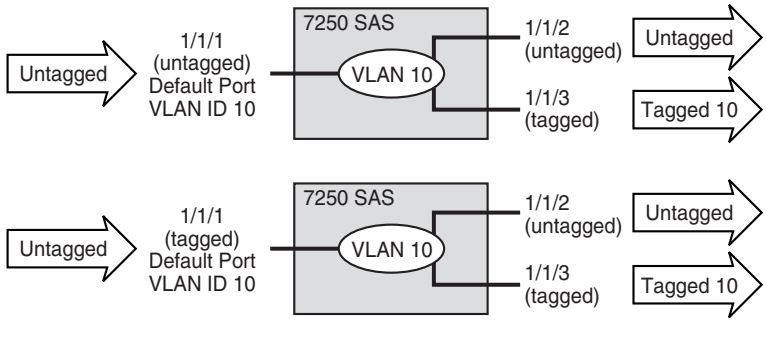
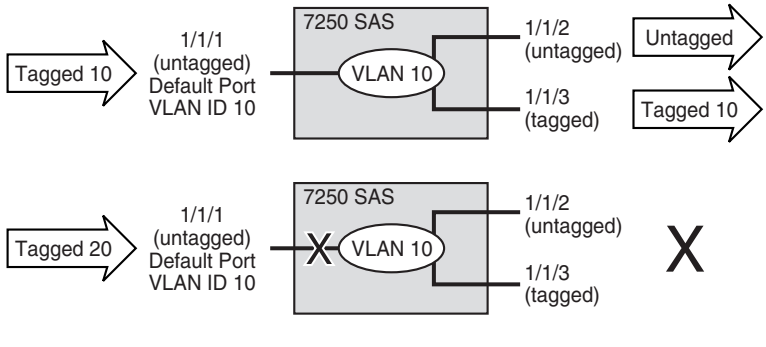


Figure 15-3 Tagged traffic and VLANs



Connection termination points for services and interfaces

Connection termination points are objects that represent terminating endpoints for a service, for example the endpoint of a VLL service. Connection termination points can be Layer 2 or Layer 3 interfaces, depending on the type of service being created. At the connection termination points you must configure the mode as Access or Network, the Encap Type as required, the MTU size as required, and the configured MAC address as required when configuring the port or channel. The following objects can be used for connection termination points:

- STS-3 to STS-192 clear channels
- DS3 clear channel
- DS0 groups
- ports
- bundle

STS-3 to STS-192 clear channel

STS-3 to STS-192 clear channel SONET/SDH ports can be used to create SAPs or IP interfaces with one clear channel on each port that operates at the rate of the parent object. Clear channel SONET applications can be performed on any OC-*n* card. SONET channel termination for 1 x 10-Gig MDAs are not supported. See "SONET clear channel applications" in this section for more information.

DS3 clear channel

A DS3 clear channel can be a connection termination point when it is explicitly configured as unchannelized, that is, when the Configuration Type is set to None, which is the default setting for a DS3. DS3 clear channel connections cannot be channelized to a lower level than the one full DS3 channel. See "TDM channelization and clear channel applications" in this section for more information.

DS0 channel groups

Only the DS0 group level can be used as a connection termination point for SONET STS-1 sub-channels. Channelization on the 1 × OC12 can be used to create up to 12 SONET STS-1 sub-channels. Each of these STS-1 channels can be used to create a DS3 frame on which you can build DS1 or E1 channels that can be configured to the DS0 channel group level. You can configure the DS0s of a DS0 group in any sequence and you do not need to use all of them. For example, you may use DS0 1, 3, 5, and 9 only, or anther combination. See "SONET VT1.5 and VT2 payloads" in this section for more information.

Only the DS0 group level can be used as an endpoint on the channelized 12 × DS3 card. Channelization can be used on each DS3 port of this card to create independent TDM channels in the form of DS1 or E1 data channels that handle DS0 groups. As with SONET sub-channels, the DS0s of a DS0 group can be configured in any sequence and you do not need to use all of them. For example, you may use DS0 1, 3, 5, and 9 only, or another combination. See "SONET and SDH sub-channel applications and structure" in this section for more information.

Ethernet ports

Ethernet ports can be configured as connection termination points in SAPs and IP interfaces. They cannot be channelized.

You must configure the class of port, such as fast Ethernet, Gigabit Ethernet, or 10G Ethernet. You must also configure the port encapsulation at the connection termination point. Ethernet access ports use:

- dot1q—supports multiple services on the port; the outer encapsulation value that distinguishes services is the VLAN ID in the IEEE 802.1Q header
- QinQ—supports multiple services on the port/channel; the inner and outer encapsulation values that distinguish services is the VLAN ID in the IEEE 802.1Q header
- null—supports a single service on the port

You must configure the duplex parameter from the Ethernet tab if the port is to be added to a LAG. Configure the Dot1 Q Ethertype and Q in Q Ethertype parameters from the Ethernet tab, if required. The range is 1536 to 65 535.

You must also configure the speed parameter from the General tab. The options are 10, 100, 1000, or 10 000, depending on the speed of the Ethernet interface.

Most OmniSwitch chassis offer four hybrid or combo ports. These ports consist of four paired 10/100/1000Base-T ports and four 1000 SFP ports. Preferences for these ports are configurable and, depending on the configuration, redundancy can be provided if a link fails.

PoE is supported on the OmniSwitch, except for the Metro version of the OS 6250, and provides power directly from the Ethernet ports. Powered devices such as IP phones, wireless LAN stations, Ethernet hubs, and other access points can be plugged directly into the Ethernet ports. The powered devices receive both electrical power and data flow from the RJ-45 ports.

OmniSwitch learned port security

LPS provides a mechanism to control network device access on one or more OmniSwitch ports. Configurable LPS parameters allow you to restrict the source learning of host MAC addresses to:

- a specific amount of time in which the switch allows source learning to occur on all LPS ports
- a maximum number of learned MAC addresses allowed on the port
- a list of configured authorized source MAC addresses allowed on the port

The following options allow you to specify how the LPS port handles unauthorized traffic.

- Block only traffic that violates LPS port restrictions; authorized traffic is forwarded on the port.
- Disable the LPS port when unauthorized traffic is received; all traffic is stopped and a port reset is required to return the port to normal operation

See Procedure 28-51 for information about enabling LPS on Ethernet ports and configuring LPS properties. See Procedure 17-62 for information about configuring static MAC addresses on LPS enabled Ethernet ports

MTU size and port configuration

You must specify the MTU size for an Ethernet port using the MTU (bytes) parameter on the General tab at the connection termination endpoint.

Consider the following when you configure MTU parameters.

- The managed devices must handle MTU limitations at many service points. The physical (access and network) ports, service, and service tunnel MTU values must be individually defined.
- The ports to be designated as network ports and the ports to be designated as access ports intended to carry service traffic must be identified.
- MTU values should not be frequently modified.
- Service MTU values must be less than or equal to the service tunnel MTU.
- Service MTU values must be less than or equal to the access port MTU.
- The MTU value for an in-band management port should be less than or equal to the MTU value for the peer port connected to the in-band management port.

See the device specific documentation for end-to-end considerations for configuring maximum MTU size throughout the managed network.

The Ethernet port MTU parameter indirectly defines the largest physical packet that the port can transmit or that the far-end Ethernet port can receive. Packets received that are larger than the MTU are discarded. Packets that cannot be fragmented at egress and that exceed the MTU are discarded.

The parameters for MTU configuration include the destination MAC address, source MAC address, Ethernet encapsulation type, length field, and complete Ethernet payload.

The MTU value for a port is associated with the port mode, such as access or network, and the port encapsulation type. If you change the mode or encapsulation type value for a port, the 5620 SAM adjusts the MTU value to a default value. If you do not want the MTU values for ports to revert to the defaults, you can configure the 5620 SAM to retain the currently configured MTU values for ports regardless of a mode or encapsulation type change. See Procedure 15-3 for more information.

HSMDA Egress Secondary Shapers

The egress port scheduler combines all subscriber queues of the same scheduling class and services the queues in a byte fair round robin fashion. This results in more packets being forwarded into the aggregation network towards a DSLAM than the DSLAM can accept. If the HSMDA egress port is congested, the egress bandwidth represented by the downstream discarded packets to the DSLAM may be allocated packets destined to other DSLAMs.

The HSMDA supports egress secondary shapers to provide a control mechanism to prevent downstream overruns without affecting the class-based scheduling behavior on the port. All subscribers destined to the same DSLAM have their queue groups mapped to the same egress secondary shaper. As the scheduler services the queues within the groups according to scheduler class, the destination shaper is updated.

After the shapers rate threshold is exceeded, scheduling for all queues associated with the shaper is stopped. When the dynamic rate drops below the threshold, the queues are allowed to be placed back on the scheduler service lists. By removing the queues from their scheduling context for a downstream congested DSLAM, the port scheduler is allowed to fill the egress port with packets destined to other DSLAMs without affecting class behavior on the port.

Egress secondary shapers are configured per port.

Procedure 15-3 To configure the 5620 SAM to retain non-default port MTU values

Use this procedure to configure a 5620 SAM server for non-default MTU refresh behavior.

Note — If the 5620 SAM is deployed in a redundant cluster configuration, you must perform this procedure on each 5620 SAM main server in the cluster.

1 Log in to the 5620 SAM main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory or folder, typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

3 Open the nms-server.xml file with a plain-text editor.

4 Add the following line to the end of the file:

```
<customMTURefresh refresh="true"/>
```

5 Save the nms-server.xml file.

6 Close the nms-server.xml file.

7 Open a console window.

8 Navigate to the 5620 SAM server binary directory or folder, typically /opt/5620sam/server/nms/bin on Solaris or C:\5620sam\server\nms\bin on Windows.

9 Perform one of the following actions.

a If the 5620 SAM server is installed on a Solaris workstation, enter the following at the console prompt:

```
# ./nmsserver.bash read_config ↵
```

b If the 5620 SAM server is installed on a Windows PC, enter the following at the console prompt:

```
nmsserver.bat read_config ↵
```

The 5620 SAM server reads the nms-server.xml file and puts the configuration change into effect.

10 Close the console window.

Moving and copying SAPs between ports

You can move and copy SAPs between physical Ethernet ports, logical ports, or a combination of both. You can also move and copy SAPs between endpoints configured with ATM encapsulation. For example, you can move a SAP on an IMA bundle to another bundle or to a TDM channel configured with ATM encapsulation. This functionality is typically used in redundancy scenarios, or to recover from a hardware failure.

Consider the following before you attempt to copy or move a SAP:

- Ports:
  - The source and destination ports can be on the same or different chassis. Inter-chassis copy and move is supported only when both NEs are of the same type and in the same chassis mode. Both NEs must run the same major software release version, for example, 8.0 R1 and 8.0 R3.
  - The source and destination ports can be the same. This configuration allows you to change the encapsulation values for a group of SAPs on the same port using outer and inner encapsulation offset values. These values can be positive or negative, depending on whether the encapsulation values must increase or decrease.
  - The physical Ethernet ports can be of different types; for example, Fast Ethernet (10/100/1000 Base-T), Gigabit Ethernet (1000 Base-T), and 10 Gigabit Ethernet (10 GBase-T).
  - The source and destination ports must be configured as access ports.
  - The encapsulation type must be the same on the source and destination ports.
- SAPs:
  - The SAPs can be associated with either L2 access interfaces on services such as Apipes, Epipes, Ipipes, VPLS, and MVPLS, or L3 access interfaces or subscriber interfaces that are associated with services such as IES and VPRN.
  - The copy and move operation does not copy and move MEPs that are configured on a VPLS, MVPLS and Epipe L2 access interface. MEP configuration is discarded during the copy and move operation.
  - For L2 and L3 access interfaces, you can move all SAPs or a subset of the SAPs on a port. You can also copy all SAPs or a subset of the SAPs on a port for L2 access interfaces.
  - All SAPs associated with a specific port within a group interface contained in an L3 subscriber interface can be moved at the same time.
  - The copy and move operations fail if the encapsulation value for a SAP on the source port is used by a SAP on the destination port. You can modify the SAP encapsulation values used on the destination port, if required.
  - The selected SAPs on the source port do not need to belong to the same service.
  - If a SAP on the source port belongs to a service not supported on the destination port, the SAP is not copied or moved.
  - The maximum number of SAPs varies for ports and MDAs. The SAP copy or move operation fails if the SAP capacity is exceeded for the destination port.
  - You cannot change SAP encapsulation from bridged to routed if ARP and DHCP options have been configured.
- SAP attributes:
  - VPLS and MVPLS dynamic FIB entries that are associated with copied or moved SAPs are discarded. Static FIB entries are transferred to the destination port after a successful SAP copy or move.
  - All SAP redundancy relationships at the source port, such as those provided by an MVPLS, are discarded during a copy or move operation.
  - All alarms, statistics, or OAM test results that are associated with a copied or moved SAP are discarded.

- When a source SAP belongs to an SHG, the 5620 SAM attempts to preserve the SHG membership. The destination SHG must have the same name as the source SHG, and must have the same residential SHG status. If an SHG with the same name does not exist on the destination service site, the 5620 SAM creates it.
- When a source SAP is uses an aggregation scheduler, the scheduler is copied to the destination. The aggregation scheduler must be unique to the destination NE and must have the same scope, for example, MDA or port.

Procedure 15-4 To copy or move L2 access interface SAPs between ports

Note — In this release, you cannot move or copy an MSAP.

You can also use the 5620 SAM clipboard functionality to copy or move SAPs. See chapter 2 for information about using the 5620 SAM clipboard.

1 For the source NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE, by configuring the Auto Backup Scheme parameter appropriately. See chapter 21 for more information about configuring automatic configuration backup for an NE.

2 On the source NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

admin save *file_name* ↵

where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the copy or move operation

Caution — An unsuccessful SAP copy or move may result in the deletion of one or more source SAPs from the source NE. The backed-up configuration file is required to restore the configuration on the source NE if a SAP copy or move operation fails.

See the appropriate device documentation for more information about saving the device configuration to a file.

3 For the destination NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE by configuring the Auto Backup Scheme parameter appropriately. See chapter 21 for more information about configuring automatic configuration backup for an NE.

4 On the destination NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

admin save *file_name* ↵

where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the copy or move operation

See the appropriate device documentation for more information about saving the device configuration to a file.

5 Open the Deployment form to monitor deployments as they occur during the SAP copy or move operation. Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Incomplete Deployments tab is displayed.

Caution — Alcatel-Lucent strongly recommends that you monitor the NE deployments and the Alarm window during a SAP copy or move operation to ensure that faults that may arise during the operation are immediately detected.

The Incomplete Deployments tab of the Deployment form notifies the 5620 SAM operator of configuration changes that are not successfully deployed to the NE, and the 5620 SAM Alarm window alerts the operator to object failures on the NE that are related to the copy or move operation.

6 Choose Tools→Copy/Move SAPs. The Copy/Move SAPs form opens with the General tab displayed.

7 Arrange the forms on the GUI so that the Copy/Move SAPs form, the Deployment form, and the Alarm window are all shown.

8 Click on the Result Export Path tab button. The Result Export Path form opens.

9 Specify the file name and location in which to save a text file that contains the results of the SAP copy or move operation.

10 Click on the Set button. The Result Export Path form closes.

11 Click on the Select button beside the Source Node parameter. The Select Network Elements form opens.

12 Choose a source NE from the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Source panel.

13 Click on the Select button beside the Source Port parameter. The Select Port form opens.

14 Configure the filter criteria. A list of available ports is displayed.

15 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Source panel.

16 Click on the Select button beside the Destination Node parameter. The Select Network Elements form opens.

17 Select a destination NE in the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Destination panel.

18 Click on the Select button beside the Destination Port parameter. The Select Port form opens.

19 Configure the filter criteria. A list of available ports is displayed.

20 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Destination panel.

21 Configure the parameters:

- Current Mode
- Outer Encap Value Start
- Outer Encap Value End
- Inner Encap Value Start
- Inner Encap Value End
- Service Type
- Outer Encap Value Offset
- Inner Encap Value Offset
- Action Type
- Continue on individual Failure

22 Click on the Execute button to begin the copy or move operation. The Execution Result panel displays the execution state of the copy or move operation and the number of successful and failed operations based on the input criteria.

Note — When you copy or move a SAP on an L2 interface and there is a non-zero value assigned to the PIM Snooping parameter Max. Number of Groups, the value is not copied or moved to the new location. You must manually configure the Max. Number of Groups parameter in the new location.

23 Monitor the Deployments form and the Alarm window for any deployment failures and faults related to the SAP copy or move operation. Click on the Refresh button of the Deployments form to update the list, if required.

24 Click on the Result tab button to view a list of the successful and failed operations as identified by the 5620 SAM.

25 Click on the Refresh Result button to view the most recent results.

26 To view the information for an individual SAP copy or move operation, move the mouse pointer over the Message field of the operation.

27 If a copy or move operation fails, you can restore the previous source NE configuration using the backup configuration file created in step 2. To restore the previous NE configuration:

i Open a CLI on the source NE.

ii Enter the following at the command prompt to load the saved configuration file:

```
exec file_name ↵
```

where *file_name* is the name of the configuration file that was specified in step 2

The SAPs that were deleted during the unsuccessful copy or move operation are restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

```
admin save ↵
```

28 If a copy or move operation partially fails, you can restore the previous destination NE configuration using one of the following methods.

Note — If the copy or move operation fails completely, there is no need to restore the previous configuration because no SAPs are created on the destination NE.

a Restore the backed-up configuration file.

i Open a CLI on the destination NE.

ii Enter the following at the command prompt to load the saved configuration file:

```
exec file_name ↵
```

where *file_name* is the name of the configuration file specified in step 4

The previous configuration is restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

```
admin save ↵
```

b Manually delete the SAPs that the copy or move operation created on the destination NE.

29 Restore the previous automatic configuration backup functionality in the backup policy used by the source NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See chapter 21 for more information about configuring automatic configuration backup for an NE.

30 Restore the previous automatic configuration backup functionality in the backup policy used by the destination NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See chapter 21 for more information about configuring automatic configuration backup for an NE.

31 Close the Copy/Move SAPs and the Deployments forms.

Procedure 15-5 To move L3 access interface SAPs within or between ports on the same NE

Perform this procedure to move one or more L3 access interface SAPs within a port, or from one port to another port on the same NE.

To copy one or more L3 access interface SAPs from one port to another port on the same NE, see Procedure 15-7 for more information.

To copy or move L3 access interface SAPs from one port to another on different NEs, see the *5620 SAM Scripts and Templates Developer Guide* for information about the administrative tasks associated with service templates.

You can also use the 5620 SAM clipboard functionality to move SAPs. See chapter 2 for information about using the 5620 SAM clipboard.

Note — L3 access interfaces are not bound to a port; for example, loopback interfaces cannot be moved.

1 For the NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE, by configuring the Auto Backup Scheme parameter appropriately. See chapter 21 for more information about configuring automatic configuration backup for an NE.

2 On the NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

admin save *file_name* ↵

where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the move operation

See the appropriate device documentation for more information about saving the device configuration to a file.

3 Open the Deployment form to monitor deployments as they occur during the SAP move operation. Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Incomplete Deployments tab is displayed.

Caution — Alcatel-Lucent strongly recommends that you monitor the NE deployments and the Alarm window during a SAP move operation to ensure that faults that may arise during the operation are immediately detected.

The Incomplete Deployments tab of the Deployment form notifies the 5620 SAM operator of configuration changes that are not successfully deployed to the NE, and the 5620 SAM Alarm window alerts the operator to object failures on the NE that are related to the move operation.

4 Choose Tools→Copy/Move SAPs. The Copy/Move SAPs form opens with the General tab displayed.

5 Arrange the forms on the GUI so that the Copy/Move SAPs form, the Deployment form, and the Alarm window are all shown.

6 Click on the Result Export Path tab button. The Result Export Path form opens.

7 Specify the file name and location in which to save a text file that contains the results of the SAP move operation.

8 Click on the Set button. The Result Export Path form closes.

9 Click on the Select button beside the Source Node parameter. The Select Network Elements form opens.

10 Choose an NE from the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Source panel.

11 Click on the Select button beside the Source Port parameter. The Select Port form opens.

12 Configure the filter criteria. A list of available ports is displayed.

13 Choose a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Source panel.

14 Click on the Select button beside the Destination Port parameter. The Select Port form opens.

15 Configure the filter criteria. A list of available ports is displayed.

16 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Destination panel.

17 Configure the parameters:

- Current Mode
- Outer Encap Value Start
- Outer Encap Value End
- Inner Encap Value Start
- Inner Encap Value End
- Service Type
- Outer Encap Value Offset
- Inner Encap Value Offset
- Continue on individual Failure

18 Click on the Execute button to start the move operation. The Execution Result panel displays the execution state of the move operation and the number of successful and failed operations based on the input criteria.

19 Monitor the Deployments form and the Alarm window for any deployment failures and faults related to the SAP move operation. Click on the Refresh button of the Deployments form to update the list, if required.

20 Click on the Result tab button to view a list of the successful and failed operations as identified by the 5620 SAM.

21 Click on the Refresh Result button to view the most recent results.

22 To view the information for an individual SAP move operation, move the mouse pointer over the Message field of the operation.

23 If a move operation fails, you can restore the previous NE configuration using the backup configuration file created in step 2. To restore the previous NE configuration:

i Open a CLI on the NE.

ii Enter the following at the command prompt to load the saved configuration file:

exec *file_name* ↵

where *file_name* is the name of the configuration file specified in step 2

The SAPs that were deleted during the unsuccessful move operation are restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

admin save ↵

24 Restore the previous automatic configuration backup functionality in the backup policy used by the NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See chapter 21 for more information about configuring automatic configuration backup for an NE.

25 Close the Copy/Move SAPs and the Deployments forms.

Procedure 15-6 To move L3 subscriber interface SAPs between ports on the same NE

Perform this procedure to move one or more L3 subscriber interface SAPs from one port to another port on the same NE.

To copy or move L3 subscriber interface SAPs from one port to another on different NEs, see the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

You can also use the 5620 SAM clipboard functionality to move SAPs. However, you can only move all of the SAPs in a group interface; you cannot be used to move a subset of SAPs. See chapter 2 for information about using the 5620 SAM clipboard.

1 For the NE, disable automatic configuration backup if enabled in the backup policy assigned to the NE, by configuring the Auto Backup Scheme parameter appropriately. See chapter 21 for more information about configuring automatic configuration backup for an NE.

2 On the NE, use a CLI to back up the device configuration to a file. Ensure that you use a unique name for the backup file to ensure that it is not accidentally overwritten. Enter the following at the CLI prompt:

admin save ***file_name*** ↵

where *file_name* is a name that differs from the existing configuration file names on the NE and identifies this as the configuration in effect before the move operation

See the appropriate device documentation for more information about saving the device configuration to a file.

3 Open the Deployment form to monitor deployments as they occur during the SAP move operation. Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Incomplete Deployments tab is displayed.

Caution — Alcatel-Lucent strongly recommends that you monitor the NE deployments and the Alarm window during a SAP move operation to ensure that any faults that arise during the operation are immediately detected.

The Incomplete Deployments tab of the Deployment form notifies the 5620 SAM operator of configuration changes that are not successfully deployed to the NE, and the 5620 SAM Alarm window alerts the operator to object failures on the NE that are related to the move operation.

4 Choose Tools→Copy/Move SAPs. The Copy/Move SAPs form opens with the General tab displayed.

5 Arrange the forms on the GUI so that you can view the entire Copy/Move SAPs form, the Deployment form, and the Alarm window.

6 Click on the Result Export Path tab button. The Result Export Path form opens.

7 Specify the file name and location in which to save a text file that contains the results of the SAP move operation.

8 Click on the Set button. The Result Export Path form closes.

9 Click on the Select button beside the Source Node parameter. The Select Network Elements form opens.

10 Choose an NE from the list and click on the OK button. The Select Network Elements form closes and the NE identifier is displayed in the Source panel.

11 Click on the Select button beside the Source Port parameter. The Select Port form opens.

12 Configure the filter criteria. A list of available ports is displayed.

13 Choose a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Source panel.

14 Configure the filter criteria. A list of available ports is displayed.

15 Choose a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed in the Destination panel.

16 Configure the parameters:

- Current Mode
- Service Type
- Outer Encap Value Offset
- Inner Encap Value Offset
- Continue on individual Failure

17 Click on the Execute button to start the move operation. The Execution Result panel displays the state of the move operation, and the number of successful and failed operations based on the input criteria.

18 Monitor the Deployments form and the Alarm window for any deployment failures and faults related to the SAP move operation. Click on the Refresh button of the Deployments form to update the list, if required.

19 Click on the Result tab button to view a list of the successful and failed operations, as identified by the 5620 SAM.

20 Click on the Refresh Result button to view the most recent results.

Note — If one SAP fails, all SAPs under the same group interface fail because the SAPs can only move together. In this case, there is insufficient information to determine which SAP caused the problem using the 5620 SAM.

21 To view information about an individual SAP move operation, move the mouse pointer over the Message field of the operation.

22 If a move operation fails, you can restore the previous NE configuration using the backup configuration file created in step 2. To restore the previous NE configuration:

i Open a CLI on the source NE.

ii Enter the following at the command prompt to load the saved configuration file:

exec *file_name* ↵

where *file_name* is the name of the configuration file specified in step 2

The SAPs that were deleted during the unsuccessful move operation are restored on the NE.

iii Enter the following at the command prompt to save the NE configuration:

admin save ↵

23 Restore the previous automatic configuration backup functionality in the backup policy used by the NE, if required, by configuring the Auto Backup Scheme parameter appropriately. See chapter 21 for more information about configuring automatic configuration backup for an NE.

24 Close the Copy/Move SAPs and the Deployments forms.

Procedure 15-7 To copy L3 access interface SAPs between ports on the same NE

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Click on the L3 Access Interface tab button.

5 Choose an L3 access interface and click on the Properties button. The L3 Access Interface (Edit) form opens.

6 Click on the Port tab button.

7 Click on the Copy button.

a If you are copying an IES L3 access interface, an L3 Access Interface (Create) form opens. Go to step 9.

b If you are copying a VPRN L3 access interface, a Select Site form opens. Go to step 8.

8 Select a site and click on the OK button. The L3 Access Interface (Create) form opens.

9 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State

10 Click on the Port tab button.

11 Click on the Select button in the Terminating Port panel to choose a port to associate with the L3 access interface. The Select Terminating Port - L3 Access Interface form opens.

12 Configure the filter criteria. A list of available ports appears.

Note — Only ports in access mode appear in the list.

13 Select a port and click on the OK button. The Select Terminating Port - IES Service Access Point form closes, and the IES Service Access Point (Create) form reappears with the port information displayed.

14 Click on the OK button. A dialog box appears.

15 Click on the OK button to confirm the action. The L3 Access Interface (Create) form closes and the service configuration form appears with the newly created L3 access interface.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The service configuration form closes.

SONET/SDH and TDM port encapsulation

SONET/SDH and TDM ports can be configured as connection termination points in SAPs and IP interfaces. They can be channelized.

An access port is used for customer-facing traffic on which services are configured. SAPs can only use an access port. When a port is configured for access mode, the appropriate encapsulation type must be specified to distinguish the services on the port.

You must configure the Encap Type parameter from the General tab at the connection termination point. SONET/SDH or TDM ports or channels support the following encapsulation types, depending on the MDA type:

- BCP Null
- IPCP
- BCP Dot1 Q
- FR — Support multiple services using the DLCI header to distinguish services
- ATM — Support multiple services using the VCI or VPI of the PVC
- PPP Auto
- CEM

MTU size considerations apply to SONET/SDH and TDM channels. See "MTU size and port configuration" in section 15.17 for more information.

SONET clear channel applications

Ports on OC-*n* cards can be used for SONET clear channel applications. SONET or TDM clear channel applications allow you to create a full channel on a port which can be configured as access or network mode for SONET and access only for TDM. For example, when you create a 16 × OC3 SFP card, 16 ports are created. You can create one full channel on each of these ports. For more information about the 4-port OC3/STM1 ASAP SFP card for clear channel support on the 7705 SAR-8, see OC3/STM1 clear channel support on the 7705 SAR-8 in this section.

STS-192/48/12/3 clear channel applications use the following syntax:

```
card slot/daughtercard/port.STSType
```

For example, the clear channel STS-12 on slot 4, MDA 1, port 1 is named 4/1/1.sts12

Table 15-5 lists available SONET channel applications and parameters for clear channel, sub-channel, and TDM applications.

Table 15-5 SONET channel parameters

Applications	Channel ranges								
	STS-192	STS-48	STS-3	STS-1	DS3	DS1	DS0	E1	DS0
SONET Clear channel	1	1	1		1				
SONET Sub channel			1 to 4	1 to 3	1	1 to 28	1 to 24	1 to 21	2 to 32
TDM					1	1 to 28	1 to 24	1 to 21	2 to 32

OC3/STM1 clear channel support on the 7705 SAR-8

The 7705 SAR-8 supports the 4-port OC3/STM1 ASAP SFP card. The 4-port OC3/STM1 ASAP SFP card supports access mode for ATM-encapsulated traffic only. See ATM encapsulation in this section for more information. The interface must be configured as UNI.

All of the ports on this card can be independently configured for either SONET (OC3) or SDH (STM1) framing. The transmit clock rate for a port can be device- or loop-timed.

The section trace (J0) byte can be configured by the operator to check the physical cabling. The port can activate and deactivate local line and internal loopbacks. The MTU size for a 4-port OC3/STM1 ASAP SFP access port is fixed at 1572 for ATM encapsulation.

CSM activity switches for a 4-port OC3/STM1 ASAP SFP card on the 7705 SAR-8 are hitless on the data path.

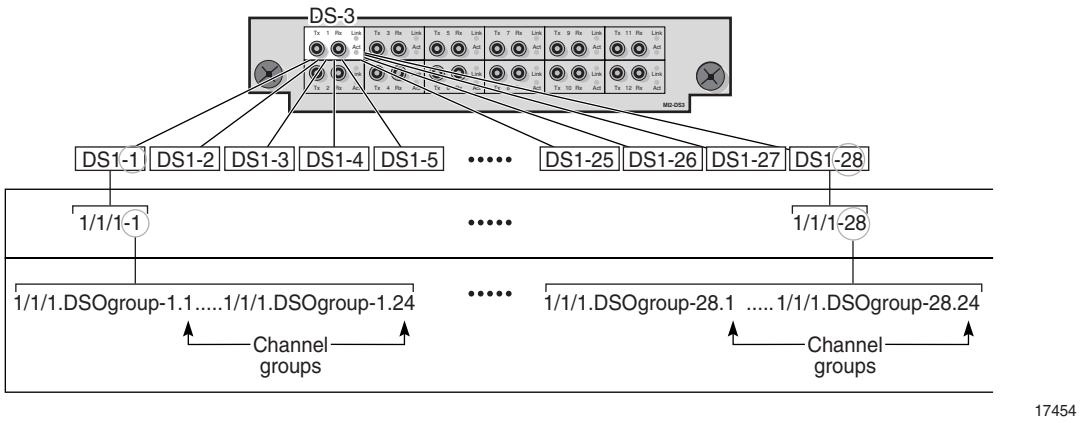
Note — Channels on the 4-port OC3/STM1 ASAP SFP adapter card cannot be configured as IES SAPs.

TDM channelization and clear channel applications

When you create a 4 or 12 ×DS3/E3 card, 4 or 12 DS3/E3 ports are created. You can then create DS3/E3 channels using the 5620 SAM, one per port. Each DS3/E3 channel can be channelized into 28 independent DS1 or 21 independent E1 data channels or, in clear channel applications, the DS3 can be the connection termination point. For channelized DS3 connections, each DS1 channel can be channelized to 24 DS0 groups and each E1 channel can be channelized to 31 DS0 groups. To use a DS1 or E1, you must create at least one DS0 group for the DS1 or E1.

By default, DS3 ports are automatically created for clear channel connections. To create a channelized DS3, you must configure the DS3 channel type as E3 or DS3 on the port. To channelize the DS3 to the DS0 level, you must set the Channelization Type to Channelized DS1 or E1. Figure 15-4 shows the channelized DS3 port structure for DS1 channels.

Figure 15-4 Channelized 12 × DS3 port structure for DS1 Channels



The channelized DS3 port structure for E1 channels has the following parameter values:

- each DS3 port supports 21 E1 channels
- each E1 channel supports 31 DS0 channel groups

TDM-based DS3 channelization uses the following syntax:

DS3 channel configured for TDM:

```
card slot/daughtercard/port.DS3-
```

DS1 channel from a TDM-based DS3 channel:

```
slot/daughtercard/port.DS1-[DS3#].[DS1#]
```

E1 channel from a TDM-based DS3 channel:

```
slot/daughtercard/port.DS1-[DS3#].[E1#]
```

DS0 group channel from the DS1 channel:

```
slot/daughtercard/port.DS0Grp-[STS3#].[STS1#].[DS1#/E1#].[Group#]
```

Table 15-6 provides an example of the naming conventions for a 12 × DS3 port.

Table 15-6 Example of TDM channel naming convention

Syntax	Description	Additional information
Channel 1/1/1.ds3	1/1/1 is the slot number/daughtercard number/port number .ds3 identifies the channel as DS3	Because DS3s are unchannelized by default, you must configure the Channelization Type as Channelized.
Channel 1/1/1.ds1-1.2	.ds1 identifies the channel as DS1 1 is the DS3 number .2 is the DS1 number (1 to 28)	Identifies the DS1 channel and shows how the DS3 level acts as a place holder for the DS1s.

(1 of 2)

Syntax	Description	Additional information
Channel 1/1/1.e1-1.2	.e1 identifies the channel as E1 1 is the DS3 number .2 is the E1 number (1 to 21)	Identifies the E1 channel and shows how the DS3 level acts as a place holder for the E1s.
Channel 1/1/1.ds0Grp-1.2.23	.ds0Grp- identifies the channel as a DS0 group 1 is the DS3 number .2 is the DS1 number (1 to 28) or E1 number (1 to 21) .23 identifies the DS0 channel group (1 to 24) on the DS1 or (2 to 32) on the E1	The DS0 group is configured on the DS1 or E1 channel. Only a DS0 can be used as a CTP.

(2 of 2)

ATM encapsulation

SONET/SDH clear channels can be provisioned so that ATM cells are encapsulated in SONET/SDH frames. The entire SONET/SDH path of the port is then used to carry ATM cells. The channel of the port becomes the ATM interface. ATM encapsulation is supported on the following daughter cards:

- 16 × ATM OC3 SFP
- 4 × ATM OC12/OC3 SFP
- 4 × OC3/STM1 ASAP SFP
- 4 × Any Service Channelized OC3
- 16 x Any Service Channelized DS1/E1

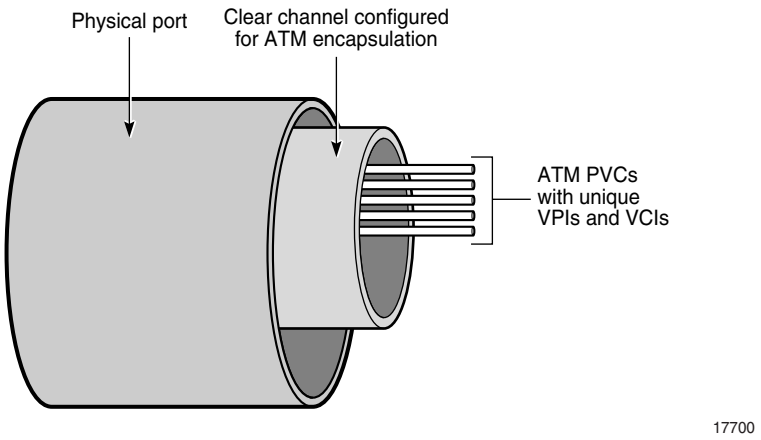
SONET/SDH clear channel applications with ATM encapsulation use the following syntax:

```
Daughter Card Slot - 3 (16 x ATMOC3), OK

Port 3/1/1 - Speed: OC3, State: OK

Channel 3/1/1.sts3, Mode: Access, Encap: ATM, State: Ok
```

Customer devices with ATM interfaces are connected directly or using the ATM access network to a 7750 SR that offers IES or VPRN services.

A SONET/SDH clear channel with ATM encapsulation can carry multiple ATM PVCs. ATM PVCs cannot be created from the 5620 SAM. They are created automatically by the router when a new Layer 3 interface over ATM is created. Figure 15-5 shows an example of ATM PVCs on a SONET/SDH clear channel.

Figure 15-5 ATM PVCs on a SONET/SDH clear channel



ILMI links between ATM interfaces

ILMI links can be configured between ATM interfaces. ILMI is a protocol that sets and sends physical layer, ATM layer, virtual path, and virtual channel parameters that are exchanged by ATM interfaces.

When ILMI is run between two ATM interfaces, the interfaces exchange ILMI packets that consist of SNMP messages across the physical connection. An ILMI link allows ILMI to run on an available virtual channel. When an ILMI link is created to carry ILMI messages, a PVC is automatically created with default PVC attributes. The PVC is deleted when the ILMI link is removed.

IMA

IMA is supported on channelized ASAP MDAs on the 7750 SR, 7710 SR, 7705 SAR, and ATM DS1/E1 CMA on the 7710 SR. IMA group bundles aggregate E1 or DS1 ATM paths into a single logical ATM interface. Each IMA group bundle can have from 1 to 8 members, or links. Up to 56 IMA group bundles can be configured on a single 7750 SR or 7710 SR MDA. Up to 8 IMA group bundles can be configured on a single 7705 SAR daughter card.

For the 9500 MPR, IMA is supported on the 16 x E1 ASAP Access (ETSI) card. Each IMA group bundle can have up to 16 links and there can be up to 8 IMA groups on a card.

Each ATM Interface supports up to 48 VP/VC connection points. Each 16 x E1 ASAP Access (ETSI) board supports up to 128 VP/VC connection points.

An IMA group bundle has the following common interface properties:

- ATM encapsulation type is displayed on the ATM Interface properties form by clicking on the "Edit ATM button".
- The ATM interface characteristics can be viewed by clicking on the "Edit ATM button" button on the Bundle Properties form. This button is displayed on the Bundle Properties form only for the 9500 MPR.
- The interface mode is access only for the 9500 MPR.

- MTU value (of the primary link)

Note — The two following paragraphs do not apply to the 9500 MPR.

Member links inherit the common properties of the IMA group to which they belong. Only the properties of the primary link can be changed. The primary link is the member with the lowest interface index or initialization sequence. The primary link may change as member links are added and deleted from the IMA group.

Consider the following when you create a multilink IMA group bundle.

- When a path becomes a member of an IMA group bundle, it is no longer a physical ATM path interface.
- The members of the IMA group bundle inherit all of the properties of the primary link, such as the SONET configuration and MTU. If you modify the configuration of the primary link, the configuration of the bundle members is also modified.
- Member links that are added after the primary link has been added to the IMA group bundle must match the configuration of the primary link.
- You cannot configure services on a member link.

15.18 SONET and SDH sub-channel applications and structure

SONET sub-channel applications allow you to create multiple STS-1 channels on deep channelized OC-12 and OC-3 ports, and to configure multiple DS0 connection termination points.

An STS-1 sub-channel is configured, or channelized, to carry one of the following payload types:

- DS3
- VT1.5
- VT2

Because of the differences between SONET and SDH in multiplexing and mapping of tributary payloads into higher digital levels, some building blocks of SDH have no SONET equivalent and therefore the containment hierarchy and terminology for SDH is different from SONET. See “Comparison of SONET and SDH hierarchies” and “SDH AU-4 and AU-3 sub-channel applications” in this section.

SONET DS3 payload

The following example, illustrated in Figure 15-6, shows the channelization sequence for a DS3 payload on a 1 × OC12 Deep Channel card.

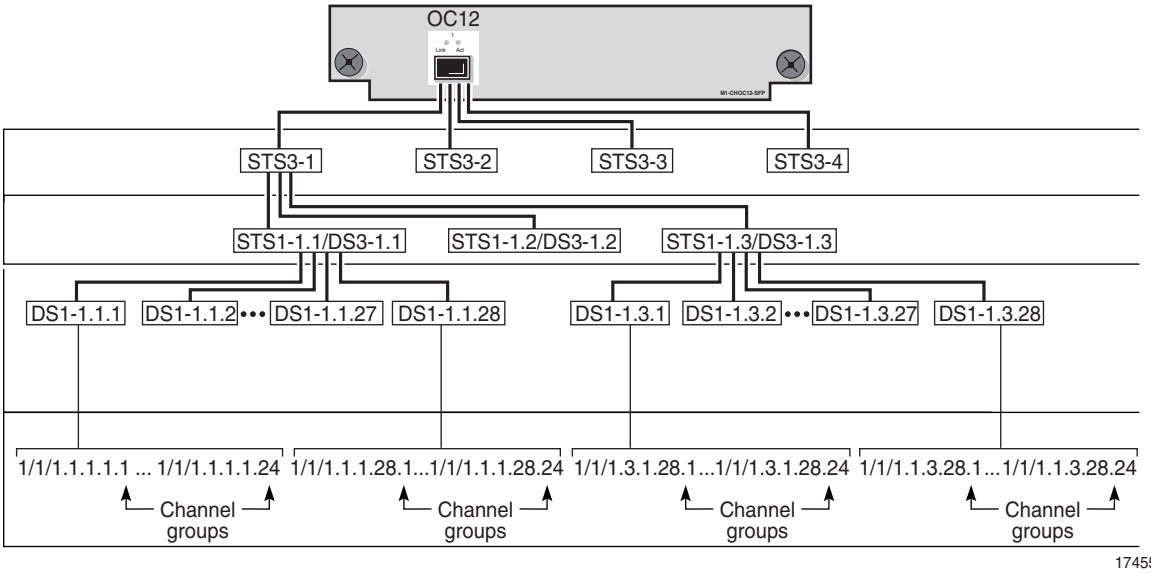
1 One OC-12 port is created when you create a channelized 1 × OC12 Deep Channel card.

2 This port can be channelized into 12 SONET STS-1 sub-channels from the four STS-3s available on the port.

3 You can then configure each of these STS-1s to carry a DS3 frame

4 Each DS3 frame can be channelized into 28 independent DS1 data channels or 21 independent E1 data channels. Each channel must be created one at a time.

Figure 15-6 Channelized 1 × OC-12 port structure using STS-1/DS3 sub-channels



SONET VT1.5 and VT2 payloads

The following example, illustrated in Figure 15-7, shows the channelization sequence for a VT1.5 or VT2 payload on a 1 × OC12 Deep Channel card.

1 One OC-12 port is created when you create a channelized 1 × OC12 Deep Channel card.

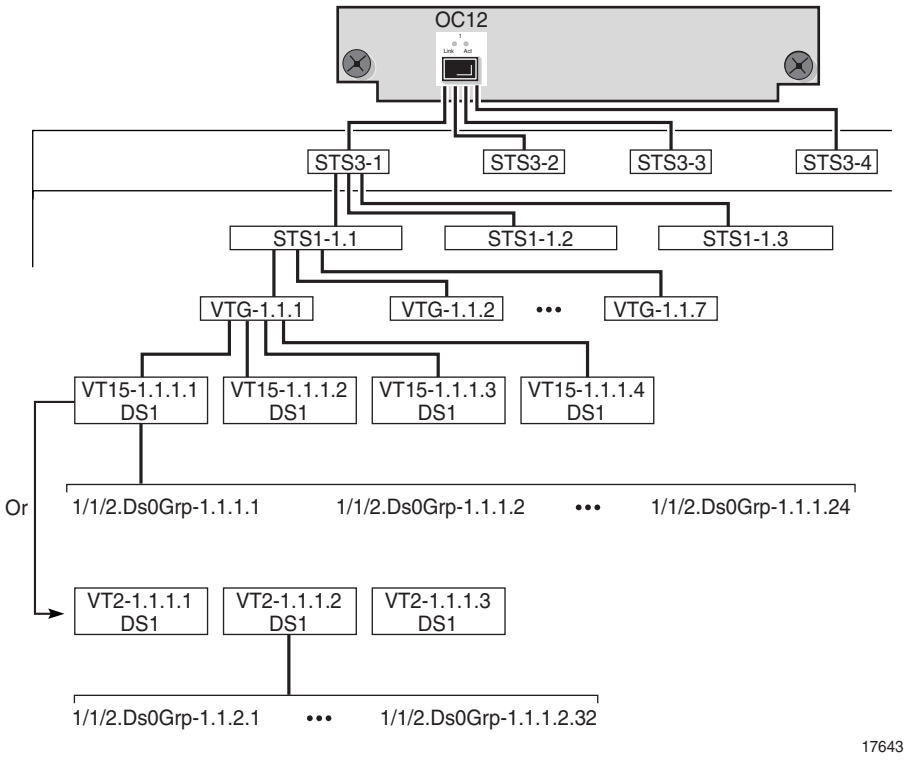
2 This port can be channelized into 12 SONET STS-1 sub-channels from the four STS-3s available on the port.

3 You can then configure each of these STS-1s to be channelized to carry up to 28 DS1. For SONET sub-channel configuration you must select payload type VT1.5 or VT2. When you choose VT1.5 payload type, seven VTG are implicitly created.

4 Each VTG is channelized into four independent VT1.5 channels or three VT2 channels, each of which can carry an independent DS1 data channel. Each channel must be created one at a time.

5 Each VT1.5 DS1 channel can be configured to handle up to 24 DS0 groups. Each VT2 DS1 channel can be configured to handle up to 32 DS0 groups. To use a DS1, you must create at least one DS0 group for the DS1 or E1.

Figure 15-7 Channelized 4 × OC-3 port structure using VT sub-channels



SONET sub-channel syntax

The 5620 SAM uses the following SONET syntax for the STS-1 sub-channel:

```
card slot/daughtercard/port.STS1-[STS3#].[STS1#]
```

DS3 channels from an STS-1 sub-channel use the following syntax:

```
slot/daughtercard/port.DS3-[STS3#].[STS1#]
```

DS1 channels from a DS3 channel use the following syntax:

```
slot/daughtercard/port.DS1-[STS3#].[STS1#].[DS1#]
```

E1 channels from a DS3 channel use the following syntax:

```
slot/daughtercard/port.DS1-[STS3#].[STS1#].[E1#]
```

VT15 or VT2 from a VT group use the following syntax:

```
slot/daughtercard/port.VTG#-[STS3#].[STS1#]
```

DS1 channels from a VT15 or VT2 use the following syntax:

```
slot/daughtercard/port.DS1-[STS3#].[STS1#].[VT15#] or
[VT2#}.[VTG#].[DS1#]
```

Table 15-7 shows an example of the SONET sub-channel syntax.

Table 15-7 Example of SONET sub-channel syntax for an OC-12 port

Syntax	Description	Additional information
Channel 1/1/1.sts1-2.2	1/1/1 is the slot number/daughtercard number/port number 2 is the STS-3 number (1 to 4) .2 is the STS-1 number (1 to 3)	The sts1 parameter is 2.2 which means that it is the fifth STS-1. There are four STS-3s for an OC-12 and each STS-3 has three STS-1s such that the fifth STS-1 is the second STS-1 of the second STS-3.
Channel 1/1/1.ds3-2.2	.ds3-2 is the STS3 number (1 to 4) .2 identifies the STS-1 number (1 to 3)	Identifies the DS3 channel and shows how the sts1 level acts as a place holder for the DS3
Channel 1/1/1.ds1 2.2.25	.ds1-2.2.25 identifies a DS1 channel (1 to 28) on the DS3	The DS1 is configured on the DS3.
Channel 1/1/1.e1 2.2.21	.e1-2.2.21 identifies a E1 channel (1 to 21) on the DS3	The E1 is configured on the DS3.
Channel 1/1/1.DS0Grp-2.2.20.5	.DS0Grp-2.2.20.5 identifies one of the DS0 channel groups: 1 to 28 for DS1; 2 to 32 for E1	The DS0 is configured on the DS1 or E1 channel.
Channel 1/1/1.ds1 2.2.3.18	ds1 2.2.3.18 identifies a DS1 channel on the VT15 or VT2 payload, where 3 is the VT group.	—

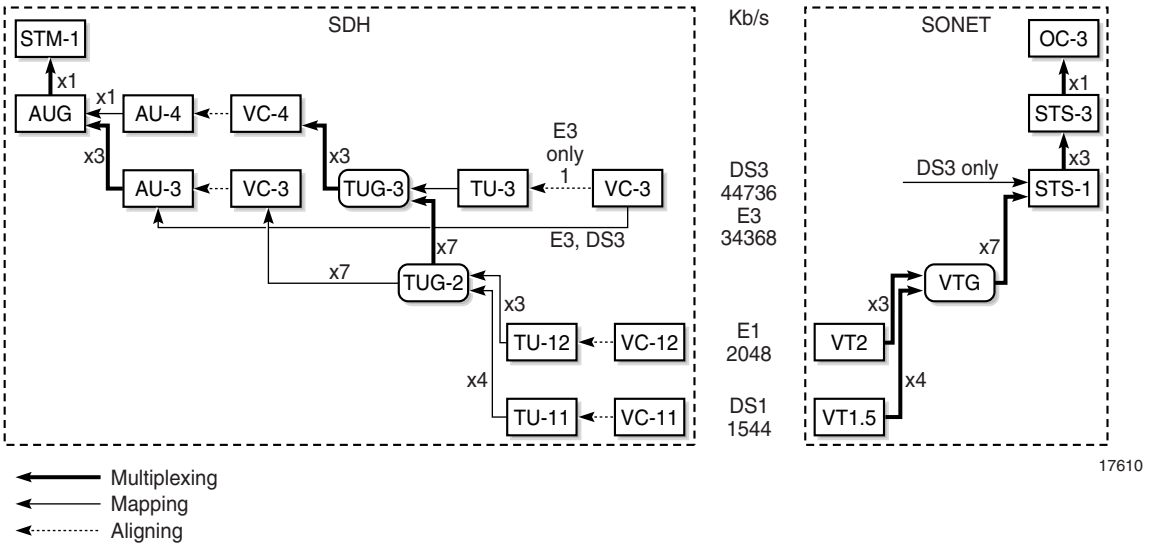
Comparison of SONET and SDH hierarchies

SONET and SDH are compatible digital hierarchies that support identical transmission rates with similar framing structures. However, SONET and SDH standards differ in the way they multiplex and map tributary payloads into higher digital levels. Because of these differences, some SDH framing blocks do not have equivalent blocks in SONET.

SONET provides one STS sub-channel, the STS-1, for mapping lower-capacity, deep-channel payloads while SDH provides two alternative sub-channels, the AU3 and the AU4. After an AU3 sub-channel is created, an AU4 cannot be created on that port in the case where the port is an OC-3 (STM-1). Conversely, if an AU4 sub-channel is created, an AU3 cannot be created on that port in the case where the port is an OC-3 (STM-1).

SONET and SDH transmission rates converge at 155.520 Mb/s where the SONET STS-3c is equivalent to the SDH STM-1 bit rate. For lower-capacity payloads, such as DS1, E1, DS3, and E3, SONET provides one unique mapping path for each payload while SDH permits two alternative paths for each payload as shown Figure 15-8.

Figure 15-8 Supported SONET/SDH multiplexing structures



SDH AU-4 and AU-3 sub-channel applications

SDH sub-channel applications allow you to create AU4 or AU3 channels on deep channelized OC-12 (STM-4) and OC-3 (STM-1) ports, and to configure multiple DS0 connection termination points.

After an AU4 sub-channel is created, it implicitly contains three TUG-3 groups. A TUG-3 is channelized to carry one of the following payload types:

- TU3
- TU11
- TU12

After an AU-3 sub-channel is created, it is channelized to carry one of the following payload types:

- DS3, E3
- TU11
- TU12

SDH TU3 payload

The following example, illustrated in Figure 15-9, shows the channelization sequence for a TU3 payload on a 4 × OC3 Deep Channel card.

1 Four OC-3 ports are created when you create a channelized 4 × OC3 Deep Channel card.

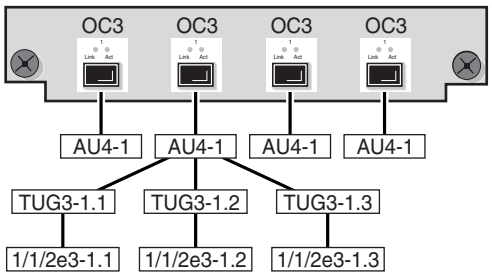
2 The user creates each required AU4 sub-channel.

3 Each AU4 sub-channel implicitly contains three TUG3 groups.

4 You can then configure each TUG3 to carry a TU3 frame

5 Each TU3 frame is channelized into an independent E3 data channel and cannot be changed.

Figure 15-9 Channelized 4 × OC-3 port structure using AU4/TU3 sub-channels



SDH E3 or DS3 payload

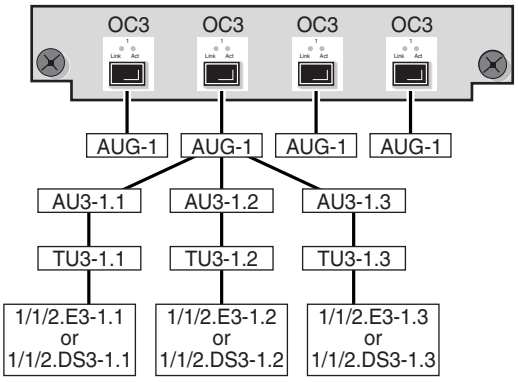
The following example, illustrated in Figure 15-10, shows the channelization sequence for an E3 or DS3 payload on a 4 × OC3 Deep Channel card using AU3 sub-channels.

1 Four OC-3 ports are created when you create a channelized 4 × OC3 Deep Channel card.

2 Each port can be channelized into up to three AU3 sub-channel.

3 Each AU3 frame can be channelized into an independent E3 or DS3 data channel.

Figure 15-10 Channelized 4 × OC-3 port structure using AU3/E3 sub-channels



SDH TU11 and TU12 payloads

TU11 and TU12 payloads can be channelized using an AU4 sub-channel or an AU-3 sub-channel. An AU4 sub-channel implicitly contains three TUG3 groups. A TUG3 and an AU3 channelized to carry TU11 or TU12 payloads implicitly contain seven TUG2 tributary groups.

The following example, illustrated in Figure 15-11, shows the channelization sequence for a TU11or a TU12 payload on a 4 × OC3 Deep Channel card.

1 Four OC-3 ports are created when you create a channelized 4 × OC3 Deep Channel card.

2 Each port can be channelized into one AU4 sub-channel or three AU3 sub-channels.

3 Each AU4 sub-channel implicitly contains three TUG3 groups.

4 You can then configure each TUG3 group or each AU3 sub-channel to carry a TU11 or TU12 payload.

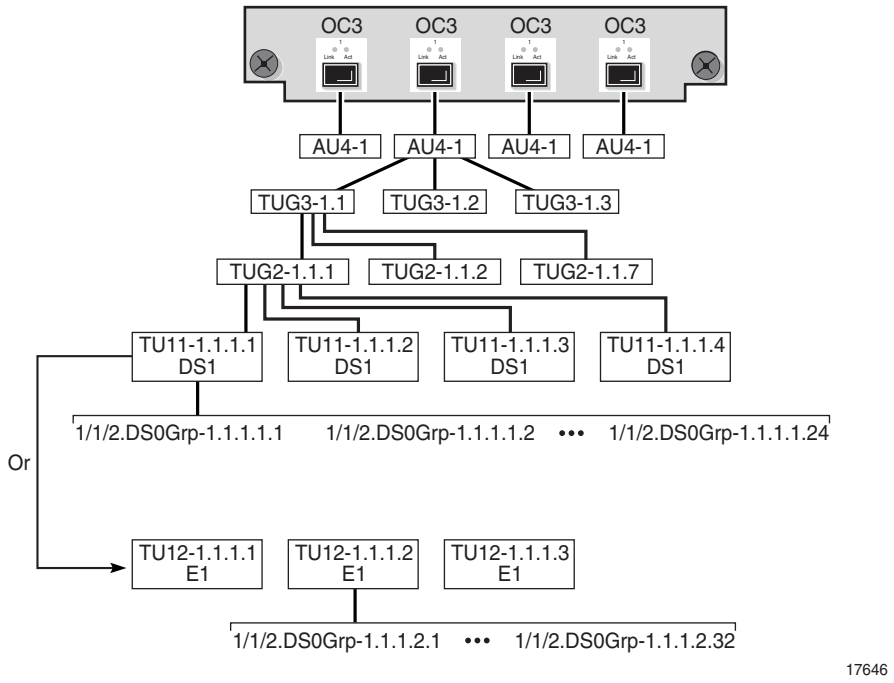
5 Each TUG3 group or AU3 sub-channel implicitly contains seven TUG2 tributary groups.

6 Each TUG2 group can be channelized into three independent TU12 channels or four independent TU11 channels.

7 Each TU12 can contain an E1 or DS1 data signal. Each TU11 can contain a DS1 data signal. Each E1 can be configured to handle up to 31 DS0 groups. Each DS1 can be configured to handle up to 24 DS0 groups. To use an E1 or a DS1, you must create at least one DS0 group for the DS1 or E1.

Note — On the same TUG3 or AU3, you cannot mix TU-1*X* with DS1 and E1 payload types. Every TU-1*X* on the same TUG3 or AU3 must use the same payload type, either E1 or DS1, not a mix of both. The mix is shown in for illustrating the structure.

Figure 15-11 Channelized 4 × OC-3 port structure using AU4/TU sub-channels



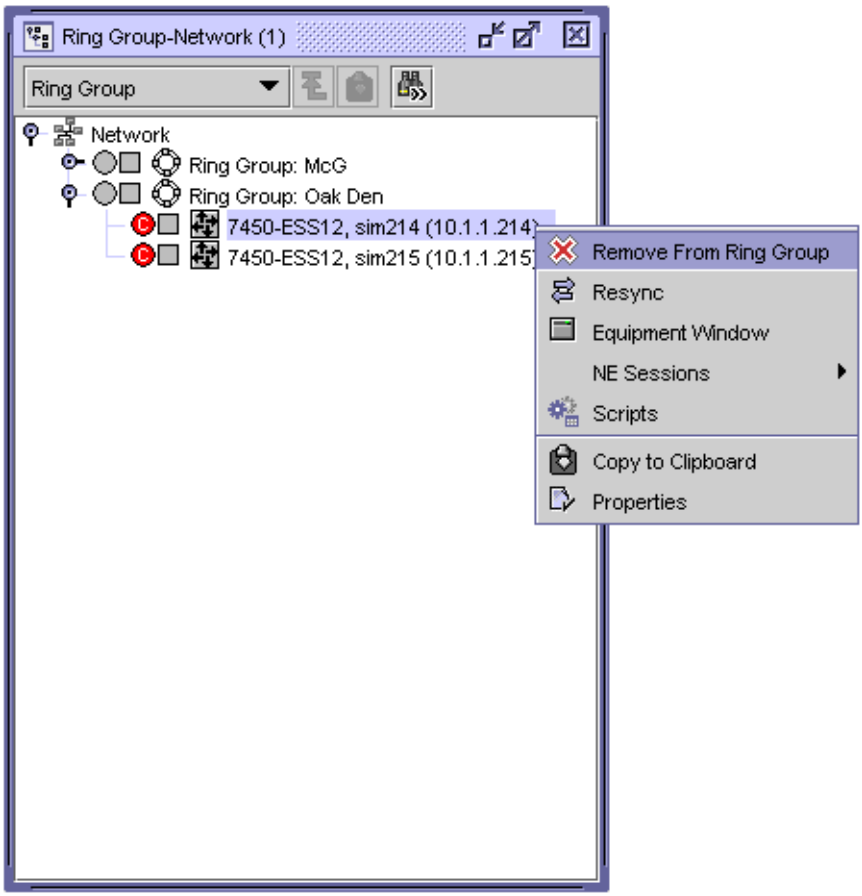
15.19 Working with ring group objects

The 5620 SAM allows you to create and manage ring groups in the ring group view of the navigation tree. Ring groups are used to group devices, such as Telco, 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESAs logically to represent a typical network topology.

Note — The 5620 SAM Release 7.0 R3 or later uses VLAN groups instead of ring groups to group OmniSwitch NEs. When you upgrade to 5620 SAM Release 7.0 R3 or later, a ring group that contains OmniSwitch NEs is automatically converted to a VLAN group. See chapter 66 for more information about VLAN groups.

In the ring group view of the navigation tree, the network icon provides the contextual menu option Create Ring Group to create ring group icons. Using the properties form of a ring group, you can group devices logically in the ring group. See chapter 17 for more information about creating and managing ring groups. Figure 15-12 shows a sample navigation tree ring group view.

Figure 15-12 Sample navigation tree ring group view



15.20 Working with physical links

The 5620 SAM allows you to create and manage links at the Layer 1 level. The physical links represent the actual physical configuration of network connections between ports. You can view and manage physical links from the equipment window, physical topology map, and the Manage Equipment list form.

Although there is no limit to the number of physical links you can have in a system, Alcatel-Lucent recommends a maximum of 10 000 physical links for optimal system performance.

Radio links between 9500 MPRs are shown as physical links by the 5620 SAM, with ports as the endpoint type.

See chapter 4 for information about configuring physical links and managing physical links using maps.

16 — Equipment window

16.1 Equipment window overview

The 5620 SAM equipment window allows network administrators and operators to do the following:

- filter different views and information for the managed devices using the equipment window filter
- view and use a graphical representation of the shelf to configure equipment objects and get statistical information about the nodes in their administrative domain
- view the services that traverse or terminate on equipment
- provision and pre-provision equipment to prepare the equipment for the creation of subscriber services
- view, configure, monitor the state of, and manage the following physical elements of the hardware:
  - a managed device
  - each device has one shelf, which is the physical shelf
  - up to 12 card slots where cards are inserted into the device
  - card slots contain cards
  - cards contain up to two daughter card slots, also known as I/O modules
  - each daughter card slot contains a daughter card
  - daughter cards contain ports
  - ports contain channels
  - up to 64 LAGs per managed device, a logical object which joins multiple Ethernet ports into a single port to aggregate bandwidth
  - up to eight CCAGs per managed device
  - up to four ISA-IPSEC groups per managed device
  - up to seven ISA-AA groups per managed device
  - up to four ISA-LNS groups per managed device
  - up to four ISA-Video groups per managed device
  - internal and external storage devices (flash memory)
  - physical links
  - OLC State
- configure network and access policies for network objects, such as ingress buffer policies for a port
- view and manage APS groups
- manage hardware fault conditions

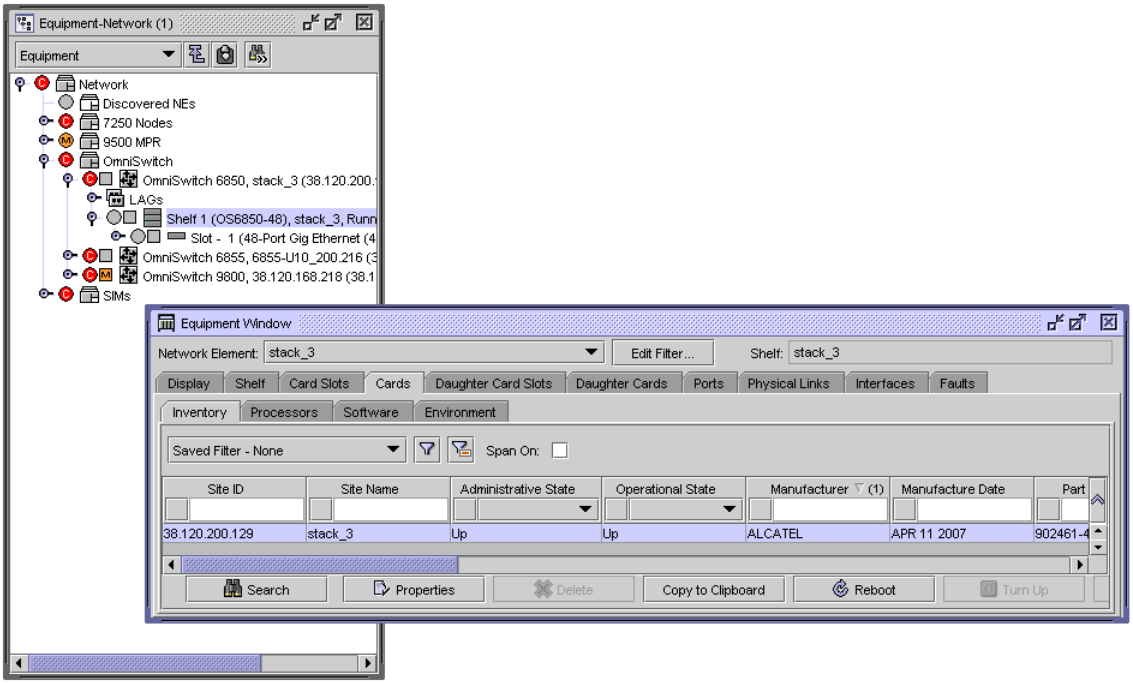
Equipment Window form

The equipment window provides a tab for each equipment component. Choose Application→Equipment Window from the 5620 SAM main menu to display the equipment component tabs.

Note — You can access the same tabs by right-clicking on the shelf in the equipment navigation tree and selecting the Equipment Window option in the contextual menu.

Figure 16-1 shows an example of the Equipment Window form displayed with the Card Slots tab displayed. The parameters displayed on each form are specific to the service that you are configuring. There are configurable and read-only parameters displayed from each tab. The read-only parameters are inherited from other configurations through device discovery.

Figure 16-1 Equipment Window form - Card Slots



Display tab

The Display tab displays a graphical representation of the device's shelf and its equipment components, such as the empty card slots and the cards that are installed on the device. You can double-click on an object under this tab to open its Properties configuration form. Right-click on the object and you have full access to the contextual menus for the object and any child objects, for example the ports of a card (dynamic graphical representation only).

Note — When you display a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA. or Telco device, the element manager for the device launches. The 5620 SAM permits users to launch the Telco element manager from the client GUI. This functionality is provided as a convenience to users, and is not part of the 5620 SAM. Contact Telco Systems for more information or support. See the appropriate device user guide for more information.

Shelf tab

The Shelf tab displays general information about the managed physical equipment.

The 7750 SR configurations include the following shelf types:

- 1-slot with five I/O slots that support two cards
- 7-slot with five I/O slots that support 10 cards. The slots are numbered from top to bottom.
- 12-slot with 10 I/O slots that support 20 cards. The slots are numbered from left to right.

The 7710 SR supports three slots, one of which is an I/O slot that supports up to 10 cards, depending on whether MDA carrier module support is enabled. The slots are numbered from top to bottom.

The 7705 SAR-8 supports three slots, one of which is an I/O slot that supports up to 6 cards.

The 7705 SAR-F supports an integrated IOM, 8-port Ethernet v3 MDA, and a 16-port DS1/E1 v2 ASAP MDA.

The 7450 ESS configurations include the following shelf types:

- 1-slot with one I/O slot that supports two cards
- 7-slot with six I/O slots that support 12 cards; the slots are numbered from top to bottom
- 12-slot with 10 I/O slots that support 20 cards; the slots are numbered from left to right

The 7210 SAS-E supports an integrated 2 x 12-Gig IOM card on a single chassis. The equipment navigation tree displays a card slot with one daughter card that contains 12 x 100/1000 Ethernet SFP ports and 12 x 10/100/1000 Ethernet ports.

The 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7210 SAS-X24F2XFP support an integrated 2 x 12-Gig IOM card on a single chassis. The equipment navigation tree displays a card slot with one daughter card that contains 24 x 10/100/1000 Ethernet SFP ports. In addition, the 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7210 SAS-X24F2XFP support 2 x 10 GigE XFP ports.

The 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA support one shelf type, a 1-slot I/O slot that supports five daughter cards.

The OS 6250 Enterprise version, OS 6850 and OS 6400 support up to 8 individual chassis that are connected as a stack. The OS 6250 Metro version supports up to 2 individual chassis that are connected as a stack. A single chassis or a stack appears in the navigation tree as Shelf 1; each chassis is assigned a slot from 1 to 8. There are several supported OS 6850 and OS 6400 chassis types; see the appropriate user documentation for more information.

The OS 6855 is a hardened Ethernet switch that offers up to 24 Gigabit copper and fiber ports. A single chassis or a stack appears in the navigation tree as Shelf 1; each chassis is assigned a slot from 1 to 4. There are several supported OS 6855 chassis types; see the OS 6855 user documentation for more information.

Note — The OS 6855 U24X is the stackable NE version. Up to four OS 6855 U24X NEs can be stacked and cannot be stacked with any other OmniSwitch NEs.

The OS 9600, OS 9700, OS 9800, OS 9700E, and OS 9800E chassis support plug-in CMM and Ethernet cards; see chapter 15 for more information on the supported CMM and Ethernet card types.

The 9500 MPR supports two shelf types; the MSS-4 and MSS-8. The MSS-4 supports four plug-in card slots and the MSS-8 supports eight plug-in card slots. Slots 1 and 2 of are dedicated to the core-enhanced card, slots 3 to 8 support the 32xDS1/E1 or radio modem cards. See "9500 MPR support" in section 11.1 for more information about the 9500 MPR.

The Shelf tab displays shelf information and chassis environment data, including the temperature, fans, power supplies, LEDs, storage, and fault information.

- The Shelf tab displays information about the managed device, including the site ID, shelf part number, equipment location codes, shelf type, base MAC address, total available slots, and the number of installed ports.
- The Fan Trays tab displays information about each fan tray. Double-click on a row in the fan tray list to view additional information, such as operational state and speed.
- The Power Supply Trays tab displays information about the router power supply, including voltage and temperature.
- The LED Panels tab displays the status of LEDs on the device, including the number of critical, major, and minor LEDs currently showing on the device.
- The Flash Memory tab displays information about the flash memory installed on the device. Double-click on a row representing the flash memory to view additional information, including the serial number, firmware revision, capacity, and percentage of flash memory used.
- The Cross Connects tab lists all of the cross-connects on a 9500 MPR.
- The Port Segregation tab lists ports that are configured as segregated ports on a 9500 MPR. When a port is segregated, the port cannot be part of a cross-connection. See Procedure 17-70 for information about configuring 9500 MPR port segregation.
- The Software Bank Details tab list the standby and committed software banks for a 9500 MPR. See Procedure 17-50 for information about managing 9500 MPR running software.
- The Hardware Environment tab displays the current and threshold temperature settings of the configured cards.
- The Statistics tab displays CPU and memory statistics.

Card Slots tab

The Card Slots tab displays the cards that are installed on or provisioned for the node, the supported card type for each slot, and fault information. To pre-provision a slot, the allowed card types, and the line card must be specified.

- The Inventory tab displays cards configured in the slots.
- The Supported Card Types tab indicates the types of cards that can be configured for the slots.

Cards tab

The Cards tab has several tabs to display the line or system daughter cards, also called IOM cards, that are installed on, pre-provisioned, or provisioned for the node.

- The Inventory tab displays the card type, serial number, revision number, and equipment state.
- The Processors tab displays information about the two processors Control cards, also called the CPM or switch fabric cards. Double-click on the A or B slot Control card for information about the control processors and switch fabric processors.
- The Software tab displays the card version, boot code information, and state.
- The Environment tab displays card environment information, for example, temperature thresholds.

Daughter Card Slots tab

The Daughter Card Slots tab displays the daughter cards that are provisioned for the node, the supported daughter card types, and fault information. To pre-provision a daughter card slot, the slot, and daughter card types must be specified before the daughter card is configured.

Choose a specific daughter card type for the slot. The daughter card can be pre-provisioned but a daughter card must be provisioned before ports can be configured. Ports can be configured when the daughter card is properly provisioned.

Up to two daughter cards can be provisioned on an IOM. Only one daughter card can be provisioned per IOM daughter card slot. To modify a daughter card slot, shut down all port associations.

The additional daughter card slots tabs include:

- The Inventory tab lists the daughter card slots and the daughter cards configured for the slots.
- The Supported Daughter Card Types tab lists the types of cards allowed and supported in each daughter card slot.

Daughter Cards tab

The Daughter Cards tab displays daughter card information, including the daughter card slot ID, daughter card types, serial numbers, manufacture date, hardware revision, administrative and operational states, network ingress buffer policy ID, and fault information.

The additional daughter card tabs include:

- The Inventory tab lists the daughter cards configured for the slots. Double-click on a row representing the daughter card to view the properties form for the card, including ports configured on the daughter card
- The Environment tab lists temperature information for each daughter card.

Ports tab

The Ports tab displays information about physical ports, SONET or SDH channels, TDM channels, link aggregation groups, protocols, APS groups, and faults. Double-click on a row to open the properties form for the port.

For each network and access port, you can view and configure parameters using the tab buttons. See chapter 17 for more information about configuring properties.

- The Physical Ports tab lists all ports on the configured daughter card. Double-click on a row to open the properties form for the physical port.
- The SONET Channels tab lists all channels on the configured daughter card ports. Double-click on a row to open the properties form for the channel.
- The Link Aggregation Group tab lists all LAGs on the configured daughter card ports. Double-click on a row to open the properties form for the LAG.
- The Protocols tab lists the ID and the running protocols, for example, IPv4 or MPLS, on the configured daughter card ports.
- The Terminations tab lists the number of connections on each endpoint, the encapsulation type of the endpoint, and bandwidth usage information. Terminations on SONET channels of 1 x 10-Gig MDAs are not supported.
- The TDM Channels tab lists all channels on the configured daughter card port. Double-click on a row to open the properties form for the channel.
- The Multilink Bundles tab lists all multilink bundles on the configured daughter cards. Double-click on a row to open the properties form for the multilink bundle.
- The APS Groups tab lists the APS groups to which the ports belong.

Physical Links tab

The Physical Links tab displays physical link information, including the physical link ID, description, operational state, type, fault management, any notes entered by the user about the link, and the ports that form the endpoints of the link. If endpoint B is an unmanaged device, and the ID and IP address of the unmanaged device are also displayed.

Interfaces tab

The Interfaces tab displays the interfaces that are configured for the port, including the device interfaces and the IP addresses. You can select the interface and click Edit to reconfigure the interface.

The interfaces tabs include:

- The Network Interfaces tab lists the ports configured for network access.
- The L2 Interfaces tab lists the ports and channels configured as Layer 2 interfaces, and the services using those Layer 2 interfaces.
- The L3 Interfaces tab lists the ports and channels configured as Layer 3 interfaces, and the services using those Layer 3 interfaces.
- The Address tab lists routing instance information for Layer 3 interfaces and other network interfaces, including the system IP address.

Faults tab

The Faults tab has several tabs to display alarm information for the device.

- The Object Alarms tab displays information about the alarm as viewed from the dynamic alarm list.
- The Affecting Alarms tab displays a list of the alarms on objects that are directly affecting this object.
- The Aggregated Alarms tab displays a list of all alarms for objects below the listed object in the containment hierarchy.
- The Alarms on Related Objects tab displays a list of all alarms that have an indirect relationship with the object.

16.2 Workflow to manage equipment using the equipment window

1 Ensure the routers are configured before they are discovered by the 5620 SAM.

2 Access the equipment and begin configuration and management.

  i Choose Application→Equipment Window from the 5620 SAM main menu.

  ii Use the equipment window to edit or view objects and configuration parameters.

  iii Edit the properties of objects as required in equipment window.

16.3 Equipment window procedures

Use the following procedures to manage equipment using the equipment window.

Procedure 16-1 To use the equipment window filter

The Equipment Window Filter form filters the display of the Equipment Window form based on device properties. You can use the Equipment Window Filter form to quickly see a snapshot of various selected parameters, or click on the OK button of the Simple filter to view or edit all the forms and configured parameters in the equipment window for the managed device.

1 Choose Application→Equipment Window from the 5620 SAM main menu.

  The Equipment Window Filter and Equipment Window forms are displayed.

2 You can close the filter form or create a filter.

  a Click on the OK button to close the filter form and access the Equipment Window form.

    The Equipment Window Filter form closes and the Equipment Window form is brought to the foreground.

  b Configure the filter criteria.

The Equipment Window Filter form closes and the Equipment Window form is brought to the foreground.

3 Select a managed device using the Network Element parameter.

Procedure 16-2 To change the configuration of devices using the equipment window

An object must be created before it can be configured. A created object is seen in the navigation tree. See chapter 17 for more information about using the navigation tree.

1 Right-click on a discovered device in the navigation tree and choose Equipment Window from the contextual menu.

The Equipment Window Filter and Equipment Window forms are displayed.

Note — When you display a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device, the element manager for the device launches. See the appropriate user guide for the device for more information.

2 Select the filter type and filtered properties, as described in Procedure 16-1.

3 Click on the OK button.

The 5620 SAM displays a graphical representation of the shelf under the Display tab.

4 Choose tabs to configure the equipment parameters in the sequence displayed.

a Double-click on any of the slots displayed under the Display tab to open the Properties form for the slot and create or edit the parameters of an object in the shelf.

b Select a parameter in any of the form lists and click on the Properties button to configure the parameter.

c Double-click on any object in any form to show the object Properties form.

5 Save the configuration changes, as required.

17 — Equipment navigation tree

17.1 Navigation tree overview

The view selector in the 5620 SAM navigation tree is a drop-down menu that lists the physical and logical network views that are available. You can use the contextual menu for an object in the navigation tree to create, configure, and manage specific parameters for the object and child objects. You can choose the following views:

- Equipment—displays the physical objects that the 5620 SAM manages
- OSPF—displays the OSPF objects in the network
- IS-IS—displays the OSPF objects in the network
- Routing—displays the device routing instances and child objects such as the network interfaces and the configured protocols
- Ring Group—displays the ring group objects that the 5620 SAM manages

Table 17-1 describes the objects in the equipment view of the navigation tree that the 5620 SAM allows you to create and manage.

Table 17-1 5620 SAM navigation tree object descriptions — Equipment view

Object	Description
Routing	Contains the routers, devices, and topology groups, including the default Discovered NEs topology group
Router, device, topology group	The second level in the hierarchy
CCAG, ISA-AA groups, ISA-IPsec groups, ISA-LNS groups, ISA-NAT groups, ISA-Video groups, LAG, IGH, shelf	The third level in the hierarchy
APS groups	Located under the shelf object; contain the APS groups for a device
Card	Located under the shelf object
Daughter card	A child object of the card object
Bundles	A child object of the daughter-card object; a group of DS0 channels on a SONET- or TDM-capable daughter card
Port	A child object of the daughter-card object
Channel, sub-channel, timeslot	Child objects of the port object

You can use the following methods to view and manage objects in the 5620 SAM navigation tree:

- Double-click on an object or press the + key when the object is selected to open the object and to display the child objects.
- Double-click on an object or press the - key when the object is selected to close the object and to hide the child objects.

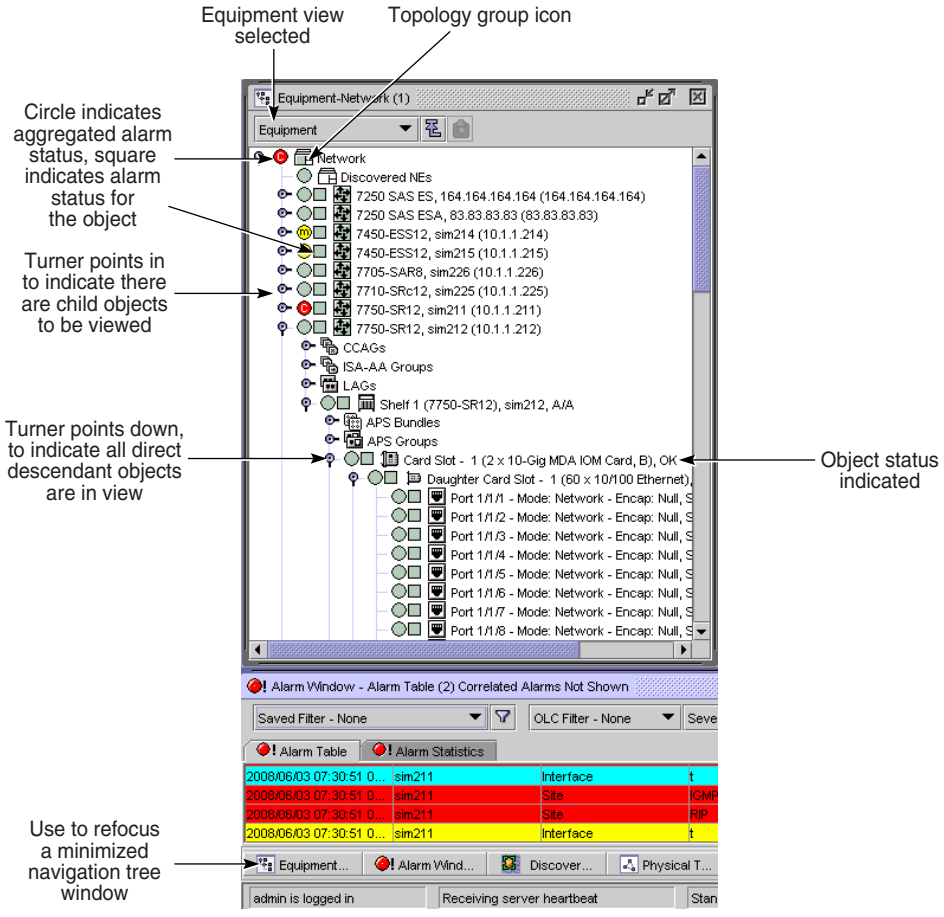
- Click on an object and use the cursor keys to navigate the object hierarchy. In the Equipment view, for example, you can navigate from the device to the ports and channels.
- Right-click on an object to open the contextual menu and choose a function. The menu options are specific to the object type.

Note — Keyboard-based navigation-tree operations may not function as expected when you open the client GUI using a third-party access tool, for example, a Citrix server.

The navigation tree uses color highlights to display object status information such as the current alarm level and the aggregated alarm status. The operational and administrative states of an object are displayed in text form beside the object icon, as are the object type and description.

Figure 17-1 shows some of the navigation tree objects that you can manage using the Equipment view.

Figure 17-1 5620 SAM navigation tree objects - Equipment view



18030

Contextual menus for navigation-tree objects

Each object in the 5620 SAM navigation tree has a contextual menu that opens when you right-click on the object. You can use the contextual menus to do the following:

- create objects
- configure object properties
- perform maintenance functions
- change the state of objects
- open a different management interface, for example, a CLI
- designate an object as the root object in the navigation tree

Equipment view contextual menus

The following describes the contextual menu options for each object in the navigation tree hierarchy of the equipment view:

- The contextual menu options for a network include:
  - Create Group

    The Create Group contextual menu option opens the Group (Create) form to create a topology group in the equipment view of the navigation tree and on the appropriate topology maps.
  - Properties

    The Properties contextual menu option opens the Group (Edit) form. This form displays read-only information and configurable parameters. Using the Copy button, you can create additional topology groups in the network based on existing parameter information.
- The contextual menu options for a device include:
  - Add to Ring Group

    The Add to Ring Group menu option specifies whether to add the device to a group.
  - Resync

    The Resync menu option specifies that SNMP MIB and CLI information bases are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Equipment Manager

    The Equipment Manager option opens the 5620 SAM Equipment Manager. The information for the selected device is displayed.
  - NE Sessions

    The NE Sessions option opens a Telnet session, an SSH session, an FTP file browser session, or an SSH file browser session on the selected device.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected device as the root of the tree.
  - Make Root

    The Make Root option makes the selected device the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the property form for the chosen object. This form displays read-only information and configurable parameters.

- The contextual menu options for a generic NE include:
  - Resync

    The Resync menu option specifies that SNMP MIB bases are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - NE Sessions

    The NE Sessions option opens a Telnet session, an SSH session, an FTP file browser session, or an SSH file browser session on the selected device.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected device as the root of the tree.
  - Make Root

    The Make Root option makes the selected device the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the property form for the chosen object. This form displays read-only information and configurable parameters.
  - Open URL

    The Open URL option opens the Web browser to manage the GNE.
- The contextual menu options for the default topology group Discovered NEs include:
  - List

    The List option opens the Discovered NEs form with a list of newly discovered NEs.
- The contextual menu options for a topology group include:
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected topology group as the root of the tree.
  - Make Root

    The Make Root option makes the selected topology group the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the properties form for the selected object. This form displays read-only information and configurable parameters.
- The contextual menu options for CCAGs include:
  - Create CCAG

    The Create CCAG option opens the CCAG (Create) form, which allows you to create a cross-connect aggregation group. You define CCAG properties, configure CCAG parameters, and configure CCAG members.
- The contextual menu options for IGHs include:
  - Create IGH

    The Create IGH option opens the IGH (Create) form, which allows you to create an IGH. You define IGH properties, and configure IGH subgroups and members.

- The contextual menu options for IGH groups include:
  - Resync

    The Resync menu option specifies that MIB tables are re-read to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not affect the contents of the historical statistics database.
  - Create IGH Members

    The Create IGH Members option opens the Create IGH Member configuration form which allows you to configure IGH member ports.
  - Turn Up

    The Turn Up option specifies that the IGH group is changed to administratively up.
  - Shut Down

    The Shut Down option specifies that the IGH group is changed to administratively down.
  - Delete

    The Delete option deletes the IGH group but you must delete the IGH members before deleting the IGH group.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected IGH group as the root of the tree.
  - Make Root

    The Make Root option makes the selected IGH group the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the IGH (Edit) form which allows you to configure IGH parameters, and add IGH subgroups and members.
- The contextual menu options for an IGH members include:
  - Resync

    The Resync menu option specifies that MIB tables are re-read to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not affect the contents of the historical statistics database.
  - Delete

    The Delete option deletes the IGH member.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected IGH member as the root of the tree.
  - Make Root

    The Make Root option makes the selected IGH member the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the IGH Member (Edit) form which allows you to view IGH member parameters.
- The contextual menu options for ISA-AA groups include:
  - Create ISA-AA Group

    The Create ISA-AA Group option opens the ISA-AA Group (Create) form, which allows you to create an ISA-AA group and ISA-AA partitions. You define ISA-AA group and ISA-AA partition properties, configure ISA-AA group and ISA-AA partition parameters, and specify ISA-AA members.

- The contextual menu options for ISA-IPsec groups include:
  - Create ISA-IPsec Group

    The Create ISA-IPsec Group option opens the ISA-IPsec Group (Create) form, which allows you to create an ISA-IPsec group. You define ISA-IPsec properties, configure ISA-IPsec parameters, and specify ISA-IPsec members.
- The contextual menu options for ISA-LNS groups include:
  - Create ISA-LNS Group

    The Create ISA-LNS Group option opens the ISA-LNS Group (Create) form, which allows you to create an ISA-LNS group. You define ISA-LNS properties, configure ISA-LNS parameters, and specify ISA-LNS group members.
- The contextual menu options for ISA-LNS groups include:
  - Create ISA-NAT Group

    The Create ISA-NAT Group option opens the ISA-NAT Group (Create) form, which allows you to create an ISA-NAT group. You define ISA-NAT properties, configure ISA-NAT parameters, and specify ISA-NAT group members.
- The contextual menu options for ISA-Video groups include:
  - Create ISA-Video Group

    The Create ISA-Video Group option opens the ISA Video Group (Create) form, which allows you to create an ISA-Video group. You define ISA-Video properties, configure ISA-Video parameters, and specify ISA-Video group members.
- The contextual menu options for LAGs include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Create LAG

    The Create LAG option opens the Create LAG configuration form. You define LAG properties, configure LAG parameters, configure LAG subgroups and members, and configure LACP.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected LAG as the root of the tree.
  - Make Root

    The Make Root option makes the selected LAG the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the LAGs (Edit) form where you configure the LACP System Priority parameter.

- The contextual menu options for a LAG group include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Create LAG Members

    The Create LAG Members option opens the Create LAG Member configuration form where you define LAG member ports.
  - Turn Up

    The Turn Up option specifies that the LAG group is changed to administratively up.
  - Shut Down

    The Shut Down option specifies that the LAG group is changed to administratively down.
  - Delete

    The Delete option deletes the LAG group and everything contained in the LAG group.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected LAG group as the root of the tree.
  - Make Root

    The Make Root option makes the selected LAG group the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the LAG (Edit) form where you configure LAG properties, configure LAG parameters, add LAG subgroups and members, configure LACP, configure access parameters, and create network interfaces.
- The contextual menu options for a MC LAG include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Turn Up Peer

    The Turn Up Peer option specifies that the MC peer is changed to administratively up.
  - Shut Down Peer

    The Shut Down Peer option specifies that the MC peer is changed to administratively down.
  - Turn Up MC LAG

    The Turn Up MC LAG option specifies that the MC LAG is changed to administratively up.
  - Shut Down MC LAG

    The Shut Down MC LAG option specifies that the MC LAG is changed to administratively down.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected MC LAG as the root of the tree.
  - Make Root

    The Make Root option makes the selected MC LAG the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the MC Peer (Edit) form where you configure MC peer properties and configure MC LAG members and MC synchronization protocols.

- The contextual menu options for a MC LAG Member include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected MC LAG member as the root of the tree.
  - Make Root

    The Make Root option makes the selected MC LAG member the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the MC LAG Member (Edit) form where you configure MC LAG identifiers and remote LAG properties.
- The contextual menu options for a shelf include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Reboot

    The Reboot option specifies that all cards in the chassis are re-initialized.
  - Force Mode

    The Force Mode menu option forces an upgrade of the hardware.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected shelf as the root of the tree.
  - Make Root

    The Make Root option makes the selected shelf the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the Shelf (Edit) form where you can view and edit properties contained in the shelf. You can view general properties for the shelf, such as fan trays, power supply trays, and LED panels. You can also view and change the chassis mode and the properties for objects that are contained in the shelf, such as hardware environment, card slots, timing, statistics policies, and faults.
- The contextual menu options for the APS Groups object include:
  - Create APS Group

    The Create APS Group menu option opens the APS Group (Create) form that allows you to create and manage APS groups on the shelf.
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected APS Groups object as the root of the tree.
  - Make Root

    The Make Root option makes the selected APS Groups object the root of the navigation tree. The default root is the network.

- The contextual menu options for the APS Group object include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Create APS Working Channel

    The Create APS Working Channel menu option opens the APS Channel, Working (Create) form that allows you to create and manage APS working channels.
  - Create APS Protection Channel

    The Create APS Protection Channel menu option opens the APS Channel, Protection (Create) form that allows you to create and manage APS protection channels.
  - Create APS SONET Channel

    The Create APS SONET Channel menu option opens the SONET Channel (Create) form that allows you to create the APS common configuration.
  - Delete

    The Delete option deletes the APS group and everything contained in the APS group.
  - Turn Up

    The Turn Up option specifies that the APS group is changed to administratively up.
  - Shut Down

    The Shut Down option specifies that the APS group is changed to administratively down.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected APS Group object as the root of the tree.
  - Make Root

    The Make Root option makes the selected APS Group object the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the properties form for the selected object. This form displays read-only information and configurable parameters.

- The contextual menu options for the MC APS Group Member object include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Create APS Working Channel

    The Create APS Working Channel menu option opens the APS Channel, Working (Create) form that allows you to create and manage APS working channels.
  - Create APS Protection Channel

    The Create APS Protection Channel menu option opens the APS Channel, Protection (Create) form that allows you to create and manage APS protection channels.
  - Create APS SONET Channel

    The Create APS SONET Channel menu option opens the SONET Channel (Create) form that allows you to create the APS common configuration.
  - Delete

    The Delete option deletes the APS group and everything contained in the APS group.
  - Turn Up

    The Turn Up option specifies that the APS group is changed to administratively up.
  - Shut Down

    The Shut Down option specifies that the APS group is changed to administratively down.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected APS Group object as the root of the tree.
  - Make Root

    The Make Root option makes the selected APS Group object the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the properties form for the selected object. This form displays read-only information and configurable parameters.
- The contextual menu options for the APS Channel object include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Delete

    The Delete option deletes the APS channel and everything contained in the APS channel.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected APS Channel object as the root of the tree.
  - Make Root

    The Make Root option makes the selected APS Channel object the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the properties form for the selected object. This form displays read-only information and configurable parameters.

- The contextual menu options for the APS Bundles object include:
  - Create Bundle

    The Create Bundle option opens the APS Bundle Display configuration form, which allows you to create a group of DS0 channel groups on a channelization-capable MDA to provide bi-directional APS protection on IMA bundles. You configure bundle parameters and add bundle members.
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the device. Resynchronization does not impact the contents of the historical statistics database.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the APS bundle as the root of the tree.
  - Make Root

    The Make Root option makes the APS bundle as the root of the navigation tree. The default root is the network.
- The contextual menu options for the APS Bundle object include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the device. Resynchronization does not impact the contents of the historical statistics database.
  - Create APS Working Bundle

    The Create APS Working Bundle menu option opens the Create Multilink Bundle form, which allows you to create and manage APS working bundles. You must create an APS working bundle before you can create an APS protection bundle or add members to the APS bundle.
  - Create APS Protection Bundle

    The Create APS Protection Bundle menu option opens the Create Multilink Bundle form, which allows you to create and manage APS protection bundles. You must create an APS working bundle before you can create an APS protection bundle or add members to the APS bundle.
  - Create Bundle Members

    The Create Bundle Members option opens the Add Bundle Member form, which allows you to add members to an APS bundle.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the APS bundle as the root of the tree.
  - Make Root

    The Make Root option makes the APS bundle as the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the properties form for the selected object. This form displays read-only information and configurable parameters.

- The contextual menu options for the SC APS Bundle object include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the device. Resynchronization does not impact the contents of the historical statistics database.
  - Create APS Working Bundle

    The Create APS Working Bundle menu option opens the Create Multilink Bundle form, which allows you to create and manage APS working bundles. You must create an APS working bundle before you can create an APS protection bundle or add members to the APS bundle.
  - Create APS Protection Bundle

    The Create APS Protection Bundle menu option opens the Create Multilink Bundle form, which allows you to create and manage APS protection bundles. You must create an APS working bundle before you can create an APS protection bundle or add members to the APS bundle.
  - Create Bundle Members

    The Create Bundle Members option opens the Add Bundle Member form, which allows you to add members to an APS bundle.
  - Delete

    The Delete option deletes the APS common configuration from the APS group.
  - Turn Up

    The Turn Up option specifies that the APS common configuration is changed to administratively up.
  - Shut Down

    The Shut Down option specifies that the APS common configuration is changed to administratively down.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the APS bundle as the root of the tree.
  - Make Root

    The Make Root option makes the APS bundle as the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the properties form for the selected object. This form displays read-only information and configurable parameters.
- The contextual menu options for the MC APS Bundle object include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the device. Resynchronization does not impact the contents of the historical statistics database.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the APS bundle as the root of the tree.
  - Make Root

    The Make Root option makes the APS bundle as the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the properties form for the selected object. This form displays read-only information and configurable parameters.

- The contextual menu options for the APS Common Config SONET Channel object include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Delete

    The Delete option deletes the APS common configuration from the APS group.
  - Turn Up

    The Turn Up option specifies that the APS common configuration is changed to administratively up.
  - Shut Down

    The Shut Down option specifies that the APS common configuration is changed to administratively down.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected APS common configuration as the root of the tree.
  - Make Root

    The Make Root option makes the selected APS common configuration as the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the properties form for the selected object. This form displays read-only information and configurable parameters.
- The contextual menu options for a card slot include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Configure Card

    The Configure Card option opens the Create Card properties form that allows you to create a card configuration for the slot. You assign a supported card type to the slot. The options available are displayed with check marks beside them in the Supported Card Types parameter. The Equipped Card Type displays the card type that is physically in the slot. When there is a mismatch between the Equipped Card Type and the Assigned Card Type, a check mark appears in the Card Mismatch box. When the configured card types are correct, you can change the Administrative State as required.
  - Shut Down

    The Shut Down option specifies that the card slot is changed to administratively down.
  - Turn Up

    The Turn Up option specifies that the card slot is changed to administratively up.
  - Remove Card

    The Remove Card option deletes the card from the slot when the slot and everything contained in the slot is changed to administratively down.
  - Soft Reset

    The Soft Reset option resets the card. A soft reset is preferable to a reboot, as it results in minimal downtime. A soft reset causes the card to stop all processes it is running and restart.
  - Reboot

    The Reboot option specifies that all cards in the chassis are re-initialized.

- Make Root In New Tree

  The Make Root In New Tree option opens another navigation tree window with the selected card as the root of the tree.
- Copy to Clipboard

  The Copy to Clipboard option copies the MDA information to the clipboard.
- Make Root

  The Make Root option makes the selected card the root of the navigation tree. The default root is the network.
- Properties

  The Properties option opens the Card Slot (Edit) form where you can view and change properties contained in the card slot. After the card object is created, you can use the properties option on the slot to view, edit, and create all the properties that can be contained in the card slot, for example daughter cards and ports.

- The contextual menu options for a daughter card slot include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the device. Resynchronization does not impact the contents of the historical statistics database.
  - Configure Daughter Card

    The Configure Daughter Card option opens the Daughter Card (Create) form that allows you to create a daughter card configuration for the slot. You assign a supported daughter card type to the daughter card slot. The options are displayed with check marks beside them in the Supported Daughter Card Types area of the form. The Equipped Daughter Card Type displays the daughter card type that is physically in the slot. When there is a mismatch between the Equipped Daughter Card Type and the Assigned Daughter Card Type, a check mark appears in the Daughter Card Mismatch box. When the configured card types are correct, you can change the Administrative State as required.
  - Shut Down

    The Shut Down option specifies that the daughter card slot is changed to administratively down.
  - Turn Up

    The Turn Up option specifies that the daughter card slot is changed to administratively up.
  - Delete

    The Delete option deletes the daughter card from the slot when the slot and everything contained in the slot is changed to administratively down.
  - Reboot

    The Reboot option specifies that all MDAs in the chassis are re-initialized.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected daughter card as the root of the tree.
  - Make Root

    The Make Root option makes the selected daughter card the root of the navigation tree. The default root is the network.
  - Copy to Clipboard

    The Copy to Clipboard option copies the MDA information to the clipboard.
  - Properties

    The Properties option opens the Daughter Card Slot (Edit) form. You can view and change properties in the daughter card slot. After the daughter card object is created, you can use the properties option on the slot to view, modify, and create all the properties that can be contained in the slot, for example, daughter cards and the QoS Pool for the daughter card slot.

- The contextual menu options for the Bundles object include:
  - Create Bundle

    The Create Bundle option opens the Create Multilink Bundle configuration form which allows you to create a group of DS0 channel groups on a channelization-capable MDA. Creating a multilink bundle provides a mechanism to distribute data across multiple links to achieve higher bandwidth on a SAP. You can create IMA group bundles on channelized ASAP MDAs. You configure bundle parameters and add bundle members.
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the device. Resynchronization does not impact the contents of the historical statistics database.
- The contextual menu options for bundles include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the device. Resynchronization does not impact the contents of the historical statistics database.
  - Create Bundle Members

    The Create Bundle Members option opens the Add Bundle Member configuration form that allows you to add members to a multilink bundle.
  - Delete

    The Delete option deletes the bundle when everything contained in the port is changed to administratively down.
  - Shut Down

    The Shut Down option specifies that the bundle is changed to administratively down.
  - Turn Up

    The Turn Up option specifies that the bundle is changed to administratively up.
  - Make Root

    The Make Root option makes the selected bundle the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the properties form. You can view and change properties for the bundle, or view and modify bundle members.

- The contextual menu options for ports include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the device. Resynchronization does not impact the contents of the historical statistics database.
  - Create Channel

    The Create Channel option allows you to create channels on ports with available channels.
  - Create All Channels

    The Create All Channels option allows you to automatically create all of the channels on ports with available channels. This option is available for OC12, OC3, and DS3 and E3 ASAP ports.
  - Create Interface

    The Create Interface option is available for CES ports on the 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA. This option allows you to create an interface for a TDM line, such as E1 or T1, for backhauling the TDM signal through the IP/MPLS network.
  - Shut Down

    The Shut Down option specifies that the port is changed to administratively down.
  - Turn Up

    The Turn Up option specifies that the port is changed to administratively up.
  - Delete

    The Delete option deletes the port when everything contained in the port is changed to administratively down.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected port as the root.
  - Make Root

    The Make Root option makes the selected port the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the properties form. You can view and change properties contained in the port. Port objects are automatically created when the daughter card object is created. Use the properties option on the slot to view, change, and create all the properties that can be contained in the slot, for example, SONET channels.

- The contextual menu options for channels include:
  - Resync

    The Resync menu option specifies that MIB tables are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the device. Resynchronization does not impact the contents of the historical statistics database.
  - Delete

    The Delete option deletes the channel when all objects contained in the channel are changed to administratively down.
  - Shut Down

    The Shut Down option specifies that the channel is changed to administratively down.
  - Turn Up

    The Turn Up option specifies that the channel is changed to administratively up.
  - Make Root In New Tree

    The Make Root In New Tree option opens another navigation tree window with the selected channel as the root.
  - Make Root

    The Make Root option makes the selected channel the root of the navigation tree. The default root is the network.
  - Properties

    The Properties option opens the properties form. You can view and change properties contained in the channel.

Ring group view contextual menus

The following describes the contextual menu options for each object in the navigation tree hierarchy of the ring group view:

- The contextual menu option for a network is Create Ring Group, which is used to group devices to be able to create VLAN or VPLS ring groups.
- The contextual menu options for a ring group include:
  - Remove Ring Group

    The Remove Ring Group option removes the specified ring group. The devices contained in the ring group are not deleted; they remain in the equipment view of the navigation tree.
  - Properties

    The Properties option opens the Ring Group (Edit) form. You can view and modify properties for the ring group, or view and modify ring group members.

- The contextual menu options for a device in a ring group include:
  - Remove From Ring Group

    The Remove From Ring Group option removes the specified device from the ring group. The devices are not deleted; they remain in the equipment view of the navigation tree.
  - Resync

    The Resync menu option specifies that SNMP MIB and CLI information are reread to resynchronize them with the 5620 SAM, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.
  - Equipment Manager

    The Equipment Manager option launches the 5620 SAM equipment manager.
  - NE Sessions

    The NE Sessions option opens a Telnet session, an SSH session, an FTP file browser session, or an SSH file browser session with the selected device in the equipment view of the navigation tree.
  - Properties

    The Properties option opens the property form. You can view and modify properties for the device.

17.2 Workflow to manage equipment using the navigation tree

1. Use the 5620 SAM to discover the device.
2. Right-click on the Discovered NEs topology group in the Equipment view of the navigation tree and choose List from the contextual menu, or double-click on the Discovered NEs icon on the topology map to open the Discovered NEs form.
3. Choose the discovered NEs and drag and drop them to the network icon in the equipment view of the navigation tree or to the topology map.
4. Right-click on the object in the navigation tree to open the contextual menu.
5. Choose an option. See section 17.1 for a list of contextual menu options.
6. Configure the parameters, as required.
   - i. Edit the device parameters as required using the Properties option from the contextual menu.
   - ii. Create card objects in the shelf using the Properties option from the contextual menu in the equipment view.
   - iii. Create daughter card objects in the card objects using the Properties option from the contextual menu in the equipment view.
   - iv. View the parameters of the port objects that were created automatically with the daughter card object using the Properties option from the contextual menu in the equipment view.
   - v. Edit the parameters of the created objects as required using the Properties option from the contextual menu in the equipment view.
   - vi. Create channel objects on the SONET/SDH and TDM ports using the Properties option from the contextual menu in the equipment view.

vii Edit the channel parameters as required using the Properties option from the contextual menu in the equipment view.

viii Group DS0 channels together on an MDA to achieve higher bandwidth using the Create Multilink Bundle configuration form from the contextual menu in the equipment view.

17.3 Navigation tree equipment management procedures list

Table 17-2 lists the procedures to configure equipment using the navigation tree.

Table 17-2 5620 SAM navigation tree equipment management procedures list

Procedure	Purpose
To make a selected object the root of the navigation tree	To redefine the root of the navigation tree, including opening multiple navigation tree windows with different roots.
To make a selected object the root of another navigation tree	
To restore the default navigation tree root	
To create a ring group	Manage ring groups.
To remove a ring group or ring group device	
To create a 7210 SAS split horizon group	Configure an SHG for 7210 SAS NEs.
To enable frame-based accounting on a 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, or 7210 SAS-M24F2XFP [ETR]	Enable frame-based accounting on a 7210 SAS.
To change device properties	Modify an NE configuration.
To enable and configure global Cflowd on an NE	Enable and configure global Cflowd parameters on an NE, and create Cflowd collectors.
To add a span of control to an NE	Associate a span of control with an NE.
To configure an ATM OAM loopback	Create an ATM OAM loopback on an NE for diagnostic purposes.
To enable or disable ICMP extensions on the 7705 SAR	Configure the use of vendor-specific ICMP extensions on a 7705 SAR.
To enable or disable 802.1X	Configure 802.1x authentication on an NE.

(1 of 5)

Procedure	Purpose
To create and configure a CCAG	Create and configure NE logical groups.
To create an IGH and add members	
To create and configure an ISA-IPsec group	
To create and configure an ISA-AA group and ISA-AA partition	
To enable and configure Cflowd on an ISA-AA group	
To create and configure an ISA-LNS group	
To create and configure an ISA-NAT group	
To start or stop a NAT address-pool drain operation	
To create and configure an ISA-Video group	
To create a LAG	
To configure a LAG	
To create and configure an OmniSwitch LAG	Create and configure a LAG on an OmniSwitch.
To create and configure OmniSwitch dynamic LAG members	Create and configure a dynamic LAG member on an OmniSwitch.
To assign a card type	Assign a card type to a chassis slot.
To add 9500 MPR card protection	Configure protection for 9500 MPR hardware components.
To remove 9500 MPR card protection	
To add 9500 MPR port protection	
To remove 9500 MPR port protection	

(2 of 5)

Procedure	Purpose
To configure switch fabric multicast ingress replication rates	Configure low-level NE parameters.
To configure the chassis mode of a device	
To configure timing synchronization	
To modify the IEEE 1588 PTP clock on the 7705 SAR	
To modify the IEEE 1588 PTP port on the 7705 SAR	
To configure auxiliary alarm definitions on the 7705 SAR	
To configure OmniSwitch PoE Ports	
To configure OmniSwitch stacks	
To configure an OmniSwitch CPU temperature threshold	
To configure an MDA	
To configure egress WRED queue control on an IOM 3 or IMM forwarding plane	
To configure IMPM on an MDA	
To configure IMPM on a 2 x XP MDA IOM 3 or IMM forwarding plane	
To view operational multicast channel properties on an MDA	
To enable named pool mode	
To enable LLDP on a router	
To create a chassis-level PBB configuration	
To manage OmniSwitch running configuration	Perform element management.
To manage 9500 MPR running software	
To configure OmniSwitch Health Monitoring	
To start and stop a Webview or Secure Webview session on an OmniSwitch	
To start the 9500 MPR external element manager from the 5620 SAM GUI	
To configure an 802.3ah EFM OAM diagnostic	Configure and perform Ethernet diagnostics.
To configure an 802.3ah EFM OAM diagnostic on an OmniSwitch at the NE or port level	Configure and perform Ethernet diagnostics on an OmniSwitch.
To configure Dying Gasp on an OmniSwitch 6250 (Metro) NE	
To configure an advanced loopback test on an OmniSwitch port	
To configure port/queue statistics on an OS 6250 port	
To configure Ip statistics on an OmniSwitch routing instance	
To configure an HSMDA override	Configure an HSMDA port scheduler override.

(3 of 5)

Procedure	Purpose
To configure Ethernet ports	Configure ports.
To configure OmniSwitch Ethernet ports	
To configure 9500 MPR Ethernet ports	
To configure power source type on 2+2 x Ethernet (EAS) card slots for 9500 MPR (ETSI 2.1)	
To configure Telco and 7250 SAS uplink ports as network ports	
To configure 9500 MPR E1 and DS1 ports	
To configure 9500 MPR DS3 ports	
To configure 9500 MPR radio modem ports	
To configure analog performance management on 9500 MPR radio modem ports	
To configure 9500 MPR port segregation	
To configure SONET ports	
To configure a loopback test on a 9500 MPR DS1, ES1 or radio modem port	
To configure TDM DS3 ports	
To configure a 7250 SAS CES TDM DS1/E1 port	
To configure a 7710 SR channelized TDM DS1 or E1 port	
To configure a 7705 SAR ASAP channelized TDM port	
To configure a 7210 SAS-M channelized TDM DS1 or E1 port	
To configure 7250 SAS-ESA or 7210 SAS-M24F2XFP [ETR] dry contact sensors	Configure dry-contact sensor monitoring.
To configure a 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA CES module	Configure circuit emulation on NEs.
To configure a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES port	
To create a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA unstructured CES interface	
To create a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA structured CES interface	
To modify a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES interface	

(4 of 5)

Procedure	Purpose
To configure SONET clear channels	Create and configure channels and framing links.
To automatically create all channels	
To configure SONET sub-channels	
To configure SDH sub-channels	
To create VT15 (TU11) or VT2 (TU12) sub-channels	
To create TDM DS1 channels	
To configure TDM DS1 or E1 channels	
To create TDM DS3 channels	
To configure TDM DS3 channels	
To configure a DS3/E3 channel as a network interface on a channelized ASAP MDA	
To configure an L3 interface on a DS3/E3 channel on a channelized ASAP MDA	
To configure a PVC	
To create an ILMI link	
To modify an ILMI link	
To create a multilink PPP bundle	Create and configure bundles.
To create an IMA group bundle	
To create an FR group bundle	
To modify a multilink PPP bundle	
To modify an IMA group bundle	
To modify an FR group bundle	
To configure an MLPPP bundle as a network interface on a channelized ASAP MDA	
To delete network equipment	See the *7750 SR OS System Guide* for more information.

(5 of 5)

17.4 Navigation tree equipment management procedures

Use the following procedures to manage equipment using the navigation tree.

Procedure 17-1 To make a selected object the root of the navigation tree

Use the Make Root option of the contextual menu to make a selected object the root of the navigation tree. The Make Root option is only available in the Equipment view. See section 17.1 for information about the navigation tree objects that support the menu option.

The Make Root option of the contextual menu is not available for an object that is positioned one object level below the root of the tree. For example, in a navigation tree where the device is the root of the tree, the LAG object and the shelf object do not support the Make Root option.

Right-click on the navigation tree object that you want to make the root of the tree and choose Make Root from the contextual menu. The navigation tree is refreshed with the selected object as the root of the tree. The Make Root At Top Level button is enabled.

See Procedure 17-3 for information about restoring the default root of the navigation tree.

Procedure 17-2 To make a selected object the root of another navigation tree

Use the Make Root In New Tree option of the contextual menu to make a selected object the root of another navigation tree.

Note — Up to seven navigation tree windows can be open at the same time and each tree must have a different root when it is first created.

The Make Root In New Tree menu option is only available in the equipment view. The Make Root In New Tree option is not available in the contextual menu for the root object of a tree. See section 17.1 for information about the navigation tree objects that support the menu option.

Right-click on the navigation tree object that you want to make the root of another navigation tree and choose Make Root In New Tree from the contextual menu. Another navigation tree window appears with the selected object as the root of the tree.

Procedure 17-3 To restore the default navigation tree root

The default root of the navigation tree is the network object. When the root is not the network object, the Make Root At Top Level button is enabled.

Click on the Make Root At Top Level button in the navigation tree toolbar to restore the default root of the tree. See section 2.1 for more information about the Make Root At Top Level button.

Procedure 17-4 To create a ring group

You can use the ring group creation function to:

- indicate a VLAN ring topology, for example, by grouping 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices with 7450 ESSs that operate in the same spanning tree or Ethernet ring
- indicate a VPLS ring topology, for example by grouping 7250 SAS-ES and 7250 SAS-ESA devices with 7450 ESS, 7750 SR, and 7710 SR devices
- configure the properties of the ring group to provide VLAN Internet, BTV (MVR), and L2 VPN (TLS) services
- group devices by geographic region

Consider the following before you create a ring group.

- Ensure that the devices are commissioned, as described in chapter 12.
- Ensure that mediation policies are configured to allow CLI access to the managed devices, as described in chapter 13.
- The VLAN ID for 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco devices must be unique in a ring group.
- If you want specific access interfaces to be part of a VLAN service, ensure that the parent device of the interface is a member of the ring group.

1 Choose Ring Group from the view selector in the navigation tree. The navigation tree displays the Ring Group view.

2 Right-click on the Network object and choose Create Ring Group from the contextual menu. The Ring Group (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Group Name
- Description
- Ring Group Type

4 Click on the Apply button.

5 If you set the Ring Group Type parameter to VPLS in step 3, go to step 8.

6 Click on the TLS tab button to configure L2 VPN parameters.

7 Configure the TLS parameters:

- Enabled
- Ethertype
- Jumbo Frame

The Ethertype and Jumbo Frame parameters are configurable when the Enabled parameter is selected.

8 Perform one of the following to add a device to the ring group.

a Perform the following steps to use the current properties form.

i Click on the Group Members tab button.

ii Click on the Add button. The Select Network Elements form opens.

iii Choose one or more NEs and click on the OK button. A dialog box appears.

iv Click on the OK button. The Select Network Elements form closes and the selected devices are listed on the Ring Group (Create) form.

v Click on the OK button. A dialog box appears.

vi Click on the Yes button. The Ring Group (Edit) form closes and the device objects are listed in the navigation tree under the new ring group object.

b Perform the following steps to use the navigation tree.

i Right-click on the device object in the Equipment view of the navigation tree and choose Add To Ring Group from the contextual menu. The Select Group form opens to display a list of ring groups.

ii Choose the new ring group and click on the OK button. The Select Group form closes and the device object is listed under the ring group in the Ring Group view of the navigation tree.

Note — All device types can be added as members of a VLAN ring group. Only devices that support VPLS can be added to a VPLS ring group.

9 To apply a span of control to a ring group, click on the Spans tab button.

i Click on the Add button. The Select Span(s) - Ring Groups form opens with a list of available spans.

ii Choose one or more spans of control to apply to the ring group.

iii Click on the OK button. The Select Span(s)-Ring Group form closes and a dialog box appears.

iv Click on the OK button.

10 To view network-level alarms from a 7250 SAS or other device in a ring group, click on the Faults tab button.

11 Provision VLAN services, as described in chapter 65.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The Ring Group (Create) form closes.

Procedure 17-5 To remove a ring group or ring group device

1 Choose Ring Group from the view selector in the navigation tree. The navigation tree displays the Ring Group view.

2 Navigate to the required ring group object.

3 To remove a device from the ring group, right-click on the device object under the ring group and choose Remove From Ring Group from the contextual menu. The device is removed from the ring group.

4 To remove a ring group:

i Perform step 3 for each device in the ring group to remove all devices from the ring group.

ii Right-click on the Ring Group object and choose Remove Ring Group from the contextual menu. A dialog box appears.

iii Click on the Yes button. The ring group is removed.

Caution — Removing a ring group deletes the VLAN services that are associated with the ring group.

Procedure 17-6 To create a 7210 SAS split horizon group

Traffic that arrives on a access or access uplink port or LAG within a split horizon group is not copied to other ports and LAGs in the same split horizon group; the traffic is copied to ports and LAGs in other split horizon groups if they exist within the same VPLS. Ports and LAGs are added to a split horizon group when you configure a port or LAG on a 7210 SAS. Split horizon groups are not supported for a VPLS instance.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Locate the device on which to configure the split horizon group.

3 Right-click on the device icon and choose Properties from the contextual menu. The Network Element (Edit) form opens.

4 Click on the Split Horizon Groups tab button.

5 Click on the Add button. The Split Horizon Group (Create) form opens.

6 Configure the parameters:

- Name
- Description

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The split horizon group is added to the displayed list.

9 Repeat steps 5 to 8 for each split horizon group that you need to add. The 7210 SAS supports 24 split horizon groups.

10 To view the ports, LAGs, and faults that are associated with a split horizon group choose a split horizon group from the list and click on the Properties button.

11 If you need to delete a split horizon group, choose the group from the list and click on the Delete button. A dialog box appears.

12 Enable the check box and click on the Yes button. You cannot delete a split horizon group if there are any ports or LAGs bound to it.

13 Close the Network Element (Edit) form.

Procedure 17-7 To enable frame-based accounting on a 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, or 7210 SAS-M24F2XFP [ETR]

The 7210 SAS-E, Release 1.0 R5 or later, the 7210 SAS-M24F, Release 1.1 R3 or later, the 7210 SAS-M24F2XFP and the 7210 SAS-M24F2XFP [ETR], Release 1.0 or later, support frame-based accounting for QoS policies.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Locate the device on which to configure frame-based accounting.

3 Right-click on the device icon and choose Properties from the contextual menu. The Network Element (Edit) form opens.

4 Click on the Frame Based Accounting tab button.

5 Configure the parameters:

- Egress
- Ingress

6 Click on the OK button. The Network Element (Edit) form closes.

Procedure 17-8 To change device properties

1 Right-click on a discovered device in the navigation tree and choose Properties from the contextual menu. The properties form for the device opens.

2 Use the properties form to view or modify the device parameters, as required using the following tabs.

- The General tab displays:
  - the Location, Resource Group ID, Latitude (degrees), and Longitude (degrees) parameters
  - the VPLS Mode parameter if the device is a 7250 SAS-ES or 7250 SAS-ESA
  - an Auto-Provision button if the device is a 7705 SAR; see chapter 26 for information about configuring and deploying configuration profiles to a 7705 SAR
  - the Physical Impedance parameter if the device is a 9500 MPR
- The Polling tab displays polling parameters. See chapter 13 for more information about configuring in-band or out-of-band polling policies.
- The Protocols tab displays the routing protocols configured for the device. See chapter 28 for more information about configuring protocols.
- The Globals tab contains multiple tabs. Not all tabs apply to every NE type:
  - Load Balancing—displays the L4 Load Balancing parameter
  - LACP—displays the LACP System Priority parameter
  - LLDP—displays several LLDP parameters. The parameters displayed vary according to the NE type.

    7210 SAS, 7450 ESS, 7710 SR, 7710 SR, and 7750 SR NEs display the Administrative Status, Transmission Interval (Seconds), Transmission Multiplier, Re-Init Delay (Seconds), Notification Interval (Seconds), Maximum Consecutive Transmissions, Fast Transmission Interval (Seconds), and PDUs in Fast Transmission parameters.

    OmniSwitch NEs display the Transmission Interval (Seconds), Transmission Multiplier, Re-Init Delay (Seconds), Notification Interval (Seconds), and Transmission Delay (Seconds) parameters.
  - MEP—displays the MEP Id parameter, which is used for automatic MEP ID assignment during automatic MEP creation
  - PAE—displays the Administrative State parameter
- The ATM tab for a 7750 SR displays ATM OAM loopback parameters for interfaces that host IES and VPRN SAPs. See Procedure 17-11 for more information.
- The Scripts tab displays the script instances and versions that are applied to the device. In addition, you can execute scripts and open the script manager using this tab. See the *5620 SAM Scripts and Templates Developer Guide* for more information.
- The Redundancy tab displays two sub-tabs: BGP Multi-homing and MC Peer. The BGP Multi-homing tab allows you to configure NE-level parameters used in BGP VPLS multi-homing. See Procedure 68-6 for more information. The MC Peer sub-tab allows you to add or remove MC peers. See chapter 38 for more information.
- The Ring Groups tab displays the ring groups associated with the device. See Procedure 17-4 for more information.
- The Rule-Based Groups tab displays the rule-based groups that support rule-based service-tunnel creation.

- The CFLOWD tab displays global NE Cflowd parameters, and allows the configuration of NE-based Cflowd collectors.
- The Frame Based Accounting tab displays the parameters that enable ingress and egress frame-based accounting for the 7210 SAS-E, Release 1.0 R5 or later, the 7210 SAS-M24F, Release 1.1 R3 or later, the 7210 SAS-M24F2XFP and the 7210 SAS-M24F2XFP [ETR], Release 1.0 R1 or later.
- The Split Horizon Groups tab lists the SHGs that include the device as a member.
- The LI Configuration Status tab which is viewable by an operator with LI privileges, displays the LI operational configuration. See chapter 31 for more information about configuring LI.
- The QoS tab displays the QoS Classification parameter for a 9500 MPR.
- The VLAN Groups tab displays VLAN group information for a 9500 MPR.
- The System Settings tab displays the Admission Control parameter for a 9500 MPR.
- The Physical Links tab displays physical link information. Only radio link information is displayed for the 9500 MPR. See chapter 4 for more information.
- The Spans tab displays the spans of control. See chapter 8 for more information about configuring a span of control on an NE.
- The Statistics tab displays statistics available for the device. See the *5620 SAM Statistics Management Guide* for more information.
- The Faults tab displays the network-level alarms for the device.

3 Close the device properties form.

Procedure 17-9 To enable and configure global Cflowd on an NE

Perform this procedure to enable Cflowd and configure global Cflowd parameters on an NE. You can also configure Cflowd sampling for AA flows. See chapter 73 for information about configuring Cflowd collectors for AA applications groups.

1 Right-click on an NE in the navigation tree and choose Properties from the contextual menu. The NE properties form opens.

2 Click on the CFLOWD tab button. The General tab is displayed.

3 Set the CFLOWD State parameter to Enabled. The form displays additional parameters.

4 Configure the remaining parameters:

- Active Time-out (minutes)
- In-Active Time-out (seconds)
- Cache Size
- Sample Rate
- Over Flow (percent)
- Administrative State
- Template Re-transmit (seconds)

5 Click on the Collector tab button.

6 Perform the following steps to add a collector.

i Click on the Add button. The Cflowd Collector Configuration (Create) form opens.

ii Configure the parameters:

- Host Address
- Port Number
- Description
- Version (version)
- Aggregation Type
- Autonomous System
- Template Type

The Aggregation Type parameter is configurable when the Version (version) parameter is set to version-8.

The Autonomous System parameter is configurable when the Version (version) parameter is set to version-5 or version-8.

The Template Type parameter is configurable when the Version (version) parameter is set to version-9.

iii Click on the OK button. The CFLOWD Collector Configuration (Create) form closes and a dialog box appears.

iv Click on the OK button. The collector is listed on the NE properties form.

7 Repeat step 6 to add another collector, if required.

Note — A global NE Cflowd configuration can contain a maximum of five collectors.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The NE properties form closes.

Procedure 17-10 To add a span of control to an NE

1 Right-click on a discovered device in the navigation tree and choose Properties from the contextual menu. The properties form for the device opens.

2 Click on the Spans tab button.

3 Click on the Add button. The Select Span(s) - Network Element form opens with a list of available spans.

4 Choose one or more spans to apply to the NE.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Select Span(s) - Network Element form closes.

Procedure 17-11 To configure an ATM OAM loopback

ATM OAM loopback settings are configured globally on supported devices. However, a loopback must be enabled on an IES or VPRN SAP.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Locate the device on which to configure an ATM OAM loopback.

3 Right-click on the device icon and choose Properties from the contextual menu. The Network Element (Edit) form opens.

4 Click on the ATM tab button.

5 Configure the parameters:

- ATM OAM Loopback Location ID
- ATM OAM Loopback Period
- Number of Tries for Up State
- Number of Tries for Down State

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Network Element (Edit) form closes.

Procedure 17-12 To enable or disable ICMP extensions on the 7705 SAR

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Locate the 7705 SAR on which to configure ICMP extensions.

3 Right-click on the device icon and choose Properties from the contextual menu. The Network Element (Edit) form opens.

4 Click on the ICMP tab button.

5 Configure the Vendor-Specific ICMP Extensions parameter.

6 Click on the OK button. The Network Element (Edit) form closes.

Procedure 17-13 To enable or disable 802.1X

You can view the status of 802.1X authentication on a device in a managed network.

Note — Before you can create an 802.1X policy, 802.1X must be enabled on the device. Before you can configure 802.1X on an Ethernet access port, 802.1X must be enabled on the device and an 802.1X policy must be created and distributed to the device.

1 Enable 802.1X on a managed device:

- **i** Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.
- **ii** Right-click on a managed device in the equipment view of the navigation tree.
- **iii** Choose Properties from the contextual menu. The Network Element (Edit) form opens.
- **iv** Click on the Globals tab button. The Load Balancing tab opens.
- **v** Click on the PAE tab button.
- **vi** Set the Administrative State parameter to Up.
- **vii** Click on the OK button. The Network Element (Edit) form closes.
- **viii** Repeat step 1 for each device for which you want to enable 802.1X.

To create and distribute 802.1X policies to the devices that use 802.1X, see chapter 52.

To configure 802.1X on Ethernet access ports, see Procedure 17-61.

2 To disable 802.1X on a managed device, repeat step 1 but set the Administrative State to Down.

Procedure 17-14 To create and configure a CCAG

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Locate and expand the device on which you want to create a CCAG.

3 Right-click on the CCAG icon and choose Create CCAG. The CCAG (Create) form opens with the General tab displayed.

4 Configure the parameters:

- CCAG ID
- Description
- CCA Rate Enabled
- CCA Rate (kbps)
- Access Adapt QoS
- Administrative State

5 Click on the CCAG MDA Members tab button to display and configure CCAG MDA members associated with this CCAG.

6 Click on the Add button. The CCAG MDA Member (Create) form opens.

7 Click on the Select button. The Select Member MDA - CCAG MDA Member form opens with a list of available VSM-CCA cards.

8 Choose the MDA to add to this CCAG and click the OK button. The Select Member MDA - CCAG MDA Member form closes and the CCAG MDA Member (Create) form reappears.

9 Click on the OK button. The CCAG MDA Member (Create) form closes.

10 Click on the CCAG Paths tab button. The Alpha and Beta paths are displayed. To modify a path, go to step 11. Otherwise, go to step 24.

11 Choose a path and click on the Properties button. The CCAG Internal Path (Edit) form opens with the General tab displayed.

12 Configure the parameters:

- Path Rate Enabled
- Path Rate (Kb/s)
- Path Rate Option
- Path Weight (%)

13 Click on the Path Cross Connects tab button. This tab displays the cross- connects associated with the path.

14 Choose a cross-connect to be configured and click Edit. The Cross Connect (Edit) form opens with the General tab displayed.

15 Configure the parameters:

- Description
- Configured MAC
- MTU (octets)

16 Click on the States tab button.

17 Configure the Administrative State.

18 Click on the Policies tab button.

19 To specify an egress slope policy other than the default, perform the following steps.

i Click on the Clear button in the Egress Slope Policy panel.

ii Click on the Select button in the Egress Slope Policy panel. The Select Egress Slope Policy form opens.

iii Choose a policy and click on the OK button. The Select Egress Slope Policy form closes and the policy name is displayed on the Cross Connect (Edit) form.

20 Configure the parameters:

- Egress Reserved CBS (%)
- Ingress Reserved CBS (%)

21 To specify an ingress slope policy other than the default, perform the following steps.

i Click on the Clear button in the Ingress Slope Policy panel.

ii Click on the Select button in the Ingress Slope Policy panel. The Select Ingress Slope Policy form opens.

iii Choose a policy and click on the OK button. The Select Ingress Slope Policy form closes and the policy name is displayed on the Cross Connect (Edit) form.

22 Click on the OK button. The Cross Connect (Edit) form closes and the CCAG Internal Path (Edit) form reappears.

23 Click on the OK button. The CCAG Internal Path (Edit) form closes and the CCAG (Edit) form reappears.

24 Click on the OK button. The CCAG (Edit) form closes.

Procedure 17-15 To create an IGH and add members

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on the IGH object below a device in the Equipment view and choose Create IGH from the contextual menu. The Create IGH form opens.

3 Configure the parameters:

- IGH ID
- Minimum Active Link Threshold
- Administrative State

4 Click on the Ok button. The Create IGH form closes.

5 Right-click on the IGH group object below the IGH in the Equipment view and choose Create IGH Members from the contextual menu. The Create IGH Members form opens.

6 Click on the Select button beside the CLI Name parameter. The Select Port States - IGH Member form opens.

7 Choose a port from the list and click on the Ok button. The Create IGH Members form reappears.

8 Click on the OK button. The Create IGH Members form closes.

9 Repeat steps 7 and 8 to add more members, if required.

Procedure 17-16 To create and configure an ISA-IPsec group

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Locate and expand the device on which you need to create an ISA-IPsec group.

3 Right-click on the ISA-IPsec Group icon and choose Create ISA-IPsec Group. The IPsec Group (Create) form opens.

4 Configure the parameters:

- Group Number
- Description
- Administrative State

5 Click on the Apply button.

6 Click on the IPsec ISA Group Members tab button.

7 Click on the Add button. The ISA Group Member (Create) form opens.

8 Click on the Select button. The Select Daughter Card - ISA Group Member form opens with a list of available ISA IPsec cards.

9 Choose the MDA to add to this ISA-IPsec Group and click the OK button. The Select Daughter Card - ISA IPsec Group Member form closes and the ISA Group Member (Create) form reappears.

10 Click on the OK button. The ISA Group Member (Create) form closes.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The IPsec Group form closes.

13 Repeat steps 3 to 12 to configure the backup ISA-IPsec group member.

Procedure 17-17 To create and configure an ISA-AA group and ISA-AA partition

When you create or delete an ISA-AA partition, a default AA group partition policy and a default AA accounting policy are automatically created or deleted under the ISA-AA partition.

Note — An ISA-AA partition provides ISA-AA group functions but only in the context of the created partition. Application ID, policy, and statistics configuration apply only to the partition you created for the ISA-AA group.

1 Choose Equipment from the view selector in the navigation tree.

2 Locate and expand the device on which you need to create an ISA-AA group.

3 Expand the Logical Groups icon.

Note — You can also create an ISA-AA group or ISA-AA partition from the Manage→ISA Functions→ISA-AA form.

4 Right-click on the ISA-AA Group icon and choose Create ISA-AA Group. The ISA-AA Group (Create) form opens.

5 Configure the parameters:

- Group Number
- Description
- Operation Upon Failure
- Administrative State
- Partitions
- Capacity Cost High Threshold
- Capacity Cost Low Threshold

Note — If there are AA group policies on the ISA-AA group that you are configuring, you cannot modify the Partitions parameter from "Enabled" to "Disabled" or from "Disabled" to "Enabled." Before you can modify the Partitions parameter, you must delete the AA group policies and the associated SAP dependencies.

6 If you set the Partitions parameter to Enabled, perform the following steps to create and configure an ISA-AA partition.

i Click on the ISA-AA Partitions tab button.

ii Click on the Add button. The ISA-AA Group Partition (Create) form opens.

iii Configure the parameters:

- Partition ID
- Description

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The ISA-AA Group (Edit) form appears with the ISA-AA partition listed.

vi If required, repeat step 6 to create another ISA-AA partition.

7 Specify a traffic forwarding class to divert to the ISA-AA group.

i Click on the ISA-AA Group Diverted FCs tab button.

ii Click on the Add button. The ISA-AA Group Diverted FC (Create) form opens.

iii Configure the Forwarding Class Name parameter.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The ISA-AA Group Diverted FC (Create) form closes.

8 Specify an ISA-AA MDA for the ISA-AA group.

i Click on the ISA-AA Group Members tab button.

ii Click on the Add button. The ISA-AA Group Member (Create) form opens.

iii Configure the ISA-AA MDA Role parameter.

iv Click on the Select button. The Select Member MDA - ISA-AA Group Member form opens with a list of available ISA-AA cards.

v Choose the MDA to add to this ISA-AA Group and click the OK button. The Select Member MDA - ISA-AA Group Member form closes and the ISA-AA MDA Member (Create) form reappears.

vi Click on the OK button. The ISA-AA Group Member (Create) form closes.

Note — The MDA slot number assigned to an AA subscriber or AA SAP on the AA Subscriber or AA SAP Summary form is displayed as Unassigned if the AA subscribers in the configuration file cannot fit after an NE reboot.

9 Specify the QoS parameters for the ISA-AA group.

i Click on the QoS tab button.

ii Configure the Egress From-Subscriber Reserved CBS % parameter.

iii Click on the Select button in the Egress From-Subscriber Slope Policy panel. The Select Egress From-Subscriber Slope Policy form opens.

iv Choose a policy from the list and click on the OK button. The Select Egress From-Subscriber Slope Policy form closes.

v Click on the Select button in the Egress From-Subscriber Network Queue-Policy panel. The Select Egress From-Subscriber Network Queue-Policy form opens.

vi Choose a policy from the list and click on the OK button. The Select Egress From-Subscriber Network Queue-Policy form closes.

vii Click on the Select button in the Egress From-Subscriber Port Scheduler Policy panel. The Select Egress From-Subscriber Port Scheduler Policy form opens.

viii Choose a policy from the list and click on the OK button. The Select Egress From-Subscriber Port Scheduler Policy form closes.

ix Click on the QoS Egress To-Subscriber tab button.

x Configure the Egress To-Subscriber Reserved CBS % parameter.

xi Click on the Select button in the Egress To-Subscriber Slope Policy panel. The Select Egress To-Subscriber Slope Policy form opens.

xii Choose a policy from the list and click on the OK button. The Select Egress To-Subscriber Slope Policy form closes.

xiii Click on the Select button in the Egress To-Subscriber Network Queue-Policy panel. The Select Egress To-Subscriber Network Queue-Policy form opens.

xiv Choose a policy from the list and click on the OK button. The Select Egress To-Subscriber Network Queue-Policy form closes.

xv Click on the Select button in the Egress To-Subscriber Port Scheduler-Policy panel. The Select Egress To-Subscriber Port Scheduler-Policy form opens.

xvi Choose a policy from the list and click on the OK button. The Select Egress To-Subscriber Port Scheduler Policy form closes.

xvii Click on the QoS Ingress To-Subscriber tab button.

xviii Configure the Ingress To-Subscriber Reserved CBS % parameter.

xix Click on the Select button in the Ingress To-Subscriber Slope-Policy panel. The Select Ingress To-Subscriber Slope-Policy form opens.

xx Choose a policy from the list and click on the OK button. The Select Ingress To-Subscriber Slope-Policy form closes.

xxi Click on the Select button in the Ingress To-Subscriber Network Queue-Policy panel. The Select Ingress To-Subscriber Network Queue-Policy form opens.

xxii Choose a policy from the list and click on the OK button. The Select Ingress To-Subscriber Network Queue-Policy form closes.

10 Add a special-study subscriber to the ISA-AA group or ISA-AA group partition.

i Click on the AA Special Study Subscribers tab button.

ii Click on the Add button. The AA Special Study Subscriber (Create) form opens.

iii Configure the parameters:

- AA Subscriber Name
- AA Stats Type

iv Click on the OK button. The AA Special Study Subscriber (Create) form closes.

11 Add a special-study SAP to the ISA-AA group or ISA-AA partition.

i Click on the AA Special Study SAPs tab button.

ii Click on the Add Per-SAP Protocols button to add a SAP for per-protocol monitoring, if required. The Select Per-SAP Protocols form opens. Otherwise, go to step 11 iv.

iii Choose a SAP in the list and click on the OK button. The Select Per-SAP Protocols form closes and the SAP is listed on the AA Special Study SAPs tab.

iv Click on the Add Per-SAP Applications button to add SAP for per-application monitoring, if required. The Select Per-SAP Applications form opens. Otherwise, go to step 12.

v Choose a SAP in the list and click on the OK button. The Select Per-SAP Protocols form closes and the SAP is listed on the AA Special Study SAPs tab.

vi Click on the OK button. The AA Special Study Subscriber (Create) form closes.

12 Add AA objects for custom per-SAP or per-subscriber statistics collection.

i Click on the AA Subscriber Stats Objects tab button.

ii Click on the Add Applications button to add an application, if required. The Select Applications form opens.

iii Choose one or more applications in the list and click on the OK button. The Select Applications form closes and the applications are listed on the AA Subscriber Stats Objects tab.

iv Click on the Add Application Groups button to add an application group, if required. The Select Application Groups form opens.

v Choose one or more application groups in the list and click on the OK button. The Select Application Groups form closes and the application groups are listed on the AA Subscriber Stats Objects tab.

vi Click on the Add Protocols button to add a protocol, if required. The Select Protocols form opens.

vii Choose one or more protocols in the list and click on the OK button. The Select Protocols form closes and the protocols are listed on the AA Subscriber Stats Objects tab.

viii Click on the Add Custom Protocols button to add a custom protocol, if required. The Select Custom Protocols form opens.

ix Choose one or more custom protocols in the list and click on the OK button. The Select Custom Protocols form closes and the custom protocols are listed on the AA Subscriber Stats Objects tab.

13 Add special study spoke SDP bindings to the ISA-AA group or ISA-AA partition.

i Click on the AA Special Study Spoke SDP Bindings tab button.

ii Click on the Add Per-Spoke SDP Binding Protocols button to add a per-spoke SDP binding protocol, if required. The Select Per-Spoke SDP Binding Protocol form opens.

iii Choose one or more protocols in the list and click on the OK button. The Select Per-Spoke SDP Binding Protocol form closes and the protocols are listed on the AA Special Study Spoke SDP Bindings form.

iv Click on the Add Per-Spoke SDP Binding Applications button to add a per-spoke SDP binding application, if required. The Select Per-Spoke SDP Binding Applications form opens.

v Choose one or more applications in the list and click on the OK button. The Select Per-Spoke SDP Binding Applications form closes and the applications are listed on the AA Special Study Spoke SDP Bindings form.

14 Add an AA subscriber policy override to the ISA-AA group or ISA-AA partition.

Note 1 — The AA subscriber policy override is rejected if the subscriber does not have an application profile assigned.

Note 2 — You can add an AA subscriber policy override to a SAP or Spoke SDP, but not to an ESM subscriber.

i Click on the AA Subscriber Policy Overrides tab button.

ii Click on the Add button. The AA Subscriber Policy Override (Create) form opens with the General tab displayed.

iii Configure the AA Subscriber Type parameter. If you chose SAP, go to step iv. If you chose Spoke SDP Binding, go to step vi.

iv Click on the Select button in the SAP Subscriber panel. The Select SAP Subscriber - AA Subscriber Policy Override form opens.

v Choose a SAP subscriber from the list and click on the OK button. The Select SAP Subscriber - AA Subscriber Policy Override form closes and the AA Subscriber Policy Override (Create) form refreshes with the SAP subscriber. Go to step viii.

vi Click on the Select button in the Spoke SDP Binding Subscriber panel. The Select Spoke SDP Binding Subscriber - AA Subscriber Policy Override form opens.

vii Choose a Spoke SDP Binding Subscriber in the list and click on the OK button. The Select Spoke SDP Binding Subscriber - AA Subscriber Policy Override form closes and the AA Subscriber Policy Override (Create) form refreshes with the Spoke SDP Binding name. Go to step viii.

viii Click on the ASO Characteristics tab button.

ix Click on the Add button. The AA Subscriber Policy Override ASO Characteristic (Create) form opens.

x Click on the Select button beside the Override ASO Characteristic Name parameter. The Select Application Service Option form opens.

xi Choose an Application Service Option from the list and click on the OK button. The AA Subscriber Policy Override ASO Characteristic form refreshes with the ASO Characteristic Name.

xii Click on the Select button beside the Override ASO Characteristic Value parameter. The Select Application Service Option Characteristic Value form opens.

xiii Choose an ASO Characteristic Value from the list and click on the OK button. The AA Subscriber Policy Override ASO Characteristic form refreshes with the ASO Characteristic Value.

15 Click on the OK button.

16 Click on the OK button. The AA Subscriber Policy Override (Create) form closes and the ISA-AA Group (Edit) form appears.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button to apply the changes. The ISA-AA Group (Edit) form closes.

Procedure 17-18 To enable and configure Cflowd on an ISA-AA group

Note — Before you perform this procedure, you must first enable global Cflowd on the NE. See Procedure 17-9 for more information.

1 Choose Equipment from the navigation tree view selector.

2 Locate and expand the device that contains the ISA-AA group.

3 Expand the Logical Groups icon.

4 Expand the ISA-AA Group icon and choose Properties from the contextual menu. The ISA-AA Group (Edit) form opens.

5 Click on the CFLOWD tab button. The General tab is displayed.

6 Configure the remaining parameters:

- Sampling Rate
- Volume Administrative State
- Sample Flow Rate
- Performance Administrative State
- Template Re-transmit
- Administrative State

7 Click on the Collector tab button.

8 Perform the following steps to add a collector.

i Click on the Add button. The Cflowd Collector (Create) form opens.

ii Configure the parameters:

- Host Address
- Collector Port
- Description
- Administrative State
- Version

iii Click on the OK button. The CFLOWD Collector (Create) form closes and a dialog box appears.

iv Click on the OK button. The collector is listed on the ISA-AA group properties form.

9 Repeat step 8 to add another collector, if required.

Note — A Cflowd configuration on an ISA-AA group can contain a maximum of two collectors.

10 To add an AA application or AA application group for Cflowd performance monitoring, click on the Performance tab button. Otherwise, go to step 13.

11 Perform the following steps to add one or more applications, if required.

i Click on the Add Applications button. The Select Applications form opens.

ii Choose one or more applications in the list and click on the OK button. The Select Applications form closes, and the applications are listed on the ISA-AA group properties form.

12 Perform the following steps to add one or more application groups, if required.

i Click on the Add Application Groups button. The Select Application Groups form opens.

ii Choose one or more applications in the list and click on the OK button. The Select Applications form closes, and the applications are listed on the ISA-AA group properties form.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The NE properties form closes.

Procedure 17-19 To create and configure an ISA-LNS group

Perform this procedure to create and configure an ISA-LNS group. You can configure an IES or VPRN group interface to terminate LNS PPP sessions. See chapter 70 for information about configuring an IES group interface. See chapter 71 for information about configuring a VPRN group interface.

1 Choose Equipment from the view selector in the navigation tree.

2 Locate and expand the device on which you need to create an ISA-LNS group.

3 Expand the Logical Groups icon.

4 Right-click on the ISA-LNS Groups icon and choose Create ISA-LNS Group. The ISA-LNS Group (Create) form opens.

5 Configure the parameters:

- Group Number
- Description
- Administrative State

6 Click on the Apply button. The ISA-LNS Group (Edit) form opens with the General tab displayed.

7 Click on the ISA-LNS Group Members tab button.

8 Click on the Add button. The ISA-LNS Group Member (Create) form opens with the General tab displayed.

Note — You can configure up to six ISA-LNS group members. For each group member, you must choose an ISA Broadband Applications MDA. An ISA Broadband Applications MDA can be configured only on an IOM3-XP module on a 7750 SR.

9 Click on the Select button. The Select Member MDA - ISA-LNS Group Member form opens with a list of available ISA broadband applications cards.

10 Choose the MDA to add to the ISA-LNS Group and click the OK button. The Select Member MDA - ISA-LNS Group Member form closes and the ISA-LNS Group Member (Create) form reappears. The Slot Name field displays your selection.

11 Click on the OK button. The ISA-LNS Group Member (Create) form closes.

12 Repeat steps 4 to 11 to configure another ISA-LNS Group member, if required.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The ISA-LNS Group Member (Create) form closes.

Procedure 17-20 To create and configure an ISA-NAT group

Perform this procedure to create and configure an ISA-NAT group. See chapter 27 for information about configuring the NAT function on a routing instance.

Note — You can create an ISA-NAT group only on a Release 8.0 or later 7750 SR-7 or 7750 SR-12 in chassis mode B or higher. See chapter 15 for information about chassis modes.

1 Choose Equipment from the view selector in the navigation tree.

2 Locate and expand the device on which you need to create an ISA-NAT group.

3 Expand the Logical Groups icon.

4 Right-click on the ISA-NAT Groups icon and choose Create ISA-NAT Group. The ISA-NAT Group (Create) form opens.

5 Configure the parameters:

- Group Number
- Description
- Active MDA Limit
- Reservation Count
- Session Watermark High
- Session Watermark Low

6 Click on the Apply button. The ISA-NAT Group (Create) form refreshes with additional tabs, and the form name changes to ISA-NAT Group (Edit).

7 Click on the ISA-NAT Group Members tab button.

8 Click on the Add button. The MDA (Create) form opens.

Note — You can configure up to six ISA-NAT group members. Each group member must be an ISA Broadband Applications MDA.

9 Click on the Select button. The Select Daughter Card form opens.

10 Choose an MDA in the list and click the OK button. The Select Daughter Card form closes, and the MDA (Create) form displays the MDA identifier.

11 Click on the General tab button.

12 Configure the Administrative State parameter.

Note — You can set the Administrative State parameter to Up only when the ISA-NAT group contains at least one member MDA and when the Active MDA Limit parameter is set to a value greater than 0.

13 Click on the OK button. The MDA (Create) form closes and a dialog box appears.

14 Click on the OK button. The ISA-NAT Group (Edit) form lists the member MDA.

15 Repeat steps 8 to 14 to configure another ISA-NAT group member, if required.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The ISA-NAT Group (Edit) form closes.

Procedure 17-21 To start or stop a NAT address-pool drain operation

Perform this procedure to control the removal, or draining, of the host sessions associated with a NAT pool address range.

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance that has one or more configured NAT pools. The path is Routing→NE→Routing Instance.

3 Right-click on the routing instance and click on the Properties button. The Routing Instance properties form opens.

4 Click on the NAT Configuration tab button.

5 Click on the Search button. A list of NAT configurations is displayed.

6 Choose the required NAT configuration in the list and click on the Properties button. The NAT Configuration (Edit) form opens with the General tab displayed.

7 Click on the NAT Pools tab button.

8 Click on the Search button. A list of address pools is displayed.

9 Choose the required address pool in the list and click on the Properties button. The NAT Pool (Edit) form opens.

Note — You can also select multiple address pools and use the Drain or Stop Drain buttons to control the draining for the selected address pools, as described in subsequent procedure steps.

10 To start a drain operation on the address pool, click on the Drain button. The number of host sessions associated with the address range decreases as sessions close.

11 To stop an active drain operation on the address pool, click on the Stop Drain button. New host sessions are allowed to use the address range.

12 Close the open forms, as required.

Procedure 17-22 To create and configure an ISA-Video group

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Locate and expand the device on which you need to create an ISA-Video group.

3 Right-click on the ISA-Video Group icon and choose Create ISA-Video Group. The ISA-Video Group (Create) form opens.

4 Configure the parameters:

- Group Number
- Description
- Administrative State
- Local Retransmission Server
- Fast Channel Change Server
- Ad Insert server
- Reserve Retransmission Bandwidth
- Stream Selection
- Analyzer

5 Click on the Apply button. The form displays four additional tabs.

6 Click on the Video Group Members tab button.

7 Click on the Add button. The Video Group Member (Create) form opens.

8 Click on the Select button. The Select Daughter Card - Video Group Member form opens with a list of available ISA Video cards.

9 Choose the MDA to add to this Video Group and click the OK button. The Select Daughter Card - Video Group Member form closes and the Video Group Member (Create) form reappears. The Slot Name field displays your selection.

10 Click on the OK button. The Video Group Member (Create) form closes.

11 Repeat steps 3 to 10 to configure another ISA-Video Group member, if required.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The ISA-Video Group (Create) form closes.

Procedure 17-23 To create a LAG

Note — This procedure applies to 7210 SAS, 7450 ESS, 7710 SR, and 7750 SR nodes. See Procedure 17-26 for information about how to configure a LAG on an OmniSwitch.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Expand the NE object to display the Logical Groups object.

3 Right-click on the LAGs object in the Logical Groups object and choose Create LAG from the contextual menu. The Create LAG form opens.

4 Configure the parameters:

Note — The parameters that appear and which can be configured is dependant on the node type for which the LAG is being configured for.

- LAG ID
- Auto-Assign ID
- Port Type
- Description
- Configured Address
- L2Uplink
- Mode
- Encap Type
- Administrative State

5 If you are configuring a LAG on a 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, or 7210 SAS-M24F2XFP [ETR], you can add the LAG to a split horizon group. See Procedure 17-6 for information about creating a 7210 SAS split horizon group.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - LAG form opens.

ii Choose a split horizon group and click on the OK button. The Select Split Horizon Group - LAG form closes and the Create LAG form refreshes with the split horizon group name.

Note 1 — A LAG cannot be added to or deleted from a split horizon group if it has a SAP configured on it.

Note 2 — A LAG cannot belong to more than one split horizon group; you must remove any split horizon groups from the LAG before you can add the LAG to a different split horizon group.

6 If you are configuring a LAG on a 7210 SAS-E, go to step 11.

7 Click on the Next button. The Configure LAG Parameters form opens.

8 Configure the parameters:

- Port Threshold
- Port Threshold Action
- Dynamic Cost

9 Click on the Next button.

a If you set the Mode parameter in step 4 to Access, the Configure Access Parameters form opens. Go to step 10.

b If you set the Mode parameter in step 4 to Network, the Configure LACP form opens. Go to step 12.

10 Configure the QoS Adaptation and Per FP Ingress Queue parameters.

11 Click on the Next button. The Configure LACP form opens.

12 Configure the parameters:

Note — The availability of configurable parameters depends on the node type for which the LAG is being configured.

- Administrative State
  The Administrative State parameter must be enabled before you can configure LACP and select a subgroup as an active subgroup.
- LACP Mode
- LACP Transmit Interval
- LACP Transmit Standby
- Auto-Generate
- Actor System ID
- Partner System ID
- LACP System ID
- LACP System Priority
- Actor System Priority
- Partner System Priority
- Hold Time (100s of milliseconds)
- Active Sub-Group Selection Criteria
- Slave to Partner

Note — The LACP Mode, LACP Transmit Interval, Actor Administration Key, LACP System ID, and LACP System Priority parameters are configurable when the Administrative State parameter is enabled.

13 Click on the Next button. The Configure LAG Members form opens.

14 Click on the Add button to add network ports to LAGs. The Only show compatible ports form appears.

15 Configure the Show Only Compatible Ports parameter.

16 Click on the Next button. The Select Ports form opens.

17 Choose compatible ports from the list to construct the LAG.

Add ports to the LAG as follows:

- Choose up to eight ports — two if you are configuring a 7210 SAS-E, four if you are configuring a 7210 SAS-M24F, 7210 SAS-M24F2XFP, or 7210 SAS-M24F2XFP [ETR].
- Click on the Next button. The Specify the Member Properties form opens.

Note 1 — For ports to appear as compatible ports, ensure no SAPs or services are configured on them.

Note 2 — If there are no compatible ports to choose from and you have decided that you want to edit some of the existing ports that are not compatible to be compatible, disable the Show compatible ports only parameter. Click on the Next button. Choose ports to edit from the list and click on the Properties button.

Note 3 — For all ports in a LAG, you must disable auto-negotiation, configure the same speed, and set the ports to full duplex.

Note 4 — You must use the same load balance algorithm for the ports associated with the LAG.

18 Configure the parameters:

- Priority
- Sub-Group ID

19 If required, add Egress Secondary Shapers to a port member of LAGs configured on HSMDAs on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7750 SR-7, 7750 SR-12, 7450 ESS-6, 7450 ESS-7 and 7450 ESS-12, Release 7.0 R3, or later. See step 30 of Procedure 17-61 to add Egress Secondary Shapers.

Note 1 — The add/delete/modify functions for Egress Secondary Shapers apply only to the primary port.

Note 2 — The Egress Secondary Shapers on the primary port of the LAG are propagated to each non-primary port member of the LAG, with a maximum 8 ports per LAG.

For adding any new port to the LAG, the user must configure each Egress Secondary Shaper as per the primary port, otherwise the addition of the port is blocked.

Note 3 — When adding a port member to a LAG, the primary port and each selected port (maximum 8 ports) secondary shapers must have the same name and rate.

Ports with Egress Secondary Shapers cannot be added to a configured LAG which do not match the Egress Secondary Shapers of the primary port.

Note 4 — Shapers are not removed from the port when the port is removed from a LAG.

Note 5 — The SAP reference to the Egress Secondary Shapers within a LAG is supported. Only the primary port of the SAP on the LAG is used to determine the list of Egress Secondary Shapers for the SAP.

When port members are removed from the LAG, care must be taken to ensure that the last port member is not removed if the LAG is referenced to a SAP. Shapers must exist on a LAG to be referenced on a SAP. See chapters 60 to 72 for more information.

20 Click on the Finish button. The Specify Member Properties form closes and the Configure LAG Members form reappears. A dialog box appears.

21 Click on the OK button.

22 Click on the Finish button. The Configure LAG Members form closes and the Create LAG form reappears.

23 Click on the Close button.

24 Use the Properties contextual menu to view information about the created LAG or to modify LAG parameters.

- The General tab displays the LAG ID, the LAG description and configured MAC address.
- The Link Aggregation Group tab displays the threshold parameters, cost information, and the primary port in the LAG, along with all the other LAG member ports.
- LAG member ports can be added from the LAG Members tab.
- Statistics, terminations, and fault information is available from the appropriate tabs.

25 Expand the LAG object in the navigation tree to view the created LAG groups. Expand the LAG group object to view the subgroup member ports, the priority, the subgroup ID, and the subgroup mode.

Procedure 17-24 To configure a LAG

Note — This procedure applies to 7210 SAS, 7450 ESS, 7710 SR, and 7750 SR nodes. See Procedure 17-26 for information about how to configure a LAG on an OmniSwitch.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Expand the LAGs object below a device in the Equipment view.

3 Right-click on a LAG object and choose Properties from the contextual menu. The LAG (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Configured Address
- Mode
- OLC State

5 If you are configuring a LAG on a 7210 SAS you can add the LAG to a split horizon group. See Procedure 17-6 for information about creating a 7210 SAS split horizon group.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - LAG form opens.

ii Choose a split horizon group and click on the OK button. The Select Split Horizon Group - LAG form closes and the Create LAG form refreshes with the split horizon group name.

Note 1 — A LAG cannot be added to or deleted from a split horizon group if it has a SAP configured on it.

Note 2 — A LAG cannot belong to more than one split horizon group; you must remove any split horizon groups from the LAG before you can add the LAG to a different split horizon group.

6 If you are configuring a LAG on a 7210 SAS, go to step 11.

7 Click on the Link Aggregation Group tab button.

8 Configure the parameters:

- Port Threshold
- Port Threshold Action
- Dynamic Cost

9 Click on the States tab button.

10 Configure the Administrative State parameter.

11 Click on the Access tab button.

12 Configure the QoS Adaptation parameter.

13 Click on the LACP tab button.

14 Configure the parameters:

- Administrative State
  The Administrative State parameter must be enabled before you can configure LACP and select a subgroup as an active subgroup.
- LACP Mode
- LACP Transmit Interval
- LACP Transmit Standby
- Auto-Generate
- Actor System ID
- Partner System ID
- LACP system ID
- LACP System Priority
- Actor System Priority
- Partner System Priority
- Hold Time (100s of milliseconds)
- Active Sub-Group Selection Criteria
- Slave to Partner

The LACP Mode, LACP Transmit Interval, and Actor Administration Key parameters are configurable when the Administrative State parameter is enabled.

15 Click on the Next button. The Configure LAG Members form opens.

16 Click on the LAG Members tab. To add LAG members, perform steps 14 to 22 of Procedure 17-23.

17 If the LAG that you are configuring is in Network mode, the Network Interfaces tab is displayed. Click on the Add button. The Create Network Interface form opens. Perform steps 4 to 45 of Procedure 27-4 in chapter 27 to create a network interface. Otherwise go to step 18.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button. The LAG (Edit) form closes.

Procedure 17-25 To create and configure an OmniSwitch LAG

Perform the following procedure to configure a static or dynamic LAG.

Workflow for a static LAG:

- create a static LAG on the local and remote switches
- assign ports to the LAG on the local and remote switches
- create a VLAN for the static LAG on the local and remote switches (optional)

Workflow for a dynamic LAG:

- create a dynamic LAG on the local (actor) and remote (partner) switches
- assign ports with the same actor administrative key (which allows them to be aggregated) to the local and remote LAG
- create a VLAN for the dynamic link aggregation group on the local and remote switch (optional)

Note — You can configure MVRP fixed ports/LAGs, 802.1 Q ports/LAGs, aggregate ports/LAGs, and VLAN Stacking Network ports/LAGs.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a LAG object below a device in the Equipment view and choose Create LAG from the contextual menu. The Create LAG - Define General Properties form opens.

3 Configure the parameters:

- LAG ID
- Auto-Assign ID
- Mode
- Administrative State
- Automatic VLAN Binding

The Automatic VLAN Binding parameter can only be configured for network LAGs.

4 Click on the Next button. The Create LAG - Configure LAG Parameters form opens.

5 Configure the parameters:

- Size
- Name
- Type

6 Perform one of the following:

a If you set the Type parameter to Static, go to step 13.

b If you set the Type parameter to Dynamic, go to step 7.

7 Click on the Next button. The Create LAG - Configure LACP form opens.

8 Configure the parameters:

- Actor Administration Key
- Actor System ID
- Partner System ID
- Actor System Priority
- Partner System Priority
- Partner Administration Key

9 Click on the Finish button. The Create LAG - Wizard Completed form opens.

10 Enable the View the newly created interface check box if you need to view the LAG properties.

11 Click on the Close button. The Create LAG form closes.

See Procedure 17-26 in this section for information about adding members to a dynamic LAG.

12 Go to step 23.

13 Click on the Next button. The Create LAG - Configure LAG Members form opens.

14 Click on the Add button to add ports to the LAG. The Create LAG Member - Only show compatible ports form appears.

15 Configure the Show Only Compatible Ports parameter.

16 Click on the Next button. The Create LAG Member - Select Ports form opens.

17 Click on the Refresh button to display a list of compatible ports. Choose ports from the list to construct the LAG.

Add ports to the LAG as follows:

- Choose up to the maximum number of ports you require from the list of ports. You can select more than one port at a time from the list.
- Click on the Next button. The Specify the Member Properties form opens.

Note 1 — If there are no compatible ports to choose from and you have decided that you want to edit some of the existing ports that are not compatible to be compatible, disable the Show compatible ports only parameter. Click on the Next button. Choose ports to edit from the list and click on the Properties button.

Note 2 — Mobile, UNI, and NNI ports cannot be members of a LAG.

Note 3 — Only network ports can be members of a network LAG and only access ports can be members of an access LAG.

18 Click on the Finish button. A dialog box appears.

19 Click on the OK button. The Create LAG - Configure LAG Members form displays the LAG members.

20 Click on the Finish button. The Create LAG - Wizard Completed form opens.

21 Enable the View the newly created interface check box if you need to view the LAG properties.

22 Click on the Close button to close the form.

23 Use the Properties contextual menu to view information about the created LAG or to modify LAG parameters.

- The General tab displays the LAG ID and LAG description.
- The Link Aggregation Group tab displays the primary port in the LAG along with all the other LAG member ports.
- LACP parameters can be modified from the LACP tab.
- LAG member ports can be added from the LAG Members tab.
- A UNI policy can be applied to a LAG used as a SAP in a stacked VLAN from the Policies tab.
- An MVRP configuration and VLAN restriction can be applied to a LAG from the MVRP tab. If a port is a LAG member, you cannot modify parameters on the MVRP general tab on that physical port.
- Statistics, network interfaces, and fault information is available from the appropriate tabs.

24 Expand the LAG object in the navigation tree to view the created LAG groups and the unassigned dynamic LAG members group. Expand the LAG group object to view the subgroup member ports, the priority, and the LACP state. Expand the Unassigned Dynamic LAG Members group object to view dynamic LAG members that have not been assigned to a dynamic LAG group.

Procedure 17-26 To create and configure OmniSwitch dynamic LAG members

Perform the following procedure to add members to a dynamic LAG and modify existing dynamic LAG members.

LAG members are not added during the creation of the dynamic LAG, as they are with static LAGs. When a new dynamic LAG member is created it is placed into the Unassigned Dynamic LAG Members object. The new dynamic LAG members remain under the Unassigned Dynamic LAG Members object until the system identifies a LAG with matching properties. When an unassigned LAG member joins a LAG, the member is removed from the Unassigned Dynamic LAG Members object and added to the appropriate LAG object

1 Right click on the Unassigned Dynamic LAG Members object in the navigation tree and choose Create LAG Members from the contextual menu. The Create LAG Member - Only show compatible ports form appears.

2 Configure the Show Only Compatible Ports parameter.

3 Click on the Next button. The Create LAG Member - Select Ports form opens.

4 Click on the Refresh button to display a list of compatible ports. Choose ports from the list to construct the LAG.

Add ports to the LAG as follows:

- Choose up to the maximum number of ports you require from the list of ports. You can select more than one port at a time from the list.
- Click on the Next button. The Specify the Member Properties form opens.

Note 1 — If there are no compatible ports to choose from and you have decided that you want to edit some of the existing ports that are not compatible to be compatible, disable the Show compatible ports only parameter. Click on the Next button. Choose ports to edit from the list and click on the Properties button.

Note 2 — For all ports in an LAG, you must disable auto-negotiation, configure the same speed, and set the ports to full duplex. Mobile ports cannot be part of a LAG.

5 Configure the parameters:

- Priority
- System Id
- System Priority
- Admin Key
- Admin State

6 Click on the Finish button. The Create LAG - Wizard Completed form opens.

7 Enable the View the newly created interface check box if you need to view the LAG properties.

8 Click on the Close button to close the form.

9 If you need to modify a dynamic LAG member, go to step 10.

10 Right click on a LAG member and choose Properties from the contextual menu.

11 The LAG Member (edit) form opens on the General tab.

12 Configure the Priority parameter in the LAG Member panel, if required.

13 Configure parameters in the Actor panel, if required.

- System Id
- System Priority
- Admin Key
- Admin State

14 Configure parameters in the Partner panel, if required.

- Admin Key
- Admin System Id
- Admin Port
- Admin System Priority
- Admin Port Priority
- Admin State

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button to save your changes and close the form.

17 Click on the Close button to close the form.

Procedure 17-27 To assign a card type

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Expand the tree view for the required device.

3 Expand the tree view for the required shelf object of the selected device.

4 Right-click on an empty Card Slot object in the Equipment view choose Configure Card from the contextual menu. The Card Slot (Create) form opens.

5 Configure the parameters:

- Capability
- Assigned Card Type
- Shutdown IOM for Memory Parity Errors
- OLC State

Note — The correct chassis mode must be configured for the assigned card types. The chassis mode determines the behavior of the card and establishes the scaling limits and available features. See Procedure 17-33 for more information.

6 Click on the OK button. The Card Slot (Create) form closes.

The card and slot appear in the navigation tree and in the inventory list of the equipment manager.

Procedure 17-28 To add 9500 MPR card protection

The 9500 MPR supports card protection for all card types. EPS card protection for the CORE-ENH card in slot 1 is automatically configured by the system when an optional spare CORE-ENH card is provisioned into slot 2. Radio modem and 32 x DS1/E1 cards in slots 3, 5, and 7 can be protected by corresponding identical cards in slots 4, 6, and 8. Protection for cards in slots 3, 5, and 7 must be configured. The protected card is referred to as the main card and the protecting card is referred to as the spare card. Use the following procedure to configure optional card protection for radio modem and 32 x DS1/E1 cards.

Note 1 — All cross connections, flow-ids, and sync sources must be removed from the port under the spare card slot before protection can be enabled.

Note 2 — To configure protection type 1+1 FD on Radio, the Mode cannot be Adaptive Modulation.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 9500 MPR card slot object in the equipment view that you need to configure and choose Properties from the contextual menu. The Card Slot (Edit) form opens with the General tab displayed.

3 Click on the Protection tab button.

4 Configure the following parameters on the main/spare card:

- Protection Type
- Restoration Criteria
- Commands

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Card Slot (Create) form closes.

7 Verify that the protection has been enabled. The status of the main card should be Active and the status of the spare card should be Standby.

Procedure 17-29 To remove 9500 MPR card protection

Note — If 1+1 HSB is configured as the protection type for a Radio card, the transmitter must be muted from the NEtO to remove the protection.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on the 9500 MPR main or spare card slot object in the equipment view and choose Properties from the contextual menu. The Card Slot (Edit) form opens with the General tab displayed.

3 Click on the Protection tab button.

4 Set the Protection Type parameter to No Protection.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Card Slot (Create) form closes.

7 Verify that the protection has been removed from the previously main and spare cards.

Procedure 17-30 To add 9500 MPR port protection

Note 1 — The Protection tab button only appears for MPT-type ports of EAS modules if the corresponding spare port has been configured as MPT.

Note 2 — All cross connections, flow-ids, and sync sources must be removed from the port under the spare card slot before protection can be enabled.

Note 3 — To configure protection type 1+1 FD on MPT/Radio, the Mode cannot be Adaptive Modulation.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 9500 MPR port object in the equipment view that you need to configure as the main port of the protection pair and choose Properties from the contextual menu. The Port (Edit) form opens with the General tab displayed.

3 Click on the Protection tab button.

4 Configure the Protection Type parameter on the main/spare MPT port.

5 For radio ports, configure the parameters:

- Restoration Criteria in the Receiver Protection Scheme Parameters panel
- Commands in the Receiver Protection Scheme Parameters panel
- Restoration Criteria in the Transmitter Protection Scheme Parameters panel.
- Commands in the Transmitter Protection Scheme Parameters panel.

Note — For Protection Type 1+1 FD, Transmitter Protection Scheme parameters are not applicable.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Port (Create) form closes.

8 Verify that the protection has been enabled. The status of the main port should be Active and the status of the spare port should be Standby.

Procedure 17-31 To remove 9500 MPR port protection

Note — If 1+1 HSB is configured as the protection type for an MPT port, the transmitter must be muted from the NEtO to remove the protection.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on the 9500 MPR spare port object in the equipment view and choose Properties from the contextual menu. The Port (Edit) form opens with the General tab displayed.

3 Click on the Protection tab button.

4 Set the Protection Type parameter to No Protection.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Port (Create) form closes.

7 Verify that the protection has been removed from the previously main and spare ports.

Procedure 17-32 To configure switch fabric multicast ingress replication rates

Perform this procedure to configure the total multicast replication rates for primary and secondary ingress paths for each switch fabric multicast plane.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a shelf object in the equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the Multicast tab button.

4 Configure the parameters:

- Primary Multicast Bandwidth (mbps)
- Secondary Multicast Bandwidth (mbps)
- Primary Multicast Bandwidth for Dual-SFM Mode (mbps)
- Secondary Multicast Bandwidth for Dual-SFM Mode (mbps)

5 Click on the OK button. The Shelf (Edit) form closes.

Procedure 17-33 To configure the chassis mode of a device

Perform this procedure to configure the chassis mode for the device. See chapter 15 for more information about chassis modes.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a shelf object in the equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Administrative Mode
  If you downgrade the administrative chassis mode, the device must be rebooted to change the operational chassis mode.
- Force Mode
  Forcing a chassis mode change does not change the operational chassis mode unless there is a compatible card type equipped on the device. See chapter 15 for more information about the minimum card type that must be installed for each chassis mode.

4 Click on the OK button. The Shelf (Edit) form closes.

Procedure 17-34 To configure timing synchronization

Perform this procedure to configure timing synchronization. See "Timing synchronization" in chapter 15 for more information about timing synchronization.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a shelf object in the equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the Timing tab button.

4 Configure the parameters, as required:

- Reference Input Mode (revertive)
- Quality Level Reference
- First Timing Reference Input
- Second Timing Reference Input
- Third Timing Reference Input
- Type
- Interface Name
- Port or Channel Name
- Administrative State
- Quality Level Override
- Interface Type
- Input Administrative State
- Output Administrative State
- Output Line Length
- SSM
- Input Type
- Impedance Type
- Output Type
- Quality Level

Note — The parameters that appear on the Shelf (Edit) form may vary, depending on the device type and version you are configuring.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button.The Shelf (Edit) form closes.

Procedure 17-35 To modify the IEEE 1588 PTP clock on the 7705 SAR

Perform this procedure to modify the IEEE 1588 PTP clock on a 7705 SAR that is configured as an IEEE 1588 PTP client. See Procedure 17-34 for more information about how to configure the 7705 SAR as a PTP client.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 7705 SAR shelf object in the equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the Timing tab button.

4 Click on the PTP Clock Properties button. The PTP Clock (Edit) form opens.

5 Configure the Domain parameter.

6 Click on the OK button. A dialog box appears.

7 Click on the OK button. The PTP Clock (Edit) form closes.

8 Click on the OK button to save the configuration and close the Shelf (Edit) form.

Procedure 17-36 To modify the IEEE 1588 PTP port on the 7705 SAR

Perform this procedure to modify the IEEE 1588 PTP port on a 7705 SAR that is configured as an IEEE 1588 PTP client. See Procedure 17-34 for more information about how to configure the 7705 SAR as a PTP client.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 7705 SAR shelf object in the equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the Timing tab button.

4 Click on the PTP Port Properties button. The PTP Port (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Master 1 Address
- Master 2 Address
- Announce Receive Timeout
- Announce Interval
- Sync Interval

6 Click on the Recovered Clock History Master One tab button to view master 1 clock recovery statistics.

7 Click on the Recovered Clock History Master Two tab button to view master 2 clock recovery statistics.

8 Click on the OK button. The PTP Port (Edit) form closes.

9 Click on the OK button to save the configuration and close the Shelf (Edit) form.

Procedure 17-37 To configure auxiliary alarm definitions on the 7705 SAR

Perform this procedure to configure auxiliary alarm definitions for the auxiliary alarms daughter card on a 7705 SAR.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 7705 SAR shelf object in the equipment view and choose Properties from the menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the External Alarms tab button.

4 On the Auxiliary Alarm Definitions sub-tab, click on the Add button. The Auxiliary Alarm Definition (Create) form opens.

5 Configure the following parameters:

- ID
- Auto-Assign ID
- Description
- Administrative State
- Severity

6 Click on the Inputs tab button and configure the following parameters:

- Trigger Rule
- Analog Threshold (mV)
- Operation
- Input 1 through Input 8 (as required)

7 Click on the Outputs tab button and configure the following parameters:

- Log Event
- Update Chassis Relays

8 Click on the OK button in the Auxiliary Alarm Definition (Create) form. A dialog box appears.

9 Click on the OK button.

10 Click on the OK button to save the configuration and close the Shelf (Edit) form.

Procedure 17-38 To configure OmniSwitch PoE Ports

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a slot object in the Equipment view and choose Properties from the contextual menu. The Card Slot (Edit) form opens with the General tab displayed.

3 Click on the PoE tab button.

4 Configure the parameters:

- Slot Priority
- Power State
- Port Maximum Power (MilliWatts)
- Maximum Power (Watts)
- Enable Priority Disconnect
- Enable Power Capacitor Detection
- Combo Port

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 17-39 To configure OmniSwitch stacks

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a slot object in the Equipment view and choose Properties from the contextual menu. The Card Slot (Edit) form opens with the General tab displayed.

3 Click on the Stack Configuration tab button.

4 Configure the parameters:

- Saved Slot NI Number
- Command Action
- Stacking Action

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 17-40 To configure an OmniSwitch CPU temperature threshold

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a slot object in the Equipment view and choose Properties from the contextual menu. The Card Slot (Edit) form opens with the General tab displayed.

3 Click on the Hardware Environment tab button.

4 Configure the Temperature Threshold (Celsius) parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 17-41 To configure an MDA

1 Choose Equipment from the navigation tree view selector.

2 Navigate to a daughter card slot object. The path is Network→NE→Card Slot→Daughter Card Slot.

3 Perform one of the following.

a To add a daughter card to an empty daughter card slot, right-click on the daughter card slot and choose Configure Daughter Card from the contextual menu. The Daughter Card Slot (Create) form opens.

b To modify an existing daughter card, right-click on the daughter card slot and choose Properties from the contextual menu. The Daughter Card Slot (Edit) form opens.

4 Configure the parameters:

- Assigned Daughter Card Type
- In MDA Carrier Module Slot
- OLC State

Note — The Assigned Daughter Card Type and In MDA Carrier Module Slot parameters are configurable only during daughter-card creation.

5 If you are creating a daughter card on a 7710 SR, perform the following steps.

i Click on the MDA Carrier Module tab button.

ii Configure the Assigned MCM Card Type parameter.

6 Click on the Apply button.

7 Click on the Daughter Card tab button.

8 Configure the parameters:

- Administrative State
- Synchronous Ethernet

9 Configure the following parameters in the Voice panel, if required:

- Companding Law
- Signalling Type

10 Perform the following steps to configure named buffer pools, if required.

Note — You must enable pool mode on the parent I/O card to enable named buffer pool support. See Procedure 17-46 for more information.

i Click on the Select button beside the Name parameter in the Ingress Pool Policy panel. The Select Ingress Pool Policy form opens.

ii Choose a policy in the list and click on the OK button. The Select Ingress Pool Policy form closes, and the policy name is displayed in the Ingress Pool Policy panel.

iii If you are configuring an HSMDA daughter card, go to step 11.

Note — HSMDA daughter cards support only ingress named buffer pool policies, and not egress named buffer pool policies.

iv Click on the Select button beside the Name parameter in the Egress Pool Policy panel. The Select Egress Pool Policy form opens.

v Choose a policy in the list and click on the OK button. The Select Egress Pool Policy form closes, and the policy name is displayed in the Egress Pool Policy panel.

11 Perform the following steps to configure HSMDA pool policies, if required.

Note — You must enable pool mode on the parent I/O card to enable HSMDA pool support. See Procedure 17-46 for more information.

i Click on the Select button in the Ingress HSMDA Pool Policy panel. The Select Ingress HSMDA Pool Policy form opens.

ii Choose a policy in the list and click on the OK button. The Select Ingress HSMDA Pool Policy form closes, and the policy is displayed in the Ingress HSMDA Pool Policy panel.

iii Click on the Select button in the Egress HSMDA Pool Policy panel. The Select Egress HSMDA Pool Policy form opens.

iv Choose a policy in the list and click on the OK button. The Select Egress HSMDA Pool Policy form closes, and the policy is displayed in the Egress HSMDA Pool Policy panel.

12 Perform the following steps to add a fabric profile, if required.

i Click on the Select button in the Network Ingress Fabric Profile panel. The Select Fabric Profile form opens.

ii Choose a profile in the list and click on the OK button. The Select Network Ingress Fabric Profile form closes, and the profile name is displayed in the Network Ingress Fabric Profile panel.

iii Click on the Select button in the Access Ingress Fabric Profile panel. The Select Fabric Profile form opens.

iv Choose a profile in the list and click on the OK button. The Select Access Ingress Fabric Profile form closes, and the profile name is displayed in the Access Ingress Fabric Profile panel.

13 Perform the following steps to add an HSMDA scheduler policy, if required.

i Click on the Select button in the HSMDA Scheduler panel. The Select HSMDA Scheduler form opens.

ii Choose a scheduler in the list and click on the OK button. The Select HSMDA Scheduler form closes, and the scheduler name is displayed in the HSMDA Scheduler panel.

14 Perform steps 2 to 5 of Procedure 17-43 to configure IMPM on the daughter card, if required.

15 If you configure named buffer pools in step 10, perform the following steps to configure the associated Q1 pools. Otherwise, go to step 16.

Note — You cannot use this step to configure 7710 SR QoS policies.

i Click on the QoS Pool tab button.

ii Choose a pool in the list and click on the Properties button. The QoS Pool (Edit) form opens.

iii Configure the parameters:

- Reserved CBS (%)
- Default Reserved CBS

iv Click on the Select button in the Slope Policy panel. The Select Slope Policy - QoS Pool form opens.

v Choose a policy in the list and click on the OK button. The Select Slope Policy - QoS Pool form closes, and the slope policy name is displayed in the Slope Policy panel.

16 Click on the OK button. A dialog box appears.

If you are adding a new daughter card, the daughter card and the contained ports are displayed in the navigation tree.

17 Click on the Yes button. The Daughter Card Slot properties form closes.

Procedure 17-42 To configure egress WRED queue control on an IOM 3 or IMM forwarding plane

Perform this procedure to configure the egress WRED queue control function on an IOM 3 or IMM.

1 Right-click on a card slot object in the navigation tree and choose Properties from the contextual menu. The Card Slot (Edit) form opens with the General tab displayed.

2 Click on the Forwarding Plane tab button.

3 Choose an entry in the list and click on the Properties button. The Forwarding Plane (Edit) form opens.

4 Configure the Egress WRED Queue Control parameters:

- Administrative State
- Buffer Allocation Min (%)
- Buffer Allocation Max (%)
- Reserved CBS Min (%)
- Reserved CBS Max (%)

5 Click on the Select button in the Slope Policy panel. The Select Slope Policy - Forwarding Plane form opens.

6 Choose a policy in the list and click on the OK button. The Select Slope Policy - Forwarding Plane form closes, and the slope policy name is displayed in the Slope Policy panel.

7 Click on the OK button. The Forwarding Plane (Edit) form closes.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 17-43 To configure IMPM on an MDA

Perform this procedure to configure IMPM on an MDA that is not installed in a 2 x XP MDA IOM 3 or an IMM.

Note — See Procedure 17-44 for information about configuring IMPM on a 2 x XP MDA IOM 3 or IMM.

1 Perform steps 1 to 7 of Procedure 17-41.

2 Configure the following parameters in the Daughter Card Details panel:

- High Bandwidth Source
- High Bandwidth Multicast Traffic Taps Group
- High Bandwidth Alarm

3 Click on the Select button in the BW policy panel to choose a multicast bandwidth policy. The Select BW Policy form opens.

4 Choose a policy in the list and click on the OK button. The Select BW Policy form closes and the policy name is displayed in the BW Policy panel.

Note — The multicast bandwidth policy named “default” cannot be modified or deleted.

5 Configure the following parameters in the Multicast Path Management panel:

- Admin State
- Primary Path Limit (mbps)
- Secondary Path Limit (mbps)
- Ancillary Path Limit (mbps)

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Daughter Card Slot properties form closes.

Procedure 17-44 To configure IMPM on a 2 x XP MDA IOM 3 or IMM forwarding plane

Perform this procedure to configure IMPM on a 2 x XP MDA IOM 3 or an IMM.

Note — See Procedure 17-43 for information about configuring IMPM on an MDA that is not installed in a 2 x XP MDA IOM 3 or in an IMM.

1 Choose Equipment from the navigation tree view selector.

2 Navigate to a card slot object. The path is Network→NE→Card Slot.

3 Right-click on the card slot object and choose Properties from the contextual menu. The Card Slot (Edit) form opens with the General tab displayed.

4 Click on the Forwarding Plane tab button.

5 Choose an entry in the list and click on the Properties button. The Forwarding Plane (Edit) form opens.

6 Click on the Clear button to remove the selected policy. The Select button in the BW Policy panel is enabled.

7 Click on the Select button in the BW Policy panel. The Select BW Policy form opens.

8 Choose a policy in the list and click on the OK button. The Select BW Policy form closes, and the policy name is displayed in the BW Policy panel.

9 Configure the Admin State parameter.

10 Configure the following parameters:

- High Bandwidth Source
- High Bandwidth Multicast Traffic Taps Group
- High Bandwidth Alarm

11 Click on the OK button. The Forwarding Plane (Edit) form closes.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 17-45 To view operational multicast channel properties on an MDA

Perform this procedure to view specific information about an operational multicast channel on an MDA that is configured to use an Ingress Multicast Bandwidth policy.

Note — You can also view operational multicast channel information in the following locations:

- the Mcast Path Mgmt tab on the properties form of a VPLS or VPRN service site
- the Mcast Path Mgmt Channels tab on the properties form of a routing instance.

Each properties form contains information about the ingress MDA of each operational channel.

1 Choose Equipment from the navigation tree view selector.

2 Navigate to a daughter card slot object. The path is Network→NE→Card Slot→Daughter Card Slot.

3 Right-click on the daughter card slot object and choose Properties from the contextual menu. The Daughter Card Slot (Edit) form opens with the General tab displayed.

4 Click on the Mcast Path Mgmt Channels tab button.

5 Click on the Search button. A list of operational channels is displayed.

6 View the information, which includes the service site or routing instance associated with the channel, and the following properties:

Note — Channel information is displayed only when the MDA receives multicast traffic for a previously configured multicast group.

- Group Address—the operational channel multicast group address
- Source Address—the operational channel multicast source address
- Bandwidth—the operational bandwidth of the channel
- Administrative Bandwidth—the administrative bandwidth of the channel
- Last Highest Bandwidth—the value of the multicast bandwidth that is currently allocated to the channel forwarding path on the MDA. This value is calculated based on periodic statistics polls and represents the highest recorded bandwidth value since the most recent restart of the bandwidth update timer for the channel.
- Second Highest Bandwidth—the second-highest recorded bandwidth value for the channel since the most recent restart of the bandwidth update timer. The value is calculated based on periodic statistics polls and is reset to zero every time the bandwidth update timer for the channel is restarted.
- BW Update Timer expiration—the time that remains before the bandwidth update timer for the channel expires
- Current Path—the path that the channel traffic uses to reach the switching fabric; the path value is primary, secondary, or ancillary
- Explicit Path—indicates whether the current path is explicitly specified by a Multicast Info Policy
- Preference Level—the preference level of the channel
- Black-Hole—whether the channel is in the Black-Hole state
- Black-Hole Rate—specifies the bandwidth rate, in kb/s, at which the channel enters the Black-Hole state

7 Close the Daughter Card Slot (Edit) form.

Procedure 17-46 To enable named pool mode

Perform this procedure to allow named pools to be created for an MDA. Set the pool mode parameter when you are configuring the card.

Caution — The Pool Mode parameter can be enabled and disabled at anytime, however changing the pool mode resets the IOM when MDAs are provisioned on the slot. If MDAs are not provisioned the IOM is not reset.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a slot object in the navigation tree and choose Properties from the contextual menu. The Card Slot (Edit) form opens with the General tab displayed.

3 Click on the IO Card tab button.

4 Configure the Pool Mode parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Card Slot (Edit) form closes.

LLDP

Link Layer Discovery Protocol is a neighbor-discovery protocol that allows a network access device to advertise its identity and capabilities to other stations attached to the same physical IEEE 801 LAN. LLDP is one of the global node element attributes that you configure from the 5620 SAM equipment navigation tree.

LLDP is available in 5620 SAM Release 7.0 R1 and later, and is only applicable for devices using Ethernet connectivity. It is supported by the 7210 SAS-M24F, 7210 SAS-M24F2XFP, and 7210 SAS-M24F2XFP [ETR] (Release 3.0 R1 and later), and by the 7450 ESS, 7710 SR, and 7750 SR, all at Release 7.0 or later, and the OmniSwitch at Release 6.3.1 or later.

See "LLDP" in section 27.1 for more information about LLDP.

Procedure 17-47 To enable LLDP on a router

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to the router icon by choosing Routing→Router.

3 Right-click on the router icon and choose Properties. The Network Element (Edit) form opens.

4 Enable LLDP by performing the following steps.

i Click on the Globals tab button.

ii Configure the parameters:

- Administrative Status
- Transmission Interval (Seconds)
- Transmission Multiplier
- Re-Init Delay (Seconds)
- Notification Interval (Seconds)
- Transmission Delay (Seconds)
- Maximum Consecutive Transmissions
- Fast Transmission Interval (Seconds)
- PDUs in Fast Transmission

The Administrative Status, Maximum Consecutive Transmissions, Fast Transmission Interval (Seconds), and PDUs in Fast Transmission parameters do not apply to the OmniSwitch.

The Transmission Delay (Seconds) parameter only applies to the OmniSwitch.

5 Click on the OK button. A dialog box appears.

6 Confirm the action. The Network Element (Edit) form closes.

7 Configure the applicable router ports to fully enable LLDP, as described in step 31 in Procedure 17-61 and step 11 in Procedure 17-62. See step 2 in Procedure 17-8 for information about how to set global node element attributes, including LLDP.

Procedure 17-48 To create a chassis-level PBB configuration

Perform this procedure to provide the PBB MAC name configuration at the NE level.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on an NE in the Equipment view and choose Properties from the contextual menu. The Network Element form opens with the General tab displayed.

3 Click on the Globals tab button.

4 Click on the Service tab button and configure the parameters:

- PBB Source Backbone MAC Address
- MAC Notification Interval (seconds)
- MAC Notification Count

5 Click on the MAC Name tab button and click on the Add button. The PBB MAC Name (Create) form opens with the General tab displayed. Configure the parameters:

- MAC Name
- MAC Address

6 Click on the OK button.

Procedure 17-49 To manage OmniSwitch running configuration

Caution — When you reboot an OmniSwitch that is in service it is service-affecting. Ensure that the reboot activity occurs during a maintenance window.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a shelf object in the Equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the Software Control Module tab button.

4 Configure the Command to Apply parameter.

a If you specify Copy certified to working, configure the Active Timeout parameter.

b If you specify Reload from working, configure the Delayed Activation Timer parameter.

5 Click on the OK button. The Shelf (Edit) form closes.

Procedure 17-50 To manage 9500 MPR running software

Perform this procedure to manage the software in the 9500 MPR committed and standby banks. You can upgrade or downgrade the running software version on a 9500 MPR. See chapter 21 for information about creating software upgrade policies and performing software upgrades.

Caution — When you reboot a 9500 MPR that is in service it is service-affecting. Ensure that the reboot activity occurs during a maintenance window.

Warning — A 9500 MPR may require a firmware upgrade before a device software upgrade. To avoid a service outage, ensure that the device firmware version supports the software upgrade. See the device software Release Notes to obtain information about firmware and software version compatibility.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a shelf object for a 9500 MPR that you need to upgrade or downgrade and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the Software Bank Details tab button. The committed and standby software information is displayed. The committed software is the software currently running on the 9500 MPR. The standby software is new software that was uploaded to the 9500 MPR or formerly committed software.

4 Verify that the operational state of the standby software is Enabled, by examining the Operational State column of the displayed list.

You can also examine the Software Version of the standby and committed software. If the software version of the standby software is newer than the committed software version, the 9500 MPR can be upgraded. If the standby software version is older than the committed software version, the 9500 MPR can be downgraded.

5 Choose the standby entry from the displayed list.

6 Click on the Properties button.

7 The MPRSoftwarePackage (Edit) form opens with the Software Bank Details tab displayed.

8 Configure the Activation parameter.

9 Click on the OK button. The MPRSoftwarePackage (Edit) form closes. The entry in the Activation column for the standby software should be the same as the option chosen in step 8.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. When the standby and committed software versions are different or the forced activation option is selected, the 9500 MPR reboots using the standby software. If the standby and committed software versions are the same and the activation option is chosen, the 9500 MPR does not reboot and the Shelf (Edit) form closes.

12 When the 9500 MPR reboots you can confirm that the 9500 MPR is running the software stored in the former standby bank. The former standby software is the committed software and the previous committed software is the standby software.

Procedure 17-51 To configure OmniSwitch Health Monitoring

The OmniSwitch Health Monitoring function monitors the consumable resources, such as bandwidth and CPU usage, of the switch. This function monitors the switch and at fixed intervals collects the current values for each resource being monitored. You can specify resource threshold limits and when a resource value falls above or below a threshold, traps are sent to the 5620 SAM.

Perform the following procedure to configure health monitoring on an OmniSwitch.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on an OmniSwitch shelf object in the Equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the Health Monitoring tab button.

4 Configure the following parameters:

- Rx Threshold (%)
- TxRx Threshold (%)
- Temperature Threshold Unit
- Temperature Threshold
- Memory Threshold (%)
- CPU Threshold (%)
- Sampling Interval (seconds)

5 Click on the Statistics tab button and search for Card Health Stats (Physical Equipment) or Device Health Stats (Physical Equipment) to view card statistics or chassis statistics respectively. Statistics can also be viewed from the card-level statistics tab.

6 Click on the Faults tab button to view alarm information.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Shelf (Edit) form closes.

Procedure 17-52 To start and stop a Webview or Secure Webview session on an OmniSwitch

Perform the following procedure to start and stop a Webview or Secure Webview session on an OmniSwitch.

1 To start a Webview or Secure Webview session:

i Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

ii Right-click on a discovered OmniSwitch in the Equipment view and choose Launch Webview or Launch Secure Webview from the contextual menu. A web browser starts and the Webview or Secure Webview login screen appears.

Note — An alternative method of launching a Webview or Secure Webview session is to right-click on a discovered OmniSwitch in the Equipment view. Select Equipment Window from the contextual menu. The Equipment Window form opens. Select the Launch Webview or Launch Secure Webview button on the form.

iii Enter your user name and password. After a successful login, the Chassis Management Home Page appears.

2 To stop a Webview or Secure Webview session:

i Click on the Log Out text at the top of the Webview or Secure Webview window. A Confirm Log Out dialog box appears.

ii Click on the Log Out button to end the Webview or Secure Webview session.

See the appropriate OmniSwitch *Switch Management Guide* for information about configuring and using Webview or Secure Webview.

Procedure 17-53 To start the 9500 MPR external element manager from the 5620 SAM GUI

Perform the following procedure to start the 9500 MPR external element manager, NEtO, from the 5620 SAM GUI.

Warning — When you use the 5620 SAM to manage the 9500 MPR, use of the NEtO external element manager must be restricted to configuring only radio modem card parameters. If you use NEtO to configure any other parameters, services can be affected and can seriously impact network management and 5620 SAM performance.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a discovered 9500 MPR in the Equipment view and choose External Element Manager from the contextual menu. The NEtO main view screen appears.

See the appropriate 9500 MPR *User Guide* for information about configuring and using the NEtO external element manager.

Procedure 17-54 To configure an 802.3ah EFM OAM diagnostic

EFM OAM, which is described in 802.3ah, clause 57, defines the Ethernet OAM sublayer, which provides mechanisms for monitoring link operation, such as remote fault indication and remote loopback control.

The OAM information is transported in slow protocol frames, which are called OAMPDUs. OAMPDUs contain the appropriate control and status information that is used to monitor, test, and troubleshoot OAM-enabled links. OAMPDUs traverse a single link, that is passed between peer OAM entities.

802.3ah EFM OAM supports:

- EFM OAM capability discovery
- active and passive modes
- remote failure indication
- local and remote loopbacks
- EFM OAMPDU tunneling
- high-resolution EFM OAM timers

The EFM OAM diagnostic is supported for on the 7710 SR, 7750 SR, 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7450 ESS, and for 7705 SAR Ethernet ports in network mode.

For OmniSwitch NEs, see Procedure 17-55.

Caution — Performing an 802.3ah diagnostic is service-affecting. Ensure that you consider the implications of performing this test before you proceed.

Note — In order for the 802.3ah diagnostic to be successful, the local and peer ports must support the 802.3ah protocol, and be operationally and administratively up.

When a port is in loopback mode, service mirroring does not work if the port is a mirror source or a mirror destination.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

3 Click on the Ethernet tab button. The Ethernet port configuration form opens with the General tab displayed.

4 Click on the 802.3ah tab button. The 802.3ah form opens.

5 Configure the parameters:

- Administrative State
- Tunneling
- Mode
- Transmit Interval (x100 ms)
- Multiplier (Intervals)
- Received Remote Loopback Requests
- Set Remote Loopback
- Set Local Loopback

6 Click on the Apply button. A dialog box appears.

7 Click on the Yes button.

8 Click on the Resync button.

9 The 802.3ah form is updated with the results of the 802.3ah diagnostic. The values that are displayed on the form depend on the configuration of the local and peer ports.

Tables 17-3, 17-4, and 17-5 describe the displayed information.

Table 17-3 802.3ah EFM OAM results

Parameter	Value	Description
Operational Status (dot3OamOperStatus)	Disabled	The Administrative State parameter on the local port is set to Disabled.
	Active Send Local	The Mode parameter is set to Active and the local port is discovering the peer port EFM OAM capabilities.
	Passive Wait	The Mode parameter is set to Passive and the local port is waiting to receive OAMPDUs from the peer device.
	Send Local and Remote	The local port discovered the peer but has not yet accepted or rejected the configuration of the peer. The local port may determine that the peer port is not compatible and decline OAM peering.
	OAM Peering Locally Rejected	The local port declined OAM peering.
	Send Local and Remote Ok	The local port accepted OAM peering.
	OAM Peering Remotely Rejected	The remote port declined OAM peering.
	Operational	The local and remote ports accepted the OAM peering.
	Non-operational Half Duplex	The Administrative State parameter is set to Enabled but the local port is in half-duplex mode.
	Link Fault	The link detected a fault and is transmitting OAMPDUs with a link fault indication.
Max. PDU Size (dot3OamMaxOamPduSize)	PDU size	The largest OAMPDU size, in bytes, that is supported by the local port: Minimum is 64 Maximum is 1518 Default is 1514
Configuration Revision (dot3OamConfigRevision)	0 to 65 535	The configuration revision of the OAM entity obtained from the latest OAMPDU sent by the OAM entity. The value is used by OAM entities to indicate that configuration changes occurred that may require the peer OAM entity to re-evaluate whether OAM peering is allowed.
Functions Supported (dot3OamFunctionsSupported)	Event Support	The port can send and receive event notification OAMPDUs.
	Loopback Support	The port can initiate and respond to loopback commands.
	Unidirectional Support	The port supports the transmission of OAMPDUs on links that operate in unidirectional mode.
	Variable Support	The port can send and receive variable request and response OAMPDUs.

(1 of 2)

Parameter	Value	Description
Loopback Status (dot3OamLoopbackStatus)	No Loopback	The port is not in a loopback condition.
	Initiating Loopback	The local device initiated a loopback, sent a loopback OAMPDU and is waiting for a response from the peer port.
	Remote Loopback	The peer port is in loopback mode.
	Terminating Loopback	The local port is in the process of terminating a loopback on the peer port.
	Local Loopback	The peer port has put the local port into loopback mode.
	Unknown	An OAMPDU that contains an unexpected message was received by the local port.

(2 of 2)

Table 17-4 802.3ah EFM OAM Statistics

Statistics	Displayed Value	Description
Frames Lost Due to OAM(dot3OamFramesLostDueTo Oam)	*Number of frames*	The number of frames that were dropped by the OAM multiplexer. Discontinuities of this counter can occur under some conditions.
Information Rx (dot3OamInformationRx)	*Number of OAMPDUs*	The number of information OAMPDUs received on this interface
Information Tx (dot3OamInformation Tx)	*Number of OAMPDUs*	The number of information OAMPDUs transmitted on this interface. Discontinuities of this counter can occur can occur under some conditions.
Loopback Control Rx (dot3OamLoopbackControlRx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs received on this interface
Loopback Control Tx (dot3OamLoopbackConrolTx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs transmitted on this interface
Unsupported Codes Rx (dot3OamUnsupportedCodesRx)	*Number of OAMPDUs*	The number of OAMPDUs received on this interface with an unsupported opcode
Unsupported Codes Tx (dot3OamUnsupportedCodesTx)	*Number of OAMPDUs*	The number of OAMPDUs transmitted on this interface with an unsupported opcode

Table 17-5 802.3ah EFM OAM peer information

Peer Information	Displayed Value	Description
Peer MAC Address (dot3OamPeerMacAddress)	*MAC address*	The MAC address of the peer port. The MAC address is contained in the received OAMPDU.
Peer Vendor OUI (dot3OamPeerVendorOui)	*OUI*	The OUI of the OAM peer. The OUI is part of the peer MAC address contained in the received OAMPDU. The OUI can be used to identify the vendor of the remote OAM device.
Peer Vendor Info (dot3OamPeerVendorInfo)	*Vendor information text*	The vendor information field is in the local information TLV, and can be used to determine additional information about the peer device.
Peer Mode (dot3OamPeerMode)	Active or Passive	See Mode (dot3OamMode)
Peer Max PDU Size (dot3OamPeerMaxOamPduSize)	*PDU size*	The largest OAMPDU value, in bytes, that is supported by the peer port. Minimum is 64 Maximum is 1518 Default is 1514
Peer Configuration Revision (dot3OamPeerConfigRevision)	0 to 65 535	The configuration revision of the OAM device as identified in the latest OAMPDU sent by the OAM peer. The configuration revision is used by OAM devices to indicate that configuration changes have occurred which might require the peer OAM device to re-evaluate whether OAM peering is allowed.
Peer Functions Supported (dot3OamPeerFunctSupported)	Event Support	The peer port can send and receive Event Notification OAMPDUs.
	Loopback Support	The peer port can initiate and respond to loopback commands.
	Unidirectional Support	The peer port supports the transmission of OAMPDUs on links that are operating in unidirectional mode.
	Variable Support	The peer port can send and receive Variable Request and Response OAMPDUs.

10 Close the 802.3ah form when you have completed the EFM OAM diagnostic.

Procedure 17-55 To configure an 802.3ah EFM OAM diagnostic on an OmniSwitch at the NE or port level

EFM OAM, which is described in 802.3ah, clause 57, defines the Ethernet OAM sublayer, which provides mechanisms for monitoring link operation, such as remote fault indication and remote loopback control.

The OAM information is transported in slow protocol frames, which are called OAMPDUs. OAMPDUs contain the appropriate control and status information that is used to monitor, test, and troubleshoot OAM-enabled links. OAMPDUs traverse a single link, that is passed between peer OAM entities.

802.3ah EFM OAM supports:

- EFM OAM capability discovery
- active and passive modes
- remote failure indication
- local and remote loopbacks
- high-resolution EFM OAM timers

The EFM OAM diagnostic is supported at the NE level or at the Ethernet port level on the Ethernet ports in network mode.

Caution 1 — Performing an 802.3ah diagnostic is service-affecting. Ensure that you consider the implications of performing this test before you proceed.

Caution 2 — Link OAM (802.3ah) is not supported on mirroring ports.

Caution 3 — When a port is in loopback mode, service mirroring does not work if the port is a mirror source or a mirror destination.

Note — In order for the 802.3ah diagnostic to be successful, the local and peer ports must support the 802.3ah protocol, and be operationally and administratively up.

To configure Link OAM at the NE level, go to Step 1.To configure Link OAM and 802.3ah EFM OAM diagnostics at the port level, go to Step 7

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on an OmniSwitch NE in the Equipment view and choose Properties from the contextual menu. The Network Element form opens with the General tab displayed.

3 Click on the Globals tab button.

4 Click on the 802.3ah tab button. The 802.3ah form opens.

5 Configure the parameters:

6 Configure the parameters:

- Administrative Status
- Multiple PDU Count
- Statistics
- Log-history

7 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

8 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

9 Click on the Ethernet tab button. The Ethernet port configuration form opens with the General tab displayed.

10 Click on the 802.3ah tab button. The 802.3ah form opens.

11 Configure the parameters:

- Administrative State
- Mode
- Transmit Interval (s)
- Received Remote Loopback Requests
- Set Remote Loopback
- Set Local Loopback
- Hold Time (s)
- Dying Gasp Notify
- Critical Event Notify
- Statistics
- Log-history
- Errored Frame Window (dsec)
- Errored Frame Period Window (frames)
- Errored Frame Seconds Summary Window (dsec)
- Threshold (frames)
- Period Threshold (frames)
- Seconds Summary Threshold (framesec)
- Notify
- Period Notify
- Seconds Summary Notify
- Number of Frames
- Frames Delay (ms)
- Start L1-Ping

12 Click on the Apply button. A dialog box appears.

13 Click on the Yes button.

14 The 802.3ah form is updated with the results of the 802.3ah diagnostic. The values that are displayed on the form depend on the configuration of the local and peer ports.

Tables 17-6, 17-7, and 17-8 describe the displayed information.

Table 17-6 802.3ah EFM OAM results

Parameter	Value	Description
Operational Status (dot3OamOperStatus)	Disabled	The Administrative State parameter on the local port is set to Disabled.
	Active Send Local	The Mode parameter is set to Active and the local port is discovering the peer port EFM OAM capabilities.
	Passive Wait	The Mode parameter is set to Passive and the local port is waiting to receive OAMPDUs from the peer device.
	Send Local and Remote	The local port discovered the peer but has not yet accepted or rejected the configuration of the peer. The local port may determine that the peer port is not compatible and decline OAM peering.
	OAM Peering Locally Rejected	The local port declined OAM peering.
	Send Local and Remote Ok	The local port accepted OAM peering.
	OAM Peering Remotely Rejected	The remote port declined OAM peering.
	Operational	The local and remote ports accepted the OAM peering.
	Non-operational Half Duplex	The Administrative State parameter is set to Enabled but the local port is in half-duplex mode.
	Link Fault	The link detected a fault and is transmitting OAMPDUs with a link fault indication.
Max. PDU Size (dot3OamMaxOamPduSize)	PDU size	The largest OAMPDU size, in bytes, that is supported by the local port: Minimum is 64 Maximum is 1518 Default is 1514
Configuration Revision (dot3OamConfigRevision)	0 to 65 535	The configuration revision of the OAM entity obtained from the latest OAMPDU sent by the OAM entity. The value is used by OAM entities to indicate that configuration changes occurred that may require the peer OAM entity to re-evaluate whether OAM peering is allowed.
Functions Supported (dot3OamFunctionsSupported)	Event Support	The port can send and receive event notification OAMPDUs.
	Loopback Support	The port can initiate and respond to loopback commands.
	Unidirectional Support	The port supports the transmission of OAMPDUs on links that operate in unidirectional mode.
	Variable Support	The port can send and receive variable request and response OAMPDUs.

(1 of 2)

Parameter	Value	Description
Loopback Status (dot3OamLoopbackStatus)	No Loopback	The port is not in a loopback condition.
	Initiating Loopback	The local device initiated a loopback, sent a loopback OAMPDU and is waiting for a response from the peer port.
	Remote Loopback	The peer port is in loopback mode.
	Terminating Loopback	The local port is in the process of terminating a loopback on the peer port.
	Local Loopback	The peer port has put the local port into loopback mode.
	Unknown	An OAMPDU that contains an unexpected message was received by the local port.

(2 of 2)

Table 17-7 802.3ah EFM OAM Statistics

Statistics	Displayed Value	Description
Frames Lost Due to OAM(dot3OamFramesLostDueTo Oam)	*Number of frames*	The number of frames that were dropped by the OAM multiplexer. Discontinuities of this counter can occur under some conditions.
Information Rx (dot3OamInformationRx)	*Number of OAMPDUs*	The number of information OAMPDUs received on this interface
Information Tx (dot3OamInformation Tx)	*Number of OAMPDUs*	The number of information OAMPDUs transmitted on this interface. Discontinuities of this counter can occur can occur under some conditions.
Loopback Control Rx (dot3OamLoopbackControlRx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs received on this interface
Loopback Control Tx (dot3OamLoopbackConrolTx)	*Number of OAMPDUs*	The number of loopback control OAMPDUs transmitted on this interface
Unsupported Codes Rx (dot3OamUnsupportedCodesRx)	*Number of OAMPDUs*	The number of OAMPDUs received on this interface with an unsupported opcode
Unsupported Codes Tx (dot3OamUnsupportedCodesTx)	*Number of OAMPDUs*	The number of OAMPDUs transmitted on this interface with an unsupported opcode

Table 17-8 802.3ah EFM OAM peer information

Peer Information	Displayed Value	Description
Peer MAC Address (dot3OamPeerMacAddress)	*MAC address*	The MAC address of the peer port. The MAC address is contained in the received OAMPDU.
Peer Vendor OUI (dot3OamPeerVendorOui)	*OUI*	The OUI of the OAM peer. The OUI is part of the peer MAC address contained in the received OAMPDU. The OUI can be used to identify the vendor of the remote OAM device.
Peer Vendor Info (dot3OamPeerVendorInfo)	*Vendor information text*	The vendor information field is in the local information TLV, and can be used to determine additional information about the peer device.
Peer Mode (dot3OamPeerMode)	Active or Passive	See Mode (dot3OamMode)
Peer Max PDU Size (dot3OamPeerMaxOamPduSize)	*PDU size*	The largest OAMPDU value, in bytes, that is supported by the peer port. Minimum is 64 Maximum is 1518 Default is 1514
Peer Configuration Revision (dot3OamPeerConfigRevision)	0 to 65 535	The configuration revision of the OAM device as identified in the latest OAMPDU sent by the OAM peer. The configuration revision is used by OAM devices to indicate that configuration changes have occurred which might require the peer OAM device to re-evaluate whether OAM peering is allowed.
Peer Functions Supported (dot3OamPeerFunctSupported)	Event Support	The peer port can send and receive Event Notification OAMPDUs.
	Loopback Support	The peer port can initiate and respond to loopback commands.
	Unidirectional Support	The peer port supports the transmission of OAMPDUs on links that are operating in unidirectional mode.
	Variable Support	The peer port can send and receive Variable Request and Response OAMPDUs.

15 Close the 802.3ah form when you have completed the EFM OAM diagnostic.

Procedure 17-56 To configure Dying Gasp on an OmniSwitch 6250 (Metro) NE

Note — In order to see the Dying Gasp alarm in the 5620 SAM, the NE must be managed using SNMP V2, with a "public" community string, since this alarm has a pre-defined community string of "public".

1 Use the 5620 SAM navigation tree; perform the following steps.

2 Choose Equipment from the view selector.

3 Right-click on an OS 6250 (Metro) icon.

4 Choose NE Sessions→*option* from the contextual menu

where *option* is Telnet Session or SSH Session

5 Choose Telnet Session.

6 The Telnet Session window opens.

7 See Step 5 of Procedure 12-3 to configure the NE to be managed with a "public" community string using SNMP v2.

Note 1 — If the Backup/Primary power supply fails, a major alarm will be raised. This alarm will be sent only to the first two SNMP stations configured on the NE. “Show snmp station” lists the management station address. SAM ip should be first or second.

Note 2 — The "Loopback 0" address should not be used for the source IP address field on the NE.

Procedure 17-57 To configure an advanced loopback test on an OmniSwitch port

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

Note 1 — Only one test profile per port can be created, up to a maximum of 8 ports on an NE.

Note 2 — The test profile cannot be created on a port that is part of a LAG.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

3 Click on the Advanced Loopback tab button. Click on the Add button. The AOS Advanced Loopback (Create) form appears.

4 Configure the parameters:

- Test Name
- Source MAC Address
- Destination MAC Address
- VLAN
- Traffic Type
- SAP Id (OS 6250 only, see Note 1 and Note 2)

Note 1 — For OS 6250 NEs, if the Traffic Type parameter value is "Outward", the user will be provided with an option to specify the SAP Id, provided the SAP Id already exists on the NE.

Note 2 — If a loopback profile is created with a Traffic Type value of "Outward", the SAP Id option will be provided with the default value of "0". If the loopback profile is created with SAP Id, then the SAP Id must exist on the NE.

5 Click on the OK button. A dialog box appears.

6 Click on the OK button. The AOS Advanced Loopback (Create) form closes.

7 Choose a test entry on the Physical Port (Edit) form. Click on the Apply button.

8 A dialog box appears. Click on the Yes button.

9 Choose a test entry on the Physical Port (Edit) form. Click on the Properties button.

10 The AOS Advanced Loopback (Edit) form opens. Configure the Status parameter.

11 Click on the OK button. The AOS Advanced Loopback (Edit) form closes.

12 Click on the OK button of the Physical Port (Edit) form. A dialog box appears.

13 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 17-58 To configure port/queue statistics on an OS 6250 port

This procedure provides port/queue statistics on an OS 6250 (Metro) or OS 6250 (SME) NE.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with General tab displayed.

3 Click on the Statistics tab button.

4 In the Select Object Type area, choose Qos Port/Queue Stats (Physical Equipment) from the contextual menu.

5 Click on the Collect button.

6 A statistics record appears on the Physical Port (Edit) form. Select the record.

7 Click on the Properties button. The Statistics Record - QoS Port/Queue Stats form opens.

8 View the read-only port/queue statistics parameter values for the OS 6250 port.

9 Click on the Close button. The Statistics Record - QoS Port/Queue Stats form closes.

10 Close the Physical Port (Edit) form.

Procedure 17-59 To configure Ip statistics on an OmniSwitch routing instance

This procedure provides Ip traffic statistics (received or transmitted) on a routing instance of an OmniSwitch.

1 Choose Routing from the view selector in the navigation tree. The navigation tree displays the Routing view.

2 Right-click on a Routing Instance in the Routing view and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with General tab displayed.

3 Click on the Statistics tab button.

4 In the Select Object Type area, choose Ip Traffic Stats (Received) (Routing Management General) or Ip Traffic Stats (Transmitted) (Routing Management General) from the contextual menu.

5 Click on the Collect button.

6 A statistics record appears on the Routing Instance (Edit) form. Select the record.

7 Click on the Properties button. The Statistics Record - IP Stats (Received) or Statistics Record - IP Stats (Transmitted) form opens, depending on which object is selected in Step 4.

8 View the read-only IP statistics parameter values for the OmniSwitch routing instance.

9 Click on the Close button. The Statistics Record - IP Stats (Received) or Statistics Record - IP Stats (Transmitted) form closes.

10 Close the Routing Instance (Edit) form.

Procedure 17-60 To configure an HSMDA override

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on an HSMDA in the Equipment view and choose Properties from the contextual menu. The Daughter Card Slot (Edit) form opens with the General tab displayed.

Note 1 — You can also access the HSMDA override for the port from the port properties configuration form.

Note 2 — The HSMDA override at the MDA level applies to the HSMDA ingress. The HSMDA override at the port level applies to the HSMDA port egress.

3 Click on the Override tab button. The Override configuration form opens with the HSMDA Scheduler tab displayed.

4 Click on the Add button. The HSMDA Scheduler Policy Override form opens with the General tab displayed.

5 Click on the Override tab button.

6 Configure the parameters:

- Maximum Rate (Mbps)
- Rate (Mbps)
- Weight

The Rate (Mbps) parameter is configurable when a group is not specified for the applied HSMDA scheduler policy. The Weight parameter is configurable when group 1 or group 2 is specified for the HSMDA scheduler policy.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Override configuration form is updated with the scheduler override.

9 Close the Daughter Card Slot (Edit) form.

Procedure 17-61 To configure Ethernet ports

Perform this procedure, as required, depending on the daughter card and port type that you are configuring. Different card types display different port configuration parameters.

Note — Before you can configure 802.1X on an Ethernet access port, 802.1X must be enabled on the device and an 802.1X policy must be created and distributed to the device.

See Procedure 17-13 for information about enabling 802.1X on a device. See chapter 52 for information about creating and distributing 802.1X policies.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Configured MAC

  Only one MAC address can be assigned to a port. When a new MAC address is configured while the port is operational, IP issues an ARP, if appropriate, and BPDUs are sent with the new MAC address. A default MAC address is assigned by the system.
- Mode
- L2Uplink
- Encap Type
- Speed
- MTU (bytes)
- DDM Event Suppression
- Hold Time Up (seconds)
- Hold Time Down (seconds)
- Load Balance Algorithm
- Ingress Percentage of Rate (%)
- Egress Percentage of Rate (%)
- Default VLAN
- Channel
- Rx Decision Threshold Voltage Adjustment
- Optical Transport Channel Unit
- OLC State

If the port is a LAG member, the Hold Time Up (seconds) parameter is configurable only if the port is the primary member. The Hold Time Down (seconds) parameter is not configurable when the port is a LAG member.

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

4 If you set the Mode parameter to Hybrid, configure the following parameters in the Hybrid Ingress Buffer Allocation panel. Otherwise, go to step 7:

- Access Weight
- Network Weight

5 If you set the Mode parameter to Hybrid, configure the following parameters in the Hybrid Egress Buffer Allocation panel:

- Access Weight
- Network Weight

6 If you change the Mode parameter from Access to Hybrid and there are SAPs on the port, perform Procedure 15-2 to migrate the SAPs.

7 If you are configuring a 7210 SAS Ethernet port you can add the port to a split horizon group. See Procedure 17-6 for information about creating a 7210 SAS split horizon group.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - Physical Port list form opens.

ii Choose a split horizon group and click on the OK button. The Select Split Horizon Group - Physical Port list form closes, and the Physical Port (Edit) form refreshes with the split horizon group name.

Note 1 — A port cannot be added to or deleted from a split horizon group if it has a SAP configured on it or is a member of a LAG.

Note 2 — A port cannot belong to more than one split horizon group; you must remove any split horizon groups from the port before you can add the port to a different split horizon group.

8 Configure the Named Pool Buffer Policy for the port.

i Click on the Select button beside the Name parameter in the Ingress Pool Policy panel. A Select Ingress Pool Policy window opens with a list of ingress pool policies.

ii Choose a policy from the list.

iii Click on the OK button, the Select Ingress Pool Policy window closes and the Name parameter refreshes with the selected policy.

iv Configure the Ingress Percentage of Rate (%) parameter.

v Click on the Select button beside the Name parameter in the Egress Pool Policy panel. A Select Egress Pool Policy window opens with a list of egress pool policies.

vi Choose a policy from the list.

vii Click on the OK button, the Select Egress Pool Policy window closes and the Name parameter refreshes with the selected policy.

viii Configure the Egress Percentage of Rate parameter.

Note — Ensure that the named pool mode is enabled. See Procedure 17-46 for more information.

9 Click on the States tab button.

10 Configure the Administrative State parameter.

11 Click on the Policies tab button. The Policies form opens with the General tab displayed.

12 Click on the Select button in the Accounting Policy panel to assign an accounting policy to the port. The Select Accounting Policy - Physical Port form opens.

The type of policy that you can choose depends on the type of NE, type of port, and the parameter settings.

13 Choose an accounting policy from the list and click on the OK button. The Select Accounting Policy - Physical Port form closes.

14 Configure the Collect Accounting Statistics parameter.

15 If you are configuring a 7210 SAS Ethernet port, go to step 23, otherwise go to step 16.

16 Click on the Select button in the Network Queue panel to assign a network queue policy to the port. The Select Network Queue Policy - Physical Port form opens.

17 Choose a network queue policy from the list and click on the OK button. The Select Network Queue Policy - Physical Port form closes.

18 Click on the Select button in the Port Scheduler Policy panel to assign a port scheduler policy to the port. The Select Port Scheduler Policy - Physical Port form opens.

19 Choose a port scheduler policy from the list and click on the OK button. The Select Port Scheduler Policy - Physical Port form closes.

20 Click on the Select button in the HSMDA Scheduler Policy panel to assign a scheduler policy to the port. The Select HSMDA Scheduler Policy - Physical Port form opens.

21 Choose a policy from the list and click on the OK button. The Select HSMDA Scheduler Policy - Physical Port form closes.

22 Go to step 26.

23 Perform one of the following to assign policies to a 7210 SAS Ethernet port.

a If the port is in access mode, go to step 24.

b If the port is in network mode or is an L2Uplink port, go to step 25.

24 You can assign port scheduler and access egress policies, and enable queues for statistics collection when the 7210 SAS port mode is access.

i Click on the 7210 Specific tab button.

ii Click on the Clear button in the PortScheduler Policy panel to remove the selected policy.

iii Click on the Select button in the PortScheduler Policy panel to assign a port scheduler policy to the port. The Select PortScheduler Policy - Sas Port form opens.

iv Choose a policy from the list and click on the OK button. The Select PortScheduler Policy - Sas Port form closes.

v Click on the Clear button in the Access Egress Policy panel to remove the selected policy.

vi Click on the Select button in the Access Egress Policy panel to assign an access egress policy to the port. The Select Access Egress Policy - Sas Port form opens.

vii Choose a policy from the list and click on the OK button. The Select Access Egress Policy - Sas Port form closes.

viii If you are configuring the collection of egress packet forwarding statistics, click on the 7210 Statistics tab button. Otherwise, go to step 26.

ix Configure the Queue 1 through Queue 8 parameters, as required.

Note — Enabling these queues is only applicable to the 7210 SAS-E. While any queue of any port can be enabled, only eight counters in total can be enabled for each 7210 SAS-E device.

x Go to step 26.

25 You can assign accounting, port scheduler, network, and network queue policies when the 7210 SAS port mode is network or when it is an L2Uplink port.

i Click on the 7210 Specific tab button.

ii Click on the Clear button in the PortScheduler Policy panel to remove the selected policy.

iii Click on the Select button in the PortScheduler Policy panel to assign a port scheduler policy to the port. The Select PortScheduler Policy - Sas Port form opens.

iv Choose a policy from the list and click on the OK button. The Select PortScheduler Policy - Sas Port form closes.

v Click on the Clear button in the Network Policy panel to remove the selected policy.

vi Click on the Select button in the Network Policy panel to assign a network policy to the port. The Select Network Policy - Sas Port form opens.

vii Choose a policy from the list and click on the OK button. The Select Network Policy - Sas Port form closes.

viii Click on the Clear button in the Network Queue panel to remove the selected policy.

ix Click on the Select button in the Network Queue panel to assign a network queue policy to the port. The Select Network Queue Policy - Physical Port form opens.

x Choose a policy from the list and click on the OK button. The Select Network Queue Policy - Physical Port form closes.

26 Click on the Ethernet tab button. The Ethernet port configuration form opens with the General tab displayed.

27 Configure the parameters:

- Auto-negotiate
- Duplex
- Dot1 Q Ethertype
- Q in Q Ethertype
- Ingress Rate (Mbps)
- Egress Scheduler Mode
- Egress Rate (Kbps)
- Egress Max-Burst
- Flow
- Down When Looped
- Retry Timeout (Sec)
- Xgig Mode
- Forward All Multicast Traffic
- Forbid IGMP Snooping
- Backpressure
- Broadcast Limit (Pkts/s)
- Detect Remote Faults
- Detection
- Keep Alive Interval (Sec)
- Single Fiber
- Type
- Time (seconds)
- Synchronous status messages
- SSM Code-Type
- Tx DUS/DNU

The Dot1 Q Ethertype and Q in Q Ethertype parameters are not configurable for the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco devices. The Xgig Mode parameter is only configured for 1 x 10-Gig Ethernet interfaces, and is used to treat the port as a WAN-PHY interface, which encapsulates Ethernet frames over SONET.

The Flow parameter is configurable on Telco devices when the Auto-negotiate parameter is set to False.

The Backpressure, Broadcast Limit (Pkts/s), Detect Remote Faults, Detection, Forward All Multicast Traffic, and Forbid IGMP Snooping parameters are only configurable on the 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA.

The Keep Alive Interval (Sec) and Retry Timeout (Sec) parameters are only displayed when the Down When Looped parameter is enabled.

The Single Fiber parameter is configurable for 1 and 10 Gigabit Ethernet network ports on the 7750 SR and 7450 ESS, and is supported only on the 2 x XP MDA IOM 3 and IMM.

The Type and Time (seconds) parameters in the Timed Loopback panel are configurable only on Ethernet ports on the 7705 SAR, Release 2.1 or later.

Note — Management connectivity between the 5620 SAM and the 7705 SAR may be lost if a line loopback is applied to an Ethernet port that is carrying in-band management traffic. The line loopback remains in effect until the timer expires and the 7705 SAR removes the loopback.

28 Perform one of the following:

a Click on the 802.3ah tab button to configure and initiate the 802.3ah EFM OAM diagnostic. See Procedure 17-54 for more information.

b Go to step 35.

29 Perform one of the following:

a If the port is a network port, the Network Egress Queue Group tab button is present. Click on the Network Egress Queue Group tab button to add a queue group to the port, if required, and perform the following steps.

Note — The Network Egress Queue Group tab button is available if queue groups are supported on the port, depending on the NE release and IOM type. See section "Port queue groups" in chapter 61 for more information about supported devices and IOM types.

i Click on the Add button. The Network Egress Queue Group (Create) form opens with the General tab displayed.

ii Click on the Select button in the Queue Group Template Policy panel. The Select Queue Group Template Policy - Network Egress Queue Group list form opens.

iii Choose an egress queue group template policy from the list and click on the OK button. The Select Queue Group Template Policy - Network Egress Queue Group list form closes.

iv Configure the Description parameter.

v Click on the Select button beside the ID parameter in the Accounting Policy panel. The Select Accounting Policy - Network Egress Queue Group list form opens.

Note — Only the accounting policies with the Type parameter configured to one of the following options are listed:

- Queue Group Octets
- Queue Group Packets
- Combined Queue Group

vi Choose an accounting policy from the list and click on the Ok button. The Select Accounting Policy - Network Egress Queue Group list form closes and the Network Egress Queue Group (Create) form refreshes with the accounting policy information.

vii Configure the Collect Accounting Statistics parameter.

viii Click on the Select button in the Scheduler Policy panel to assign a scheduler policy to the port. The Select Scheduler Policy - Network Egress Queue Group list form opens.

ix Choose a scheduler policy from the list and click on the OK button. The Select Scheduler Policy - Network Egress Queue Group list form closes.

x Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only if you did not select a scheduler policy in step ix. The Frame-Based Accounting parameter is configurable only if you configure the Aggregate Rate Limit (kbps) parameter.

xi Click on the Overrides: Network Egress Queue tab button.

xii Click on the Add button. The Network Egress Queue Override (Create) form opens.

xiii Click on the Select button beside the ID parameter to select an egress queue. The Select Egress Queue - Network Egress Queue Override list form opens.

xiv Choose an entry from the list and click on the OK button. The Select Egress Queue - Network Egress Queue Override list form closes and the Network Egress Queue Override (Create) form refreshes with the queue information.

xv Click on the Override tab button.

xvi Configure the parameters:

- Committed Burst Size (KB)
- Maximum Burst Size (KB)
- High Priority Reserved
- PIR Adaptation
- CIR Adaptation
- PIR (kbps)
- CIR (kbps)

The parameters are configurable when the Override check box is enabled.

xvii Click on the OK button to save the configuration and close the Network Egress Queue Override (Create) form.

xviii A dialog box appears. Click on the OK button.

xix Click on the OK button to save the configuration and close the Network Egress Queue Group (Create) form.

xx A dialog box appears. Click on the OK button.

b If the port is an access port, the Access Ingress Queue Group button is present. Click on the Access Ingress Queue Group tab button to add an access ingress queue group to the port, if required, and perform the following steps.

i Click on the Add button. The Access Ingress Queue Group (Create) form opens with the General tab displayed.

ii Click on the Select button in the Queue Group Template Policy panel. The Select Queue Group Template Policy - Access Ingress Queue Group list form opens.

iii Choose a queue group template policy from the list and click on the OK button. The Select Queue Group Template Policy - Access Ingress Queue Group list form closes.

iv Configure the Description parameter.

v Click on the Select button beside the ID parameter in the Accounting Policy panel. The Select Accounting Policy - Access Ingress Queue Group list form opens.

vi Choose an accounting policy from the list and click on the Ok button. The Select Accounting Policy - Access Ingress Queue Group list form closes and the Access Ingress Queue Group (Create) form refreshes with the accounting policy information.

Note — Only the accounting policies with the Type parameter configured to one of the following options are listed:

- Queue Group Octets
- Queue Group Packets
- Combined Queue Group

vii Configure the Collect Accounting Statistics parameter.

viii Click on the Select button in the Scheduler Policy panel to assign a scheduler policy to the port. The Select Scheduler Policy - Access Ingress Queue Group list form opens.

ix Choose a scheduler policy from the list and click on the OK button. The Select Scheduler Policy - Access Ingress Queue Group list form closes.

x Click on the Overrides: Access Ingress Queue tab button.

xi Click on the Add button. The Access Ingress Queue Override (Create) form opens.

xii Click on the Select button beside the ID parameter to select an egress queue. The Select Ingress Queue - Access Ingress Queue Override list form opens.

xiii Choose an entry from the list and click on the OK button. The Select Ingress Queue - Access Ingress Queue Override list form closes and the Access Ingress Queue Override (Create) form refreshes with the queue information.

xiv Click on the Override tab button.

xv Configure the parameters:

- Committed Burst Size (KB)
- Maximum Burst Size (KB)
- High Priority Reserved
- PIR Adaptation
- CIR Adaptation
- PIR (kbps)
- CIR (kbps)

The parameters are configurable when the Override check box is enabled.

xvi Click on the OK button to save the configuration and close the Access Ingress Queue Override (Create) form.

xvii A dialog box appears. Click on the OK button.

xviii Click on the OK button to save the configuration and close the Access Ingress Queue Groups (Create) form.

xix A dialog box appears. Click on the OK button.

c If the port is an access port, the Access Egress Queue Group button is present. Click on the Access Egress Queue Group tab button to add an access egress queue group to the port, if required, and perform the following steps.

i Click on the Add button. The Access Egress Queue Group (Create) form opens with the General tab displayed.

ii Click on the Select button in the Queue Group Template Policy panel. The Select Queue Group Template Policy - Access Egress Queue Group list form opens.

iii Choose an egress queue group template policy from the list and click on the OK button. The Select Queue Group Template Policy - Access Egress Queue Group list form closes.

iv Configure the Description parameter.

v Click on the Select button beside the ID parameter in the Accounting Policy panel. The Select Accounting Policy - Access Egress Queue Group list form opens.

vi Choose an accounting policy from the list and click on the Ok button. The Select Accounting Policy - Access Egress Queue Group list form closes and the Access Egress Queue Group (Create) form refreshes with the accounting policy information.

Note — Only the accounting policies with the Type parameter configured to one of the following options are listed:

- Queue Group Octets
- Queue Group Packets
- Combined Queue Group

vii Configure the Collect Accounting Statistics parameter.

viii Click on the Select button in the Scheduler Policy panel to assign a scheduler policy to the port. The Select Scheduler Policy - Access Egress Queue Group list form opens.

ix Choose a scheduler policy from the list and click on the OK button. The Select Scheduler Policy - Access Egress Queue Group list form closes.

x Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

The Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only if you did not select a scheduler policy in step ix. The Frame-Based Accounting parameter is configurable only if you configure the Aggregate Rate Limit (kbps) parameter.

xi Click on the Host Matching tab button.

xii Click on the Add button. The Host String (Create) form opens.

xiii Configure the Host String parameter.

xiv Click OK. The Host String (Create) form closes and the information on the Host Matching tab is updated.

xv Click on the Overrides: Access Egress Queue tab button.

xvi Click on the Add button. The Access Egress Queue Override (Create) form opens.

xvii Click on the Select button beside the ID parameter to select an egress queue. The Select Egress Queue - Access Egress Queue Override list form opens.

xviii Choose an entry from the list and click on the OK button. The Select Egress Queue - Access Egress Queue Override list form closes and the Access Egress Queue Override (Create) form refreshes with the queue information.

xix Click on the Override tab button.

xx Configure the parameters:

- Committed Burst Size (KB)
- Maximum Burst Size (KB)
- High Priority Reserved
- PIR Adaptation
- CIR Adaptation
- PIR (kbps)
- CIR (kbps)

The parameters are configurable when the Override check box is enabled.

xxi Click on the OK button to save the configuration and close the Access Egress Queue Override (Create) form.

xxii A dialog box appears. Click on the OK button.

xxiii Click on the OK button to save the configuration and close the Access Egress Queue Groups (Create) form.

xxiv A dialog box appears. Click on the OK button.

xxv Repeat to create additional egress queue groups.

30 The Egress Secondary Shapers tab button is present if the port is on an HSMDA. Click on the Egress Secondary Shapers tab button, if required.

i Click on the Add button. The HSMDA Egress Secondary Shaper (Create) form opens.

ii Configure the parameters:

- Name
- Rate (kbps)

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new entry appears in the list.

31 Click on the LLDP tab button, if required. The LLDP configuration form opens with the Nearest Bridge sub-tab displayed.

32 Configure the parameters:

- Administrative Status
- Notifications
- Transmit Management Address
- LLDP TLVs

33 Repeat step 32 for the Nearest Non TPMR and Nearest Customer sub-tabs under the LLDP tab, as required.

34 Click on the Remote Peers sub-tab under the LLDP tab to search for and display LLDP remote peers associated with the port. These remote peers are used to determine the physical topology of the network.

35 Click on the 802.1x Port tab button, if required. You cannot configure the parameters for the 7710 SR.

36 Configure the parameters:

- Initialize
- Reauthenticate Control

37 Click on the 802.1x Port Authenticator tab button, if required. You cannot configure the parameters for the 7710 SR.

38 Configure the parameters:

- Controlled Port Control
- Quiet Period
- Tx Period
- Supplicant Timeout
- Server Timeout
- Max Req
- Reauth Period
- Reauth Enabled

39 Click on the Select button to choose a RADIUS policy. The Select Policy - Physical Port form opens.

40 Choose a RADIUS policy in the list and click on the OK button. The Select Policy - Physical Port form closes and the Physical Port (Edit) form displays the RADIUS policy name.

41 The Access Group tab is present if the port is on a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device. Click on the Access Group tab, if required. Otherwise, go to step 51.

42 Click on the Add button to create an access group, or select an existing access group in the list and click on the Properties button. The Port Access Group (Create) form opens.

43 Configure the parameters:

- Displayed Name
- Description
- Type

44 Click on the OK button. A dialog box appears.

45 Click on the OK button. The new access group appears in the list.

46 The QoS tab is present if the port is on a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device. Click on the QoS tab button, if required. Otherwise, go to step 52.

47 Click on the Add button to configure QoS settings for the port. The QoSPort (Create) form opens.

48 Configure the parameters:

- Displayed Name
- Description
- Priority
- Queue Algorithm
- Drop Algorithm
- Shaper Rate

49 Click on the OK button. A dialog box appears.

50 Click on the OK button. The new QoS entry appears in the list.

51 Perform one of the following:

a Click on the Override tab button to configure HSMDA overrides. See Procedure 17-54 for more information.

b Otherwise, go to step 52.

52 To configure a 1x10-Gig Ethernet DWDM tunable optics MDA or a 1-Port OC768 OTU3 Long Reach DWDM Tunable IMM on a 7750 SR or 7450 ESS, click on the Optical Transport Channel Unit tab button. Otherwise, go to step 62.

53 Configure the following parameters on the General tab:

- FEC Mode
- SF-SD Method
- SF Threshold
- SD Threshold
- Configured Data Rate (Gb/s)
- Transmitter Mode
- Transmitter String
- Async Mapping
- Transmitter Bytes
- Expected Rx Mode
- Expected Rx String
- Expected Rx Bytes
- OTU-TIM reaction
- ODU-TIM reaction
- OPU-TIM reaction
- Payload Type (hex)
- Expected Payload Type (hex)
- OPU-PLM reaction

54 Click on the OTU Alarms tab button and select the OTU alarms for the Configured Alarms parameter.

55 Click on the Wavelength Table tab button to display the configurable channels and related wavelengths and frequencies.

56 Click on the Optical tab button and configure the following parameters on the Wavelength Track tab:

- Wave Tracker Encode
- Wave Tracker Power Control
- Configured Alarms
- Wave Key1
- Wave Key2
- Target Power

57 Click on the Optical Amplifier tab button and configure the Configured Alarms parameter.

58 Click on the Optical Tunable Dispersion Compensation Module tab button.

59 Configure the following parameters:

- Channel
- Dispersion
- Control Mode
- Configured Alarms

60 Click on the Apply button. A dialog box appears.

61 Click on the Yes button.

62 Click on the other tab buttons to view and edit additional port information.

63 Click on the Cancel if no changes were made, otherwise click on the OK button. The Physical Port (Edit) form closes.

Procedure 17-62 To configure OmniSwitch Ethernet ports

Perform the steps in this procedure as required depending on the OmniSwitch chassis type and port type that you are configuring. Different chassis types display different port configuration parameters.

Note — You can configure MVRP fixed ports, 802.1 Q ports, aggregate ports, and VLAN Stacking Network ports.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Mode

  An access port is used for customer-facing traffic on which VLAN services are configured.

  A network port or channel is configured for network access in the service provider transport or infrastructure network. Typically, only one OmniSwitch network port is required for tree topology, and two ports are required for ring topology.
- Speed
- MTU (bytes)
- Automatic VLAN Binding
- OLC State

4 Click on the States tab button.

5 Configure the Administrative State parameter.

6 Click on the Policies tab button.

Note — A port must have a service access point associated with it before you can apply a UNI policy to the port.

7 Click on the Select button in the UNI Profile panel to assign a UNI policy to the port. The Select UNI Profile - Physical Port form opens.

8 Choose a User Network Interface (UNI) profile policy from the list and click on the OK button. The Select UNI Policy - Physical Port form closes.

9 Click on the Ethernet tab button. The Ethernet port configuration form opens with the General tab displayed.

10 Configure the parameters:

- Duplex
- Auto-negotiate
- Enable Port Mobility
- Dot1 Q Acceptable Frames
- Broadcast Limit (kbps)
- Enable Multicast Limit Mode
- Inter-Frame Gap (bytes)
- Detection
- Default VLAN Restore
- Default VLAN Enable
- Ignore BPDU
- Authenticate
- Ingress Filtering

The Inter-Frame Gap parameter is only configurable on Gigabit Ethernet ports.

The Default VLAN Restore, Default VLAN Enable, Ignore BPDU, Authenticate, and Ingress Filtering parameters are only configurable when the Enable Port Mobility parameter is set to Enable.

11 Click on the LLDP tab button, if required. The LLDP configuration form opens with the Nearest Bridge tab displayed.

12 Configure the parameters:

- Administrative Status
- Notifications
- Transmit Management Address
- LLDP TLVs

13 Click on the Remote Peers sub-tab under the LLDP tab to search for and display LLDP remote peers associated with the port. These remote peers are used to determine the physical topology of the network.

14 Click on the MVRP tab button to configure MVRP, if required.

15 Configure the parameters on the General tab:

- Status
- Registration Mode
- Applicant Mode
- Periodic Transmission Status
- Join Timer
- Leave Timer
- Leave All Timer
- Periodic Timer

16 Click on the VLAN Restrictions tab to configure VLAN restrictions, if required:

i Click on the Add button. The MVRP VLAN Registration form appears.

ii Configure the parameters:

- VLAN
- Restrict-Static-VLAN-Registration
- Restrict-Registration
- Restrict-Advertisement

iii Click on OK to close the MVRP VLAN Registration form. The list on the VLAN Restrictions tab is updated with the new MVRP VLAN Registration entry.

17 Click on the QoS tab button, if required. The QoS configuration form opens with the General tab displayed.

18 Configure the parameters:

- QoS Status
- Trusted
- Default 802.1p
- Default DSCP
- Max Egress BW (kbps)
- Max Ingress BW (kbps)
- Servicing Mode
- Default Classification

19 Click on the Queue tab button.

20 If you chose WRR or DRR for the Servicing Mode parameter, configure the Q0 to Q7 parameters in the Weight panel.

21 Configure the Q0 to Q7 parameters in the Minimum Bandwidth (Kbps) panel.

22 Configure the Q0 to Q7 parameters in the Maximum Bandwidth (Kbps) panel.

23 Click on the DHCP Snooping tab button, if applicable. This tab is only available if the port is associated with a VLAN that has DHCP snooping enabled or if DHCP snooping is enabled at the switch level.

24 Configure the parameters:

- Trust Mode
- IP Source Filtering

25 Click on the Ethernet Hybrid tab button, if applicable. This tab is only available for hybrid Ethernet ports.

26 Configure the parameters:

- Mode
- Speed
- Duplex
- Auto-negotiate
- Detection

27 Click on the PoE tab button, if applicable. This tab is only available for PoE ports.

28 Configure the parameters:

- Power State
- Maximum Power (milliwatt)
- Power Priority

29 Click on the LPS Learned MAC Entries tab button to view the MAC addresses learned on the port. LPS must be enabled on the port. See Procedure 28-51 for information about configuring LPS on an Ethernet port.

30 Click on the Add button to add static MAC address entries, if required. The MAC Entries (Create) form opens.

Note — A port must be LPS-enabled and belong to a VLAN before you can add static MAC addresses to the port.

31 Click on the Select button. The Select VLAN Site - MAC Entries form opens.

32 Configure the filter criteria. A list of VLANs appears at the bottom of the Select VLAN Site - MAC Entries form.

33 Choose a VLAN from the list.

34 Click on the OK button. The Select VLAN Site - MAC Entries form closes.

35 Configure the MAC Address parameter.

36 Click on the Apply button to save the changes.

37 Repeat steps 30 to 36 to add another MAC address, if required.

38 Click on the OK button. A dialog box appears.

39 Click on the Yes button. The Select VLAN Site - MAC Entries form closes.

40 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 17-63 To configure 9500 MPR Ethernet ports

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

3 If you are provisioning port 5 under the core-enhanced card or any of ports 5-8 on the 4+4 x Ethernet (EAS) card, or any of ports 1-4 of the 2+2 x Ethernet (EAS) card, configure the Port Usage parameter.

4 Configure the OLC State parameter.

5 Click on the States tab button.

6 Configure the Administrative State parameter.

7 Click on the Ethernet tab button. The Ethernet port configuration form opens with the General tab displayed.

8 Configure the parameters:

- Auto-negotiate
- Advertised Capability

Note — Check what combination is supported for Advertised Capability in the *9500 MPR User Guide*.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 17-64 To configure power source type on 2+2 x Ethernet (EAS) card slots for 9500 MPR (ETSI 2.1)

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 2+2 x Ethernet (EAS) card slot object in the Equipment view and choose Properties from the contextual menu. The Card Slot (Edit) form opens with the General tab displayed.

3 Click on the Power Source tab button.

4 Select a displayed interface or click on the Search button if no interface is displayed, then select a displayed interface. The Power Source (edit) form opens.

5 In the Power Source panel, configure the Type parameter.

6 Click the OK button. The Power Source (Edit) form closes.

7 The Card Slot (Edit) form reappears. Click on the OK button. A dialog box appears. Click on the Yes button. The Card Slot (Edit) form closes.

Procedure 17-65 To configure Telco and 7250 SAS uplink ports as network ports

When you add a 7250 SAS or Telco device to a ring group, the device ports can be used as VLAN service access points or as network uplink ports that receive ring group traffic from a device such as a 7450 ESS.

By default, the Mode parameter for 7250 SAS or Telco devices is set to Access. You can configure the required ports to act as uplink ports by setting the parameter to Network.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Set the Mode parameter to Network.

  An access port is used for customer-facing traffic on which services are configured. The Encap Type parameter for an access port must be set to Dot1 Q.

  A network port participates in the service provider transport or infrastructure network. For 7250 SAS and Telco devices, the network port acts as the uplink for the ring to the transport network. The Encap Type parameter for an uplink port must be set to Dot1 Q.
- Speed
- OLC State

4 Click on the States tab button.

5 Configure the Administrative State parameter.

6 Configure the other Ethernet port parameters, as described in Procedure 17-61.

Procedure 17-66 To configure 9500 MPR E1 and DS1 ports

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

3 Configure the OLC State parameter.

4 Click on the States tab button.

5 Configure the Administrative State parameter.

6 Click on the DS1/E1 tab button.

7 Configure the parameters:

- Signal Mode
- Line Code
- Line Length

If you are configuring an E1 port you can only configure the Signal Mode parameter.

8 Click on the other tab buttons in the properties form to view additional port information.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 17-67 To configure 9500 MPR DS3 ports

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

3 Configure the OLC State parameter.

4 Click on the States tab button.

5 Configure the Administrative State parameter.

6 Click on the DS3/E3 tab button.

7 Configure the parameters:

- Signal Mode
- Line Length
- AIS Signal Type

8 Click on the other tab buttons in the properties form to view additional port information.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 17-68 To configure 9500 MPR radio modem ports

The 5620 SAM supports limited configuration of the radio modem ports.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with General tab displayed.

3 Configure the OLC State parameter.

4 Click on the Radio tab button to view radio modem port parameters.

5 Click on the other tab buttons in the properties form to view additional port information such as physical links and statistics.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 17-69 To configure analog performance management on 9500 MPR radio modem ports

This procedure provides the analog radio statistics for 9500 MPR radio modem ports.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with General tab displayed.

3 Click on the Statistics tab button.

4 In the Select Object Type area, choose Radio Analog Statistics (Radio Equipment) from the contextual menu.

5 Click on the Collect button.

6 A statistics record appears on the Physical Port (Edit) form. Select the record.

7 Click on the Properties button. The Statistics Record - Radio Analog Statistics form opens.

8 View the read-only analog performance parameter values for the radio modem port.

9 Click on the Close button. The Statistics Record - Radio Analog Statistics form closes.

10 Close the Physical Port (Edit) form.

Procedure 17-70 To configure 9500 MPR port segregation

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 9500 MPR shelf object in the Equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the Port Segregation tab button.

4 Click on the Add button.

5 The Port Segregation (Create) form opens.

6 Click on the Select button beside the From Port field. The Select From Port - Port Segregation form opens.

7 Select a port from the list.

8 Click on the OK button. The Select From Port - Port Segregation form closes. The Port Segregation (Create) form re-opens.

9 Click on the Select button beside the To Port field. The Select To Port - Port Segregation form opens.

10 Select a port from the list.

11 Click on the OK button. The Select To Port - Port Segregation form closes. The Port Segregation (Create) form re-opens.

To add more port combinations, go to Step 12, otherwise go to Step 19.

12 Click on the Apply button. A dialog box opens. Click on OK.

13 Click on the Clear button beside the From Port field. The Select From Port - Port Segregation form opens.

14 Select a port from the list.

15 Click on the OK button. The Port Segregation (Create) form re-opens.

16 Click on the Clear button beside the To Port field. The Select To Port - Port Segregation form opens.

17 Select a port from the list.

18 Click on the OK button. The Port Segregation (Create) form re-opens.

To add another port combination, repeat Steps 12 to 18, otherwise go to Step 19.

19 Click on the OK button. A dialog box opens.

20 Click on the OK button. The Port Segregation (Create) form closes.

21 Click on the OK button. The Shelf (Edit) form closes.

Procedure 17-71 To configure a loopback test on a 9500 MPR DS1, ES1 or radio modem port

Perform the steps in this procedure as required on the port type that you are configuring.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 9500 MPR port object (DS1, ES1, or radio modem) in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens.

3 Click on the Loopback tab button.

4 Select an interface. Click on the Properties button.

5 The Loopback (Edit) form opens.

6 Configure the parameters:

- Activation
- Timeout Period (Days)
- Timeout Period (Hrs)
- Timeout Period (Mins)

7 Click on the OK button. The Loopback (Edit) form closes.

8 On the Physical Port (Edit) form, click on the OK button.

9 The Physical Port (Edit) form closes.

Note — If the card containing the ports is not equipped but configured, a loopback test cannot be performed on the physical ports of the card.

Procedure 17-72 To configure SONET ports

Perform the steps in this procedure as required depending on the daughter card and port type that you are configuring.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens.

3 Configure the parameters:

- Description
- Speed
- DDM Event Suppression
- OLC State

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

4 Click on the States tab button.

5 Configure the Administrative State parameter.

6 Click on the Channels tab button to configure the SONET/SDH channel.

a Click on the Add button to create a new channel.

b Choose a channel from the list and click on the Properties button to view and edit the channel parameters.

c Choose a channel from the list and click on the Delete button to remove a channel from the port.

7 Click on the SONET tab button.

8 Configure the parameters:

- Framing
- Clock Source
- Loopback
- Single Fiber
- Hold Time Down (100s of ms)
- Hold Time Up (100s of ms)
- Tx DUS/DNU

9 Click on the SONET Monitoring tab button.

10 Configure the parameters:

- BER Signal Degradation Threshold
- BER Signal Failure Threshold
- Report Alarms

11 Click on the SONET Overhead tab button.

12 Configure the parameters:

- SONET Section Trace Mode
- J0 Byte

  Enter a J0 byte that identifies the circuit. This byte is inserted continuously at source. This can be checked against the expected value by the receiver. If no byte is entered, then null is used. The parameter is configurable when the SONET Section Trace Mode is set to Byte.
- J0 String

  The parameter is configurable when the SONET Section Trace Mode is set to String.

13 Click on the other tab buttons in the properties form to view and edit additional port information.

14 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 17-73 To configure TDM DS3 ports

Perform the steps in this procedure as required depending on the port type that you are configuring.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens.

3 Configure the General tab parameters:

- Description
- Speed
- OLC State
- DDM Event Suppression

4 Click on the States tab button.

5 Configure the Administrative State parameter.

6 Click on the DS3/E3 tab button.

7 Configure the parameters:

- Line Buildout
- Type

8 Click on the other tab buttons in the properties form to view and edit additional port information.

9 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 17-74 To configure a 7250 SAS CES TDM DS1/E1 port

Perform this procedure to configure a TDM DS1/E1 port on a CES 2-Port Gig Ethernet MDA card.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 7250 SAS CES port in the Equipment view and choose Properties. The Physical Port (Edit) form appears with the General tab displayed.

3 Configure the Description parameter.

4 Click on the States tab button.

5 Configure the Administrative State parameter.

6 Click on the T1/E1 tab button.

7 Configure the parameters:

- Line Buildout
- Line Length
- Line Impedance

8 Click on the OK button. A dialog box appears.

9 Click on the OK button.

Procedure 17-75 To configure a 7710 SR channelized TDM DS1 or E1 port

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 7710 SR port in the Equipment view that contains a channelized DS1 or E1.

3 Choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- OLC State

5 Click on the DS1/E1 tab button.

6 Configure the parameters:

- Port Type
- Line Buildout
- Line Length
- Db Loss

7 Click on the States tab button.

8 Configure the Administrative State parameter.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 17-76 To configure a 7705 SAR ASAP channelized TDM port

This procedure applies to 7705 SAR channelized TDM DS1/E1 ports and channelized TDM DS3/E3 ports.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 7705 SAR port in the Equipment view that contains a channelized port (DS1/E1 or DS3/E3).

3 Choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- OLC State

5 Click on the DS1/E1 or DS3/E3 tab button.

6 Configure the parameters:

- Port Type
- Line Length
- Line Impedance

All ports of the ASAP daughter card are automatically configured to the same port type when the first port is configured. A mix of DS1 and E1 ports or DS3 and E3 ports is not supported. The Port Type parameter can only be modified when no channels are configured on any port of the daughter card. If all of the channels are deleted on the daughter card, the port type is automatically set to DS1 or DS3 for all ports.

7 Click on the States tab button.

8 Configure the Administrative State parameter.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Physical Port (Edit) form closes.

Procedure 17-77 To configure a 7210 SAS-M channelized TDM DS1 or E1 port

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 7210 SAS-M port in the Equipment view that contains a channelized DS1 or E1.

3 Choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- OLC State

5 Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group - Physical Port form opens.

6 Choose a split horizon group and click on the OK button. The Select Split Horizon Group - Physical Port form closes and the Physical Port (Edit) form refreshes with the split horizon group name.

Note — To create or delete a 7210 SAS split horizon group, see Procedure 17-6.

7 Click on the DS1/E1 tab button.

8 Configure the parameters:

- Port Type
- Line Length
- Line Impedance

Note — The Line Impedance parameter only appears when the Port Type parameter is set to E1.

9 Click on the Qos Pool tab button.

10 Choose a QoS pool from the list and click on the Properties button. The QoS Pool (Edit) form opens.

11 Click on the Select button in the Slope Policy panel. The Select Slope Policy - QoS Pool form opens.

12 Choose a slope policy in the list and click on the OK button. The Select Slope Policy - QoS Pool form closes and the QoS Pool (Edit) form refreshes with the name of the slope policy.

13 Click on the OK button. The QoS Pool (Edit) form closes.

14 Click on the States tab button.

15 Configure the Administrative State parameter.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Physical Port (Edit) form closes.

Procedure 17-78 To configure 7250 SAS-ESA or 7210 SAS-M24F2XFP [ETR] dry contact sensors

Perform the following procedure to configure dry contacts. See section 11.1 for information about dry contact sensors.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a shelf object in the Equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the Dry Contacts tab button.

4 Choose one of the dry contacts and click on the Properties button. The DryContact (Edit) form opens.

5 Configure the parameters:

- Name
- Description
- Monitored Status
- Polarity
- Alarm Severity
- Alarm Trigger Message
- Alarm Clear Message

6 Click on the OK button to close the DryContact (Edit) form.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Shelf (Edit) form closes.

Procedure 17-79 To configure a 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA CES module

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA daughter card slot in the Equipment view that accommodates a CES module, such as slot 4 or 5.

3 Choose Properties from the contextual menu. The Daughter Card Slot (Edit) form appears with the General tab displayed.

4 Click on the CES tab button.

5 Configure the parameters:

- Mode
- IP Address
- Gateway IP Address
- Clock Mode
- Mask

6 Click on the OK button. A dialog box appears.

7 Click on the OK button.

Procedure 17-80 To configure a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES port

Perform this procedure to configure the framing scheme for the attached E1 or T1 line.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES port in the Equipment view and choose Properties. The Physical Port (Edit) form appears with the General tab displayed.

Right-click on a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES port in the Equipment view and choose Properties. The Physical Port (Edit) form appears with the General tab displayed.

3 Configure the Description parameter.

4 Configure the Default VLAN parameter.

5 Click on the States tab button.

6 Configure the Administrative State parameter.

7 Click on the T1/E1 tab button.

8 Configure the parameters:

- Port Framing
- Line Code
- Loopback
- Line Buildout
- Line Length
- Db Loss
- Line Impedance

The Db Loss parameter is configurable when the Line Buildout parameter is set to Long.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button.

Procedure 17-81 To create a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA unstructured CES interface

Perform this procedure to create an unstructured CES interface on a TDM port, to extend clear channel services across an Ethernet or MPLS network.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a configured 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES port in the Equipment view and choose Create Interface. The Unstructured Interface (Create) form appears.

3 Configure the Description parameter.

4 Click on the CES tab button.

5 Configure the Interface ID parameter.

6 Click on the OK button. A dialog box appears.

7 Click on the OK button. The unstructured CES interface appears in the navigation tree under the port of the daughter card.

Procedure 17-82 To create a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA structured CES interface

Perform this procedure to configure a structured CES interface to channel multiple DS-0 channels to one or more multiple destinations across an Ethernet or MPLS network.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA daughter card slot in the Equipment view that accommodates a CES module, such as slot 4 or 5.

3 Choose Create CES Channel Group from the contextual menu. The CES Channel Group (Create) form appears with the General tab displayed.

4 Configure the Channel ID parameter.

Note — Channel groups with an ID that is greater than 30 must be created, modified, or deleted using a CLI session due to SNMP limitations on the device. See chapter 14 for more information about starting a CLI session.

5 Click on the Channel Group tab button.

6 Click on the Select button in the Port panel. The Select Port - CES Channel Group form appears.

7 Choose a port from the list and click on the OK button. The Select Port - CES Channel Group form closes and the selection appears in the Name field.

8 Configure the Time Slots panel. For a DS0 group from a T1, choose from 1 to 24. For a DS0 group from an E1, choose from 1 to 31.

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The structured CES interface appears in the navigation tree under the CES channel group of the daughter card.

Procedure 17-83 To modify a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA CES interface

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a configured CES Interface in the Equipment view and choose Properties. The Unstructured Interface (Edit) form opens for a CES interface that is assigned to a TDM port, or the Structured Interface (Edit) form opens for a CES interface that is assigned to a channel group. The General tab is displayed.

3 Configure the Description parameter.

4 Click on the States tab button.

5 Configure the Administrative State parameter.

6 Click on the CES tab button.

7 Configure the parameters:

- Protocol
- Max Jitter Expected (ms)
- Samples Aggregation
- Destination Port
- Destination IP Address
- Local Port
- Destination MAC Address
- Destination ECID
- Local ECID
- Priority

8 Click on the OK button. A dialog box appears.

9 Click on the OK button.

Procedure 17-84 To configure SONET clear channels

Perform this procedure to configure SONET clear channels on OC3 to OC192 ports that provide clear channel services. Each port supports one clear channel.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a clear channel port in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed. SONET is the default framing scheme.

Note — A clear channel port is a port on a card that is not designated Deep Channelized.

3 Configure the parameters:

- Description
- Speed

4 Click on the Apply button.

5 In the navigation tree, right-click on the port and choose Create Channel. The Channel (Create) form opens with the General tab displayed. If there are no channels available on that port, the Create Channel menu option menu is dimmed.

6 Configure the parameters:

- Description
- Configured MAC
- Mode
- Encap Type
- MTU (bytes)
- DDM Event Suppression
- Load Balance Algorithm

The Encap Type parameter is configurable when the Mode parameter is set to Access.

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

7 Click on the Apply button to save the changes. The STS*n* clear channel appears in the navigation tree under the port of the daughter card.

a If the Encap Type parameter of the port is ATM, the form is refreshed.

b If the Encap Type parameter of the port is not ATM, go to step 12.

8 Click on the Edit ATM button to configure the ATM interface. The ATM interface form opens with the General tab displayed.

9 Configure the parameters:

- ATM Interface Cell Format
- ATM Minimum VPI Value
- Interface Mapping

10 To create an ILMI link, see Procedure 17-96.

11 Click on the OK button. The ATM Interface form closes.

12 Close the Channel (Edit) form.

Procedure 17-85 To automatically create all channels

Perform this procedure to automatically create all of the channels on OC12, OC3 and DS3 and E3 ASAP ports.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Create All Channels. The Create All Channels form opens.

3 Configure the parameters, as required:

- Channel Type
- STs1 Channel Payload Type
- Ds3 Channel Payload Type

4 Click on the Execute button. The channels and sub-channels appear in the navigation tree under the port of the daughter card.

Procedure 17-86 To configure SONET sub-channels

SONET sub-channels are available on deep channelized OC12 and OC3 ports. SONET STS1 channels support the following payload types:

- DS3
- VT15
- VT2

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port object in the Equipment view and choose Create Channel. The Create Channel form opens with the General tab displayed.

Note — When there are no channels available on that port, the Create Channel menu option menu is dimmed

3 Configure the parameters:

- Local Channel ID
  - For an OC3 port, use a value from 1 to 3.
  - For an OC12 port, use a value in the format <1 to 4>.<1 to 3>
- Payload Type
- DDM Event Suppression

The DDM Event Suppression parameter is configurable only on ports on SFPs and XFPs optical modular transceivers.

4 Click on the Apply button.

The STS1 (AU3) channel appears in the navigation tree under the port of the daughter card.

5 Create the STS1 (AU3) sub-channels according to the payload type configured:

a To create VT15 (Sdh TU11) sub-channels, go to Procedure 17-88.

b To create VT2 (Sdh TU12) sub-channels, go to Procedure 17-88.

c To create a DS3 or E3 (SDH framing only) clear channel, go to step 6.

6 To create a DS3 or E3 clear channel, perform the following steps:

i From the navigation tree, select an STS1 or AU3 channel and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens.

- For AU3 channels, DS3 and E3 channelization is available.
- For STS1 channels, only DS3 channelization is available.

ii Configure the Description parameter.

iii Configure the Channelized parameter.

- Choose Ds1 to channelize the DS3 to carry up to 28 DS1 channelized to the DS0 level.
- Choose E1 to channelize the DS3 to carry up to 21 E1 channelized to the DS0 level.
- Choose None to create a DS3 or E3 clear channel. Configure the following parameters:
  - Configured MAC
  - Encap Type
  - Speed
  - MTU (bytes)
  - Load Balance Algorithm

iv Click on the OK button.

If you set the Channelized parameter to None, a DS3 clear channel in Access mode is created under the STS1 or the AU3 in the navigation tree.

If you set the Channelized parameter to DS1, a DS3 channelized for DS1 is created under the STS1 (AU3). Go to step 9 in Procedure 17-91 to create the DS1 channels.

If you set the Channelized parameter to E1, a DS3 channelized for E1 is created under the STS1 (AU3) in the navigation tree. Go to step 9 in Procedure 17-91 to create the E1 channels.

Procedure 17-87 To configure SDH sub-channels

SDH sub-channels are available on deep channelized OC12 and OC3 ports. SDH AU4 channels support the following payload types:

- TU3
- TU11
- TU12

SDH AU3 channels support the following payload types:

- DS3
- E3
- TU11
- TU12

Perform this procedure to configure SDH sub-channels on ports that provide channelized services. You must first configure port framing to SDH since default framing on SONET/SDH ports is SONET.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a deep channelized port the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

3 Click on the SONET tab button and set the Framing parameter to SDH.

4 Click on the OK button.

5 Right-click on the port again and choose Create Channel from the contextual menu. The Channel Type Selection window opens.

6 Choose one of the following channel types and click on the OK button:

a SONET Sts1 (Sdh Au3).

SONET STS1 channelization and SDH AU3 channelization are equivalent. Go to step 3 of Procedure 17-86.

b SONET Sts3 (Sdh Stm1).

The Sts3 SONET Channel (Create) form opens with the General tab displayed. If there are no channels available on that port, the Create Channel menu option menu is dimmed.

The Payload Type parameter for SDH STM1 (AU4) is set to TUG3. There is no SONET framing equivalent. Go to step 7.

7 Configure the parameters:

- Description
- Local Channel ID

8 Click on the States tab button.

9 Configure the Administrative State

10 Click on the OK button. The STM1 (AU4) channel appears in the navigation tree under the port of the daughter card. It contains three TUG3 groups.

11 Right-click on a TUG3 group and choose Properties from the contextual menu. The Sdh Tug3 (Edit) form opens with the General tab displayed.

12 Choose one of the following options to configure the Payload Type parameter:

a PDH Tu3. Click on the Cancel button and go to step 13 to create a TU3 channel.

b SONET VT15 (SDH Tu11). Click on the Apply button and go to Procedure 17-88.

c SONET VT2 (SDH Tu12). Click on the Apply button and go to Procedure 17-88.

13 To create a TU channel, right-click on the TUG3 group and choose Create Channel from the contextual menu. The TU3 Channel (Create) form opens.

14 Configure the parameters:

- Description
- Payload Type

15 Click on the States tab button.

16 Configure the Administrative State

17 Click on the OK button. A TU3 channel is created under the TUG3 group in the navigation tree.

18 Right-click on the Tu3 and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens with the General tab displayed.

The E3 is the only payload type available.

19 Configure the parameters:

- Description
- Configured MAC
- Encap Type
- Speed
- MTU (bytes)
- Load Balance Algorithm

20 Click on the States tab button.

21 Configure the Administrative State

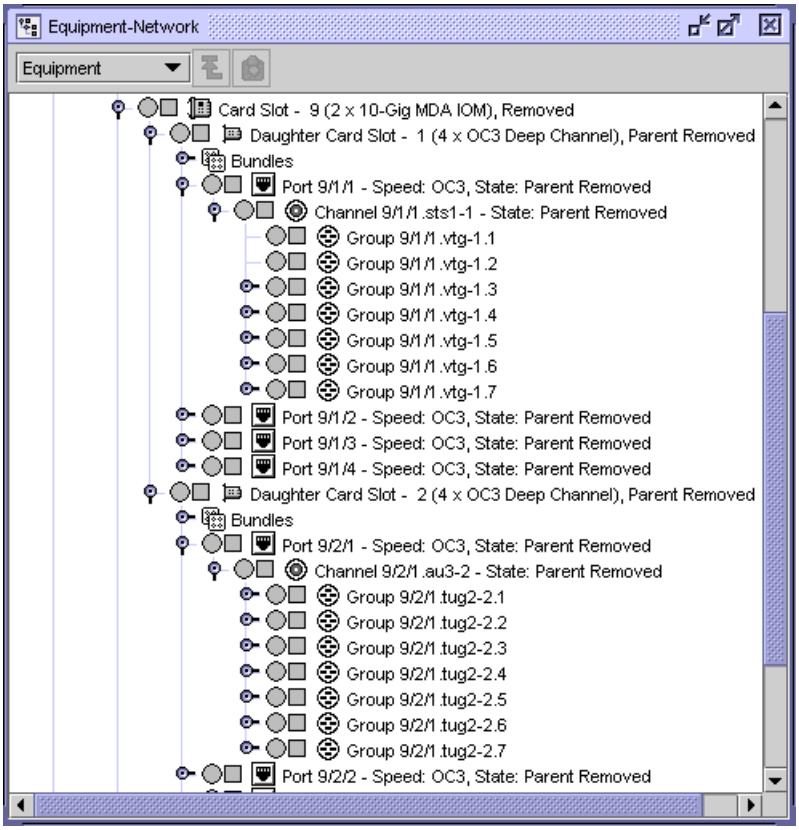
22 Click on the OK button. An E3 clear channel is created under the AU4/TUG3 in the navigation tree.

Procedure 17-88 To create VT15 (TU11) or VT2 (TU12) sub-channels

A SONET VTG and an SDH TUG2 are equivalent groups. A VTG contains four VT15 channels or three VT2. A TUG2 contains four TU11 channels or three TU12. An SDH TUG 3 has no SONET equivalent, however, it contains seven TUG2. (An STM1/AU4 contains three TUG3). See "Comparison of SONET and SDH hierarchies" in section 15.17.

An STS1 channelized to carry a VT15 or VT2 payload type contains seven VTG. An AU3 or a TUG3 channelized to carry a TU11 or TU12 payload type contain seven TUG2. STS1 and AU3 channelization are shown in Figure 17-2.

Figure 17-2 SONET VTG and SDH TUG2 in navigation tree



Each VTG (TUG2) supports up to four VT15 (TU11) channels or three VT2 (TU12) channels. Create each VTG/TUG2 channel one at time.

1 Complete Procedure 17-86 or Procedure 17-87 to carry a VT15 (TU11) or VT2 (TU12) payload type.

   a Go to step 2 to create a VT15 (TU11) channel.

   b Go to step 3 to create a VT2 (TU12) channel.

2 To create a VT15 (TU11) channel, perform the following steps:

   i Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

   ii Right-click on a VTG or TUG2 channel group in the Equipment view that is to carry a VT15 (TU11) payload and choose Create Channel from the contextual menu. The SONET VT (SDH Tu) Channel (Create) form opens.

   iii Configure the parameters:

   - Local Channel ID

     Set the Local Channel ID to a value in the range 1 to 4 since there are four VT15 (TU11) in a VTG (TU2).
   - Description

The default payload type for a VT15 (TU11) channel is PDH DS1. There is no other available payload type.

iv Click on the OK button. A VT15 channel is created under the VTG or a TU11 channel is created under the TUG2 in the navigation tree.

v Right-click on a VT15 or TU11 channel and choose Create Channel from the contextual menu. The DS1/E1 Channel (Create) form opens.

The Local Channel ID is equal to the VT15 channel Local Channel ID parameter and the channel type is set to DS1 since a VT15 or TU11 channel supports one DS1.

vi Click on the OK button A DS1 channel is created under the VT15 or the TU11 in the navigation tree.

You can create up to 28 VT15 (TU11) channels on a VTG (TUG2).

vii Repeat steps 1 and 2 for each VT15 (TU11) channel that you want to create.

viii Since a DS1 channel is not used as a SAP, create a DS0 group for each DS1 channel created. Go to step 10 of Procedure 17-91.

3 To create a VT2/TU12 channel, complete these steps:

i From the navigation tree, select a VTG or TUG2 channel group to carry a VT2 (TU12) payload and choose Create Channel from the contextual menu. The SONET VT (SDH Tu) Channel (Create) form opens.

ii Configure the parameters:

- Local Channel ID
  Set the Local Channel ID to a value in the range 1 to 3 since there are three VT2 (TU12) in a VTG (TUG2).
- Description
- Payload Type
  PDH E1 is not available for SONET framing.

iii Click on the OK button. A VT2 channel is created under the VTG, or a TU12 channel is created under the TUG2 in the navigation tree.

iv Right-click on the VT2 or TU12 channel and choose Create Channel from the contextual menu. The DS1/E1 Channel (Create) form opens.

The Local Channel ID is equal to the VT2 channel Local Channel ID parameter, since a VT2 channel supports one E1 or DS1.

v Click on the States tab button.

vi Configure the Administrative State parameter.

vii Click on the OK button. A DS1 channel is created under the VT2 in the navigation tree. An E1 or DS1 is created under the TU12. You can create up to 21 VT2 (TU12) channels on a VTG (TUG2).

viii Repeat steps 1 and 2 for each VT2 (TU12) that you want to create.

ix Since a DS1/E1 channel is not used as a SAP, create a DS0 group for each DS1 or E1 channel created. Go to step 10 of Procedure 17-91.

Procedure 17-89 To create TDM DS1 channels

Perform this procedure to create DS1 channel and children objects from a channelized DS1 port.

1. Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.
2. Right-click on a port in the Equipment view and choose Properties from the contextual menu.

   The Physical Port (Edit) form opens with the General tab displayed.
3. Configure the parameters:
   - Description
   - OLC State
4. Select the DS1/E1 tab and configure the parameters:
   - Port Type
   - Line Length
5. Click on the OK button.
6. Right-click on the port again and choose Create Channel from the contextual menu. The DS1/E1 Channel (Create) form opens. If there are no channels available on that port, the Create Channel menu option is dimmed.

7 Click on the OK button.

8 To create DS0 channel groups, complete these steps:

i From the navigation tree, select a DS1 or E1 channel and choose Create Channel from the contextual menu. The DS0 Channel Group (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Local Channel ID

  For a DS0 group from a DS1 choose from 1 to 24. For a DS0 group from an E1, choose from 2 to 32.
- Description
- Mode

  All channel groups on a 7705 SAR ASAP port must have the same mode configured. When the first channel group is configured, all other channel groups on the port must be set to the same mode.
- Encap Type

  The default encapsulation type for the 7705 SAR is N/A. The encapsulation type must be changed from N/A to a valid type (ATM, PPP Auto, or CEM). After a valid encapsulation type is configured for a channel group, the encapsulation type cannot be changed for that channel group. To change the encapsulation type, the channel group must be deleted and recreated.
- MTU (bytes)

iii Click on the Channel Group tab button.

iv Configure the parameters:

- CRC Precision
- Scramble
- Idle Cycle Flags
- Time Slots

  Choose one or more timeslots. You can use the Select All and Deselect All buttons.

v Click on the OK button. The timeslot is assigned to the DS0 channel group in the navigation tree.

Procedure 17-90 To configure TDM DS1 or E1 channels

Perform this procedure to edit properties of a DS1/E1 channel and children objects from a channelized DS1/E1 port.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Choose a DS1 or E1 channel in the Equipment view and choose Properties from the contextual menu. The DS1/E1 Channel (Edit) form opens with the General tab displayed.

3 Click on the States tab button.

4 Configure the Administrative State parameter.

5 Add a DS0 channel group, if required. Perform the following steps:

i Click on the SubChannels tab button.

ii Click on the Create Cha... tab button. The DS0 Channel Group (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Local Channel ID
- Description
- Mode
- Encap Type
- Speed
- MTU (bytes)

iv Click on the OK button. The DS0 Channel Group (Create) form closes and a dialog box appears.

v Click on the OK button.

6 Click on the Channel tab button.

7 Configure the parameters:

- Channel Framing
- Clock Source
- Loopback
- Report Alarms
- Respond to Remote Link Signal
- Signal Mode

8 Click on the Statistics tab button to view statistical information.

9 Click on the Faults tab button to view alarm information.

Note — If are configuring a 7705 SAR and selected a clock source of adaptive, you can click on the Adaptive Clock History tab button to view channel adaptive clock performance data for the preceding 15 minutes.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The DS1/E1 Channel (Edit) form closes.

Procedure 17-91 To create TDM DS3 channels

Perform this procedure to create DS3 channel and children objects from a channelized DS3 port.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a port in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- OLC State

4 Choose the DS3/E3 tab and configure the parameters:

- Line Buildout
- Type. Choose DS3.

5 Click on the OK button.

6 Right-click on the port again and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens. If there are no channels available on that port, the Create Channel menu option is dimmed.

7 To configure the DS3/E3 channel, complete these steps:

a Configure the Channelized parameter to DS1 or E1, if you want to channelize to the DS0 level.

b Configure the Channelized parameter to None if this is a clear channel application.

Configure the parameters as required:

- Description
- Configured MAC
- Encap Type
- Speed
- MTU (bytes)
- Load Balance Algorithm

The Local Channel ID parameter is configured automatically and the mode is always Access for TDM.

8 Click on the OK button.

If this is a Channelized DS1 or E1 application, continue to step 9.

9 To create Ds1 or E1 channels, complete these steps:

i From the navigation tree, select a Ds3 channel and choose Create Channel from the contextual menu. The Create DS1/E1 Channel form opens.

ii Configure the Local Channel ID parameter.

- For DS1 choose from 1 to 28.
- For E1 choose from 1 to 21.

iii Click on the OK button. The DS1 or E1 channels are created under the DS3 in the navigation tree.

10 To create DS0 channel groups, complete these steps:

i From the navigation tree, select a DS1 or E1 channel and choose Create Channel from the contextual menu to create DS0 groups. The DS0 Channel (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Local Channel ID
  For a DS0 group from a DS1 choose from 1 to 24. For a DS0 group from an E1, choose from 2 to 32.
- Description
- Configured MAC
- Mode
- Encap Type
- Speed
- MTU (bytes)
- Load Balance Algorithm

iii Click on the Channel Group tab button.

iv Configure the parameters:

- CRC Precision
- Idle Cycle Flags
- Time Slots

  Choose one or more timeslots. You can use the Select All and Deselect All buttons.
- BER SF Link Down

v Click on the OK button. The timeslot is assigned to the DS0 channel group in the navigation tree.

Procedure 17-92 To configure TDM DS3 channels

Perform this procedure to edit properties of a DS3 channel and children objects from a channelized DS3 port.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Choose a DS3 channel in the Equipment view and choose Properties from the contextual menu. The DS3/E3 Channel (Edit) form opens with the General tab displayed.

3 Configure the Description parameter.

4 Configure the Channelized parameter and click on the Apply button.

a If you choose None, go to step 5.

b If you choose DS1 or E1, perform steps 10 to 33.

5 Configure the parameters:

- Configured MAC
- Speed
- MTU (bytes)
- Load Balancing Algorithm

6 Configure the Encap Type parameter and click on the Apply button.

a If you choose BCP Null, BCP DOT1 Q, or IPCP, go to step 7.

b If you choose FR, go to step 8.

c If you choose Cisco HDLC, go to step 9.

d If you choose WAN Mirror, perform steps 11 to 20.

7 Configure the PPP interface for the channel, if required. Perform the following steps:

i Click on the Edit PPP button. The PPP Interface form opens with the General tab displayed.

ii Configure the parameters:

- Period
- Drop Count

iii To view port, PPP control protocol, statistics, or alarm information for the PPP interface, click on the appropriate tab button.

iv Click on the OK button. The PPP Interface form closes.

v Perform steps 11 to 20.

8 Configure the FR interface, if required. Perform the following steps:

i Click on the Edit FR button. The FR Interface form opens with the General tab displayed.

ii Configure the parameters:

- LMI Type
- LMI Mode
- Link Identifier
- Error Threshold
- Monitored Events
- Polling Interval
- Full Inquiry Interval

iii Click on the Frf12 tab button.

iv Set the Mode parameter to Enabled.

v Configure the Fragment Threshold parameter.

vi Click on the Select button beside the MCFR Egress QoS Profile parameter. The Select MCFR Egress Qos Profile - FR Configuration form opens.

vii Choose a profile from the list and click on the OK button. The Select MCFR Egress Qos Profile - FR Configuration form closes and the FR Interface form is refreshed with the MCFR Egress QoS Profile information.

viii To view port, statistical, or alarm information for the FR interface, click on the appropriate tab button.

ix Click on the OK button. The FR Interface form closes.

x Perform steps 11 to 20.

9 Configure the Cisco HDLC information.

i Click on the Cisco HDLC tab button.

ii Configure the parameters:

- Keep-Alive
- Up Count
- Down Count

iii Perform steps 11 to 20.

10 Configure the DS1 and DS0 channels. Perform the following steps:

i Click on the SubChannels tab button.

ii Click on the Add button. The DS1/E1 Channel (Create) form opens with the General tab displayed.

iii Configure the Local Channel ID parameter.

iv Click on the States tab button.

v Configure the Administrative State parameter.

vi Click on the OK button. The DS1/E1 Channel (Create) form closes.

11 Click on the States tab button.

12 Configure the Administrative State parameter.

13 Click on the Channel tab button.

14 Configure the parameters:

- Channel Framing
- CRC Precision
- Clock Source
- Idle Cycle Flags
- Loopback
- Subrate CSU Mode
- Subrate Range
- Loop Respond
- Report Alarms
- Bit Error Insertion Rate (E3 only)
- Pattern (E3 only)
- Duration (seconds) E3 only

15 Click on the Message Data Link tab button.

16 Configure the parameters:

The MDL Message Type parameter specifies the Line Message Data Link message for a DS3 and specifies the transmission method of a message over a channelized interface. The parameter is only applicable if the DS3 is using C-bit framing. The default is disabled. Click on the check boxes to enable transmission methods and enter text strings to choose the message options for this parameter as required. The transmission options are:

- Test Signal
- DS3 Path
- Idle Signal

Table 17-9 describes the MDL message options.

Table 17-9 MDL message options

Option	String Length	Description
Port Number String	0 to 38 characters	specifies the port ID code
Generator Number String	0 to 38 characters	specifies the generator number to send in the MDL test signal message
Equipment ID Code	0 to 10 characters	specifies the Equipment ID code
Location ID Code	0 to 11 characters	specifies the Location ID code
Frame ID Code	0 to 10 characters	specifies the Frame ID code
Unit ID Code	0 to 6 characters	specifies the unit ID code
Facility ID Code	0 to 38 characters	specifies the facility ID code

17 Click on the Terminations tab button to view channel termination information.

18 Click on the Statistics tab button to view statistical information.

19 Click on the Faults tab button to view alarm information.

20 Click on the OK button. The DS3/E3 Channel (Edit) form closes.

21 Right-click on a DS1 channel in the navigation tree and choose Properties from the contextual menu. The property form for the channel opens with the General tab displayed.

22 Click on the States tab button.

23 Configure the Administrative State parameter, if required.

24 Add a DS0 channel group, if required. Perform the following steps:

i Click on the SubChannels tab button.

ii Click on the Add button. The DS0 Channel Group (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Local Channel ID
- Description
- Configured MAC
- Encap Type
- Speed
- MTU (bytes)
- Load Balancing Algorithm

iv Click on the OK button. The DS0 Channel Group (Create) form closes.

25 Click on the Channel tab button.

26 Configure the parameters:

- Channel Framing
- Clock Source
- Idle Cycle Flags
- Loopback
- Bit Error Insertion Rate (E3 only)
- Pattern (E3 only)
- Duration (seconds) E3 only

27 Click on the Statistics tab button to view statistical information.

28 Click on the Faults tab button to view information about alarms.

29 Click on the OK button. The channel properties form closes.

30 Configure timeslots for the DS0 channel group. Perform the following steps.

i Choose a DS0 channel in the navigation tree and choose Properties from the contextual menu. The property form for the channel opens with the General tab displayed.

ii Configure the parameters, as required.

iii Click on the States tab button.

iv Configure the Administrative State parameter.

v Click on the Channel Group tab button.

vi Configure the parameters:

- CRC Precision
- Idle Cycle Flags
- Time Slots

  Choose one or more timeslots. You can use the Select All and Deselect All buttons.

vii If you set the Encap Type parameter is set to BCP Null, BCP DOT1 Q, or IPCP in step ii, you can configure the PPP for the timeslot on the Channel Groups tab.

- Click on the Edit PPP button. The PPP Interface form opens with the General tab displayed.
- Configure the parameters:
  - Period
  - Drop Count
  - Compression

    The Compression parameter is configurable if the DS1 or E1 channel group is on an ASAP MDA in a 7750 SR or 7710 SR, Release 6.1 or later.
- Click on the OK button. The PPP Interface form closes and the DS0 Channel Group (Edit) form reappears.

31 Click on the Statistics tab button to view statistical information.

32 Click on the Faults tab button to view information about alarms.

33 Click on the OK button. The DS3/E3 Channel (Edit) form closes.

Procedure 17-93 To configure a DS3/E3 channel as a network interface on a channelized ASAP MDA

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Perform one of the following.

a If you are configuring an OC-*n* channelized ASAP MDA, right-click on an available port in the Equipment view and choose Create Channel from the contextual menu. The Sts SONET Channel (Create) form opens with the General tab displayed; go to step 3.

b If you are configuring a DS3/E3 channelized ASAP MDA, right-click on an available port in the Equipment view and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens with the General tab displayed; go to step 8.

3 Configure the parameters:

- Local Channel ID
- Description
- Payload Type

4 Click on the States tab button.

5 Configure the Administrative State parameter.

6 Click on the OK button.The Sts SONET Channel (Create) form closes and the STS1 channel appears in the navigation tree under the port of the channelized ASAP daughter card.

7 Right-click on the STS1 channel and choose Create Channel from the contextual menu. The DS3/E3 Channel (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Description
- Configured MAC
- Mode
  You must set the Mode parameter to Network.
- Encap Type
  The only available encapsulation type available in network mode is PPP.
- Speed
  The only available speed is line rate.
- MTU (bytes)
- Load Balance Algorithm

9 Click on the States tab button.

10 Configure the Administrative State parameter.

11 Click on the Apply button. The form displays additional tabs.

12 Click on the Channel tab button.

13 Configure the parameters:

- Channel Framing
- CRC Precision
- Clock Source
- Idle Cycle Flags
- Loopback
- Subrate CSU Mode
- Loop Respond
- Report Alarms

14 Click on the Message Data Link tab button.

15 Configure the parameters:

The MDL Message Type parameter specifies the Line Message Data Link message for a DS3 and specifies the transmission method of a message over a channelized interface. The parameter is only applicable if the DS3 is using C-bit framing. The default is disabled. Click on the check boxes to enable transmission methods and enter text strings to choose the message options for this parameter as required. The transmission options are:

- Test Signal
- DS3 Path
- Idle Signal

Table 17-9 describes the MDL message options.

Table 17-10 MDL message options

Option	String Length	Description
Port Number String	0 to 38 characters	specifies the port ID code
Generator Number String	0 to 38 characters	specifies the generator number to send in the MDL test signal message
Equipment ID Code	0 to 10 characters	specifies the Equipment ID code
Location ID Code	0 to 11 characters	specifies the Location ID code
Frame ID Code	0 to 10 characters	specifies the Frame ID code
Unit ID Code	0 to 6 characters	specifies the unit ID code
Facility ID Code	0 to 38 characters	specifies the facility ID code

16 Click on the OK button. The DS3/E3 or Sts SONET Channel (Create) form closes and a DS3/E3 channel appears in the navigation tree under the port on the channelized ASAP MDA.

Procedure 17-94 To configure an L3 interface on a DS3/E3 channel on a channelized ASAP MDA

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a DS3/E3 channel on a channelized ASAP MDA port and choose Properties from the contextual menu. The DS3/E3 Channel (Edit) form opens with the General tab displayed.

3 Click on the Policies tab button to configure the policies for the DS3/E3 channel. Perform the following steps.

i Click on the Select button beside the Network Queue Policy Name parameter. The Select Network Queue Policy - DS3/E3 Channel list form opens.

ii Select a network queue policy from the list and click on the OK button. The Select Network Queue Policy - DS3/E3 Channel list form closes and the DS3/E3 Channel (Edit) form reappears.

iii Click on the Select button beside the ID parameter in the Accounting Policy panel. The Select Accounting Policy - DS3/E3 Channel list form opens.

iv Select an accounting policy from the list and click on the Ok button. The Select Accounting Policy - DS3/E3 Channel list form closes and the DS3/E3 Channel (Edit) form refreshes with the accounting policy information.

v Configure the Collect Accounting Statistics parameter.

vi Click on the Select button in the Port Scheduler Policy panel to assign a port scheduler policy to the port. The Select Port Scheduler Policy - Physical Port form opens.

vii Select a port scheduler policy from the list and click on the OK button. The Select Port Scheduler Policy - Physical Port form closes.

4 Click on the Network Interfaces tab button.

5 Click on the Add button. The Create Network Interface - Routing Instance form opens.

6 Perform steps 4 to 42 of Procedure 27-4 to create a network interface on the DS3/E3 channel.

The port in step 6 of Procedure 27-4 is set to the DS3/E3 channel by default. Go to step 11 of Procedure 27-4.

7 The L3 interface appears on the Network Interfaces tab. Close the Ds3/E3 Channel (Edit) form.

Procedure 17-95 To configure a PVC

PVCs are automatically created by the device when a new L3 interface over ATM is created on the 5620 SAM, and when a new ILMI link is created between ATM interfaces. See Procedure 17-96 for more information about creating ILMI links.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a SONET/SDH ATM clear channel in the Equipment view and choose Properties from the contextual menu. The property form for the channel opens with the General tab displayed.

3 Click on the L3 Interfaces tab button.

4 Choose the appropriate interface from the list and click on the Properties button. The L3 Interface form opens.

5 Click on the ATM tab button.

6 Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling

7 Click on the Apply button to save the changes.

8 To view more information about the PVC:

i Click on the View PVC Connection button. The ATM PVC Connection form opens.

ii Click on the tab buttons to view information for the ATM PVC connection.

9 Click on the Cancel button to close the ATM PVC Connection form, the L3 Interface form, and the channel form.

Procedure 17-96 To create an ILMI link

Perform this procedure to create an ILMI link between device ATM interfaces. This functionality is supported on the 7750 SR and 7710 SR. Ensure that ATM QoS policies are configured before you create the ILMI link. See chapter 43 for more information about creating ATM QoS policies.

1 Perform one of the following to open the ATM Interface properties form.

a Use the navigation tree

i Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

ii Right-click on a clear channel port and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

Note — A clear channel port is a port on a card that is not designated Deep Channelized.

iii Click on the Channels tab button.

iv Choose the appropriate channel from the list and click on the Properties button. The Channel (Edit) form opens.

v Click on the Edit ATM button. The ATM Interface form opens with the General tab displayed.

b Use the Manage Equipment list form to search for a clear channel port with an ATM interface.

i Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

ii Choose Port from the object drop-down list.

iii Configure the filter criteria to search for ATM encapsulation types.

iv Click on the Search button. The Select form displays the results of the search.

v Select an entry by double-clicking. Alternatively, select an entry and click on the Properties button. The Select form closes and the Channel (Edit) form opens.

vi Click on the Edit ATM button. The ATM Interface form opens with the General tab displayed.

2 Click on the Create ILMI Link button. The Configure ILMI Link form opens with the General tab displayed.

3 Configure the parameters:

- Administrative Status
- Protocol Version
- Ime Type
- Egress Traffic Descriptor

  Choose an ATM QoS policy by clicking on the Select button to open the egress traffic descriptor list form. Click on the Search button and choose an ATM traffic descriptor profile from the list to associate with the ILMI link. Click on the OK button.
- Ingress Traffic Descriptor

  Choose an ATM QoS policy by clicking on the Select button to launch the ingress traffic descriptor list form. Click on the Search button and choose an ATM traffic descriptor profile from the list to associate with the ILMI link. Click on the OK button.
- Keep-Alive Polling Frequency (seconds)
- Keep-Alive Polling Count
- Keep-Alive Test Frequency (seconds)
- Restore Keep-Alive Defaults
- ILMI VPI
- ILMI VCI

The Restore Keep-Alive Defaults parameter restores the default values of the Keep-Alive Polling Frequency (seconds), Keep-Alive Polling Count, and Keep-Alive Test Frequency (seconds) parameters.

The Keep-Alive Test Frequency (seconds) parameter is configurable when the Protocol Version parameter is set to 4.0.

4 Click on the Finish button. The Configure ILMI Link form closes and the ATM Interface form reappears.

5 Close the ATM Interface form. The Channel (Edit) form reappears.

6 Close the Channel (Edit) form.

Procedure 17-97 To modify an ILMI link

1 Perform step 1 of Procedure 17-96 to open the ATM Interface form.

2 Click on the Edit ILMI Link button. The Configure ILMI Link form opens with the ILMI Link Configuration tab displayed.

3 Configure the parameters, as required.

- Administrative Status
- Protocol Version
- Ime Type
- Egress Traffic Descriptor

  Choose an ATM QoS policy by clicking on the Select button to open the egress traffic descriptor list form. Click on the Search button and choose an ATM traffic descriptor profile from the list to associate with the ILMI link. Click on the OK button.
- Ingress Traffic Descriptor

  Choose an ATM QoS policy by clicking on the Select button to launch the ingress traffic descriptor list form. Click on the Search button and choose an ATM traffic descriptor profile from the list to associate with the ILMI link. Click on the OK button.
- Keep-Alive Polling Frequency (seconds)
- Keep-Alive Polling Count
- Keep-Alive Test Frequency (seconds)
- Restore Keep-Alive Defaults

The Restore Keep-Alive Defaults parameter restores the default values of the Keep-Alive Polling Frequency (seconds), Keep-Alive Polling Count, and Keep-Alive Test Frequency (seconds) parameters.

The Keep-Alive Test Frequency (seconds) parameter is configurable when the Protocol Version parameter is set to 4.0.

4 Click on the Peer Interface Configuration tab to view ILMI properties of the peer interface of the link.

5 Click on the OK button to close the Configure ILMI Link form. The ATM Interface form reappears.

6 To remove an ILMI link, click on the Remove ILMI Link button. Removing the ILMI link also removes the PVC.

Note — An ILMI link can be removed only if its Administrative Status parameter is set to Disabled.

7 Click on the Cancel button to close the ATM Interface form. The Channel (Edit) form reappears.

8 Click on the Cancel button to close the Channel (Edit) form.

Procedure 17-98 To create a multilink PPP bundle

You can create multilink PPP bundles to:

- bundle DS0 channels together to be used as a SAP
- provide a mechanism to distribute data across multiple links to achieve higher bandwidth

The following general rules apply to multilink bundles.

- Table 17-11 lists the maximum number of multilink bundles that can be created on each MDA.
- DS0 channels can be aggregated on a single MDA only.
- Up to 8 members can be added to a bundle.
- The Encap Type parameter of a member cannot be set to FR.
- A DS0 channel can host only one SAP.
- If a channel is being used as a SAP, it cannot be added to a bundle.

Table 17-11 Multilink bundle configuration maximum

MDA	Bundle maximum
All MDAs other than channelized ASAP MDAs	56
• 1 x OC12 Deep Channel • 4 x OC3 Deep Channel • 12 x DS3/E3 Deep Channel • 4 x DS3/E3 Deep Channel • 8 x DS1/E1 Channel CMA (7710 SR)	56
4 x Channelized DS3/E3 ASAP MDA	112
• 4 x Channelized OC3 ASAP • 1 x Channelized OC12 ASAP • 12 x Channelized DS3/E3 ASAP	256

Note — To create an IMA group bundle, perform Procedure 17-99.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on the Bundles object in the Equipment view and choose Create Bundle from the contextual menu. The Create Multilink Bundle form opens.

3 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description

4 Click on the Next button. The Configure Bundle Parameters form opens.

5 Set the Bundle Type parameter to PPP.

Note 1 — To create an IMA group bundle, perform Procedure 17-99.

Note 2 — To create an FR group bundle, perform Procedure 17-100

6 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)
- Bundle MRRU (bytes)
- Short Sequence
- Link Fragmentation and Interleaving

7 Click on the Next button. The Configure Bundle Members form opens.

8 Click on the Add button to add DS0 channel groups to the bundle.

The Add Bundle Member series of configuration steps appears.

9 Configure the Show Only Compatible Channels parameter.

10 Click on the Next button.

The Select Channels form opens.

11 Select compatible channels from the list to construct the bundle.

Add channels to a bundle as follows:

- Choose up to eight channel groups from the list of channels.

Note 1 — If there are no compatible channels to choose from and you have decided that you want to edit some of the existing channels that are not compatible to be compatible, click on the Back button and disable the Show Only Compatible Channels parameter. Click on the Next button. Choose channels to edit from the list and click on the Properties button.

Note 2 — The channel group with the lowest Port ID is chosen as the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member to select it as a compatible member.

12 Click on the Finish button. The Configure Bundle Members form closes and the Create Multilink Bundle form re-opens.

13 Click on the Finish button.

14 Click on the Close button. The Create Multilink Bundle form closes.

15 Use the Properties contextual menu to view information about the created bundle, or modify bundle parameters.

- The General tab displays the Bundle ID, CLI name, MTU (bytes), Mode, and Encap Type parameters.
- The MultiLink Bundle tab displays the bundle type, bundle parameters, and link information.
- The L2 Interfaces and L3 Interfaces tab lists the interfaces that the bundle is assigned to.
- The States tab displays information about the operational and administrative state of the bundle.
- The Bundle Members tab lists the bundle members. From this form you can view member information and add or remove members from the bundle.
- Statistics and fault information is available from the appropriate tabs.

Procedure 17-99 To create an IMA group bundle

IMA group bundles combine ATM-encapsulated DS0 channel groups into a single ATM interface. The following general rules apply to IMA group bundles. See Procedure 17-98 for the general rules that apply to multilink PPP bundles. See Procedure 17-100 for the general rules that apply to FR group bundles.

- IMA group bundles can only be created on:
  - channelized ASAP MDAs with SDH or SONET framing the 7750 SR or 7710 SR
  - ATM DS1/E1 CMA on the 7710 SR
  - channelized DS1/E1 ASAP daughter cards on the 7705 SAR
- The encapsulation type of the DS0 group channel must be ATM.
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.
- Table 17-12 lists the maximum number of IMA group bundles that can be created on each MDA.
- IMA group members must be on the same MDA.

Table 17-12 IMA group bundle configuration maximums

Device	MDA	Bundle maximum
7750 SR, all supported releases	All MDAs other than channelized ASAP MDAs	56
7750 SR, all supported releases 7710 SR, all supported releases	4 x Channelized DS3/E3 ASAP MDA	112
7750 SR, all supported releases 7710 SR, all supported releases	• 4 x Channelized OC3 ASAP • 1 x Channelized OC12 ASAP • 12 x Channelized DS3/E3 ASAP •	256
7710 SR, all supported releases	8 x ATM DS1/E1 CMA	8
7705 SAR, all supported releases	16 x Channelized DS1/E1 ASAP	8
7705 SAR, Release 2.1 or later	2 x Channelized OC3/STM1 ASAP	16

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on the Bundles object in the Equipment view and choose Create Bundle from the contextual menu. The Create Multilink Bundle form opens.

3 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description

4 Click on the Next button. The Configure Bundle Parameters form opens.

5 Set the Bundle Type parameter to IMA.

Note 1 — To create a PPP group bundle, perform Procedure 17-98.

Note 2 — To create an FR group bundle, perform Procedure 17-100

6 Configure the parameters:

- Bundle Type
- Red Diff Delay (milliseconds)
- Minimum Links
- IMA Version
- ATM Interface Cell Format
- ATM Minimum VPI Value
- Test Pattern
- Link Activation Timer
- Link Deactivation Timer
- Maximum Links

7 Click on the Next button. The Configure Bundle Members form opens.

8 Perform one of the following:

a To create the multilink bundle without adding any members, go to step 9.

b Add DS0 channel groups to the bundle by performing the following steps.

i Click on the Add button. The Add Bundle Member series of configuration steps appears.

ii Click on the Next button. The Select Channels form opens.

iii Choose up to 8 channel groups from the list of channels to construct the bundle.

Note — The channel group with the lowest Port ID is chosen as the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member to select it as a compatible member.

9 Click on the Finish button. The Configure Bundle Members form closes and the Create Multilink Bundle form reappears.

10 Close the Create Multilink Bundle form.

Procedure 17-100 To create an FR group bundle

FR group bundles are used to fragment lower priority DLCI frames to minimize jitter and delay on higher priority DLCI frames. The following general rules apply to FR group bundles. See Procedure 17-98 for the general rules that apply to multilink PPP bundles. See Procedure 17-99 for the general rules that apply to IMA group bundles.

- FR group bundles can only be created on channelized ASAP MDAs.
- FRF12 cannot be enabled on a SAP that is using an FR group bundle.
- DS0 channel groups must have all their timeslots selected and have their encapsulation type set to FR to be configured as bundle members.

Table 17-13 FR group bundle configuration maximum

Device	MDA	Bundle maximum
7750 SR, Release 7.0 or later 7710 SR, Release 7.0 or later	All supported channelized ASAP MDAs	128

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on the Bundles object in the Equipment view and choose Create Bundle from the contextual menu. The Create Multilink Bundle form opens.

3 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description

4 Click on the Next button. The Configure Bundle Parameters form opens.

5 Set the Bundle Type parameter to FR.

Note 1 — To create a PPP group bundle, perform Procedure 17-98.

Note 2 — To create an IMA group bundle, perform Procedure 17-99

6 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)

7 Click on the Next button. The Configure Bundle Members form opens.

8 Perform one of the following:

a To create the multilink bundle without adding any members, go to step 9.

b Add DS0 channel groups to the bundle by performing the following steps.

i Click on the Add button. The Add Bundle Member series of configuration steps appears.

ii Click on the Next button. The Select Channels form opens.

iii Choose up to 8 channel groups from the list of channels to construct the bundle.

Note — The channel group with the lowest Port ID is chosen as the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member to select it as a compatible member.

9 Click on the Finish button. The Configure Bundle Members form closes and the Create Multilink Bundle form reappears.

10 Close the Create Multilink Bundle form.

Procedure 17-101 To modify a multilink PPP bundle

Perform the following procedure to edit multilink PPP bundle parameters, add group members, and configure MC MLPPP to allow multiple classes of services to be transmitted over the bundle.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on a multilink bundle in the Equipment view and choose Properties from the contextual menu. The Multilink Bundle (Edit) form for the PPP bundle opens with the General tab displayed.

3 Configure the Description parameter.

4 Click on the Multilink Bundle tab button.

5 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)
- Bundle MRRU (bytes)
- Short Sequence
- Link Fragmentation and Interleaving

6 Click on the States tab.

7 Configure the Administrative State parameter, if required.

8 Configure the MLPPP bundle for multiclass service transmission. Perform the following steps.

Note — Consider the following when you configure MC MLPPP.

- MC MLPPP is supported only on channelized ASAP MDAs on the 7710 SR and 7750 SR, Release 6.0 or later, and on the 7705 SAR, Release 2.0 or later.
- You must configure MC MLPPP before you add bundle members to the multilink bundle.
- MC MLPPP is not supported when the port is configured as network mode.
- MC MLPPP is not supported when LFI is enabled.

i Click on the MLPPP tab button.

ii Configure the parameters:

- End Point ID
- End Point Class ID
- Class Count
- Magic Number

Note — Magic Number is supported only on channelized ASAP MDAs on the 7710 SR and 7750 SR, Release 7.0 or later.

iii Click on the Select button in the MLPPP Ingress QoS Profile or MLPPP Egress QoS Profile panel to choose an MLPPP ingress or egress QoS profile. If a profile is already selected, click on the Clear button to clear the selection and enable the Select button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form opens.

Note — You can only apply QoS profiles to an MLPPP bundle if the Class Count parameter is set to 4.

iv Select a profile and click on the OK button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form closes.

v Click on the OK button. A dialog box appears.

vi Click on the Yes button.

9 To add members to the multilink bundle, perform the following steps.

i Click on the Bundle Members tab button.

ii Click on the Add button to add DS0 channel groups to the bundle. The Add Bundle Member series of configuration steps appears.

iii Perform steps 9 to 11 of Procedure 17-98.

iv Click on the Finish button. The Add Bundle Member series of configuration steps closes.

Note — You can also add bundle members to the multilink bundle using the contextual menu in the navigation tree.

10 Click on the L2 Access Interfaces and L3 Access Interfaces tab buttons to view the interfaces that the bundle is assigned to.

11 Click on the Service Access Points tab button to view SAP information.

12 Click on the Statistics tab button to view statistical information.

13 Click on the Faults tab button to view information about alarms.

14 Click on the Close button. The Multilink Bundle (Edit) form closes.

Procedure 17-102 To modify an IMA group bundle

Perform the following procedure to edit IMA group bundle parameters, add group members, and specify a test member for IMA group bundle connectivity testing.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on an IMA group bundle in the navigation tree and choose Properties from the contextual menu. The Multilink Bundle (Edit) form for the IMA group bundle opens with the General tab displayed.

3 Configure the Description parameter.

4 Click on the Multilink Bundle tab button.

5 Configure the parameters:

- Red Diff Delay (milliseconds)
- Minimum Links
- IMA Version
- ATM Interface Cell Format
- ATM Minimum VPI Value
- Test Pattern
- Link Activation Timer
- Link Deactivation Timer
- Maximum Links

6 To specify the IMA member that is used to test link connectivity in the IMA group bundle, perform the following steps.

i Click on the Select button beside the Test Member parameter. The Select Interface - Multilink Bundle form opens.

ii Choose an interface from the list.

iii Click on the OK button. The Select Interface - Multilink Bundle form closes and the Multilink Bundle (Edit) form refreshes with the test member information.

7 Click on the Test Pattern Start button to run the test. You can click on the Test Pattern Stop button at any time to stop the test. The Multilink Bundle (Edit) form refreshes with the link connectivity information.

8 Click on the States tab.

9 Configure the Administrative State parameter, if required.

10 To add members to the IMA group bundle, perform the following steps.

i Click on the Bundle Members tab button.

ii Click on the Add button to add DS0 channel groups to the bundle. The Add Bundle Member series of configuration steps appears.

iii Perform step 8 b of Procedure 17-99.

Note — You can also add bundle members to the IMA group bundle using the contextual menu in the navigation tree.

11 Click on the L2 Access Interfaces and L3 Access Interfaces tab buttons to view the interfaces that the bundle is assigned to.

12 Click on the Service Access Points tab button to view SAP information.

13 Click on the Statistics tab button to view statistical information.

14 Click on the Faults tab button to view information about alarms.

15 Click on the Close button. The Multilink Bundle (Edit) form closes.

Procedure 17-103 To modify an FR group bundle

Perform the following procedure to edit FR group bundle parameters, add group members, and specify a test member for FR group bundle connectivity testing.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on an FR group bundle in the navigation tree and choose Properties from the contextual menu. The Multilink Bundle (Edit) form for the FR group bundle opens with the General tab displayed.

3 Configure the Description parameter.

4 Click on the Multilink Bundle tab button.

5 Configure the parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)

6 Click on the MLFR tab button.

7 Configure the parameters:

- Hello Timer
- Ack Timer
- Hello Retry Count

8 Click on the Select button beside the MCFR Ingress Qos Profile parameter. The Select MCFR Ingress Qos Profile - MultiClass Mlfr list form opens.

9 Choose a profile from the list and click on the OK button. The Select MCFR Ingress Qos Profile - MultiClass Mlfr list form closes and the Multilink Bundle (Edit) form is refreshed with the MCFR Ingress QoS Profile information.

10 Click on the Select button beside the MCFR Egress Qos Profile parameter. The Select MCFR Egress Qos Profile - MultiClass Mlfr list form opens.

11 Choose a profile from the list and click on the OK button. The Select MCFR Egress Qos Profile - MultiClass Mlfr list form closes and the Multilink Bundle (Edit) form is refreshed with the MCFR Egress QoS Profile information.

12 Click on the States tab.

13 Configure the Administrative State parameter, if required.

14 To add members to the FR group bundle, perform the following steps.

i Click on the Bundle Members tab button.

ii Click on the Add button to add DS0 channel groups to the bundle. The Add Bundle Member series of configuration steps appears.

iii Perform step 8 b of Procedure 17-99.

Note — You can also add bundle members to the FR group bundle using the contextual menu in the navigation tree.

15 Click on the L2 Access Interfaces and L3 Access Interfaces tab buttons to view the interfaces that the bundle is assigned to.

16 Click on the Service Access Points tab button to view SAP information.

17 Click on the Statistics tab button to view statistical information.

18 Click on the Faults tab button to view information about alarms.

19 Configure the FR interface, if required. Perform the following steps:

i Click on the Edit FR button. The FR Interface form opens with the General tab displayed.

ii Configure the parameters:

- LMI Type
- LMI Mode
- Error Threshold
- Monitored Events
- Polling Interval
- Full Inquiry Interval

20 Click on the OK button. The FR Interface form closes.

21 Click on the Close button. The Multilink Bundle (Edit) form closes.

Procedure 17-104 To configure an MLPPP bundle as a network interface on a channelized ASAP MDA

1 Perform Procedure 17-98 to create a MLPPP bundle on a channelized ASAP MDA.

Note — Consider the following when configuring an MLPPP as a network interface.

- LFI is not supported on MLPPP network interfaces.
- MC MLPPP is not supported on MLPPP network interfaces.
- IPv6 network interfaces are not supported.
- Up to 8 network interface members can be added to a bundle.

2 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

3 Locate and expand the Bundles object in the Equipment view.

4 Right-click on the bundle created in step 1. The Multilink Bundle (Edit) form opens with the General tab displayed.

5 Click on the Bundle Members tab button.

6 a bundle member and click on the Properties button. The Bundle Member (Edit) form opens.

7 Click on the Port tab button.

8 Click on the Properties button beside the port name. The DS0 Channel Group (Edit) form opens with the General tab displayed.

9 Set the Mode parameter to Network.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The DS0 Channel Group (Edit) form closes.

12 Close the Bundle Member (Edit) form.

13 The Multilink Bundle (Edit) form refreshes with new tabs.

14 Click on the Network Interfaces tab button.

15 Click on the Add button. The Create Network Interface - Routing Instance form opens.

16 Perform steps 4 to 42 of Procedure 27-4 to create a network interface on the DS0 channel.

The port in step 6 of Procedure 27-4 is set to the DS0 channel by default. Go to step 11 of Procedure 27-4.

17 The L3 interface appears on the Network Interfaces tab. Close the Multilink Bundle (Edit) form.

18 — NE user and device security

18.1 NE user and device security overview

The 5620 SAM provides security support for accessing managed devices, such as the 7750 SR, as follows:

- create and manage users, profiles and passwords for access to NEs
- configure RADIUS or TACACS+ authentication to control access to the managed devices using 5620 SAM user accounts
- configure device system security through traffic filtering and blocking

RADIUS is an access server AAA protocol. The protocol provides a standardized method of exchanging information between a RADIUS client, which is located on the 7750 SR and managed by the 5620 SAM, and a RADIUS server, which is located externally from the 7750 SR and the 5620 SAM.

RADIUS functionality provides an extra layer of login security. The RADIUS client relays user account information to the RADIUS server. The server authenticates the user and returns user privilege information to the RADIUS client. This determines the level of access that the user has to the device. For example, the user may not be able to FTP information to or from the device.

TACACS+ provides functionality that is similar to RADIUS.

Note — The 5620 SAM server checks for reachability to the TACACS+ server using UDP port 49 to prevent long timeout issues. However, all subsequent communication is over TCP port 49.

User and group permissions on managed devices

The following general rules apply to managed device users, such as 7750 SR users and groups:

- The authentication settings on the device override any configured and distributed authentication settings on the 5620 SAM. For example, if you configure a user account with SHA authentication, and distribute the account to a device configured to use MD5 authentication, authentication is changed to MD5 for that account.
- The management access and CPM filters applied to the managed device must be manually distributed.
- The system administrator can limit the type of access per managed device, for example, allowing FTP access, but denying console, Telnet, and SNMP access.

- User profiles exist independently of users, and are not in effect until they are linked to a user.
- Create device user accounts as a backup to RADIUS or TACACS+ authentication. If the RADIUS or TACACS+ server fails, or there are user issues on the servers, the 7750 SR user account can be used to access the managed device.

Caution — The 5620 SAM cannot obtain a secret value from an NE during resynchronization. Alcatel-Lucent recommends that you use only the 5620 SAM to configure a shared authentication secret. Do not configure a shared authentication secret directly on a managed NE using another interface, for example, a CLI, or the 5620 SAM cannot synchronize the security policy with the NE.

User and user accounts when combined local and remote authentication is used

Many organizations already have existing TACACS+ or RADIUS authentication of users, based on long standing TACACS+ and RADIUS user accounts and passwords. You can incorporate new 5620 SAM client GUI user accounts for local authentication on the 5620 SAM server with existing TACACS+ or RADIUS system and users.

Consider the following:

- system administrators can use existing TACACS+ or RADIUS user accounts
- you can create 5620 SAM client user accounts that match the exact TACACS+ or RADIUS user account, for example, if the RADIUS user account is jane, you can create a 5620 SAM user jane
- the 5620 SAM user name can be 1 to 80 characters, flexible enough to match most remote authentication user accounts
- 5620 SAM users already authenticated remotely can log in to 5620 SAM using their RADIUS or TACACS+ passwords
- for 5620 SAM users to be authenticated locally, their account passwords must meet 5620 SAM password requirements, described in this section

For example, for user Jane:

- RADIUS user name is jane and password is accessforjane
- 5620 SAM user name is jane and password is LetJane1In!

When Jane is authenticated by RADIUS, she can log in to the 5620 SAM client by typing in jane and accessforjane. If the RADIUS server was down, and she could not be authenticated remotely, to be authenticated locally Jane must log in to the 5620 SAM client by typing jane and LetJane1In!

RADIUS and TACACS+ policies and permissions

See the appropriate RADIUS and TACACS+ documentation for information about installing, configuring, maintaining lists of users, and managing these authentication servers.

For TACACS+ users, you can specify the following in a user template that is read by the global TACACS+ policy:

- The type of permitted NE access, for example, console, FTP, or both
- A home directory
- A login script that runs when the user logs in

You can enable or disable the user template as required to suit your current global policy requirements.

CPM filters and traffic management

Device CPMs provide dedicated traffic management and queuing hardware for protecting the control plane. You can use CPM filters to specify which types of traffic to accept or deny, and to allocate and rate-limit the shaping queues for traffic directed to the CPMs.

Note 1 — The 7705 SAR does not support IPv6 CPM IP filters, queue filters, or MAC CPM IP filters.

Note 2 — There is no partial distribution of CPM IP filter policies to the 7705 SAR. When you distribute a CPM IP Filter policy to a specific 7705 SAR, every entry, property, and value within that policy must be supported by that 7705 SAR, or distribution of that policy is blocked to that 7705 SAR.

The 5620 SAM supports the following CPM traffic management functionality:

- traffic classification using CPM filters
  - Packets going to the CPM are first classified by the IOM into forwarding classes before recognition by the CPM hardware. You can use CPM filters to further classify the packets using L3/L4 information, for example, destination IP, DSCP value, and TCP SYN/ACK.
- queue allocation
  - Queues 1 — 8 are the default queues. They cannot be modified or deleted. Unclassified traffic is directed to the default queues.
  - Queues 9 — 32 are reserved for future use.
  - Queues 33 — 2000 are available for allocation.
  - Queues 2001 — 8000 are used for per-peer queuing.
- queue configuration
  - PIR
  - CIR
  - CBS
  - MBS

DoS protection

The 7750 SR-7, 7750 SR-12, 7450 ESS-7, and 7450 ESS-12 support the use of DoS protection on network and access interfaces. To protect NEs from the high incoming packet rates that characterize DoS attacks, you can use the 5620 SAM to configure DoS protection for the following scenarios:

- the arrival of unprovisioned link-layer protocol packets that are received from CE devices in the core network
- the arrival of excessive subscriber control-plane packets on L2 or L3 access interfaces in aggregation networks
- the arrival of excessive Ethernet CFM frames on L2 and L3 access interfaces, SAPs, and SDP bindings, based on a combination of CFM OpCode and MEG-level values

DoS protection limits the number of packets that are received each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

DoS protection in the core network

DoS protection in the core network limits the number of link-layer protocol packets that each network interface on an NE accepts for protocols that are not enabled on the interface. The interface drops the excessive packets before they are queued or processed by the CPU.

You can configure global DoS protection on an NE using the NE System Security form. DoS protection controls the following for unprovisioned link-layer protocols:

- the packet arrival rate per source on each network interface
- the overall packet arrival rate per source on the NE
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically applies default DoS protection parameters to each network and access interface. These defaults limit only the overall packet arrival rate and apply to all of the interfaces on the NE.

DoS protection policies in aggregation networks

In a subscriber aggregation network, an NE typically receives few control-plane packets from a specific subscriber. If one or more subscribers generate excessive control-plane traffic, DoS protection policies can help to ensure that NEs do not become overburdened by these unwanted packets.

You can configure DoS protection policies to control the following on network interfaces, VPLS L2 access interfaces, and IES and VPRN L3 access interfaces:

- the control-plane packet arrival rate per subscriber host
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically assigns a default DoS protection policy to each network and access interface. This default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified.

See Procedure 18-3 for information about creating or modifying a DoS protection policy and assigning the policy to one or more NEs. See the appropriate service chapter for information about applying DoS protection policies to interfaces.

IP security

The 5620 SAM supports the IPsec MDA which provides IP security support including tunneling and encryption functions. See the 7750 SR IP security node documentation for more information about configuring IP security.

18.2 Workflow to manage NE user and device security

Note — 5620 SAM security management support for the OmniSwitch is limited to the configuration of RADIUS and TACACS+ access policies for user authentication.

1. Specify the type of authentication keys used on the device; for example, SHA or MD5. See chapter 13 for more information.
2. Specify the types of access to be granted to each device from the 5620 SAM.
3. Create filter policies for device CPM modules.
4. Create site user profiles based on job classifications and the access needed to the managed devices.
5. Create individual site user accounts based on the configured profiles.
6. Specify password policies for access to managed devices and for users.
7. Manage the user profiles and users:
   - modify profiles and users
   - delete profiles and users
   - change passwords as specified in the password policy
8. Create RADIUS or TACACS+ policies for user authentication.
9. Configure NE system security parameters such as the following:
   - peer queuing for hardware CPM queues
   - enabling or disabling FTP, Telnet, or SSH servers on managed devices
   - RADIUS and TACACS+ user templates
   - global NE DoS protection parameters
10. Create subscriber authentication policies for DHCP sessions, as required.

11 Release and distribute the policies to the managed devices.

Note 1 — Before you distribute policies to managed devices, ensure the management access filter Action parameter is not set to deny. Shut down the filter, distribute the policies, and then turn the filter back up.

Note 2 — If the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed. You must first release the policy for distribution.

When you change the configuration mode of a management access filter or CPM IP filter to released, the policy is not distributed to existing local definitions. When all other policies are changed to released, the policy is distributed to existing local definitions

12 Delete policies, as required.

18.3 NE user and device security procedures

This section provides procedures to create and manage security on the managed devices.

Procedure 18-1 To create or modify a site management access filter policy for a managed device

A site management access filter performs the following functions:

- Restricts the type of management access allowed
- Specifies a strict underlying connection protocol usage and the accepted IP addresses and ports that can gain access to the device

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE Management Access Filters from the 5620 SAM main menu. The NE Management Access Filter form opens.

2 Perform one of the following:

a Specify a filter to search for and edit and existing site management access filter. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Site Management Access Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

4 Configure the following parameters on the IPv4, IPv6, and MAC panels, as required:

- Default Filter Action
- Administrative Status

5 Click on the IPv4 Entries tab button.

6 Perform one of the following.

a Click on the Add button to add a new site entry. The Site MAF Match Entry (Create) form opens.

b Select an entry in the list and click on the Properties button to modify an existing entry. The Site MAF Match Entry (Edit) form opens.

7 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Action
- Source IP
- Source IP Mask
- Source Port Type
- Source Port ID
- Destination Port
- Destination Port Mask
- Protocol

When you set the Action parameter to deny, you cannot distribute the policy to the managed device. Before setting the parameter to deny, set the parameter to permit, distribute the configuration to the managed devices, then reconfigure the parameter to deny.

8 Click on the OK button. The Site MAF Match Entry (Create) or Site MAF Match Entry (Edit) form closes.

9 Click on the IPv6 Entries tab button.

10 Perform one of the following.

a Click on the Add button to add a new site entry. The Site IPv6 MAF Match Entry (Create) form opens.

b Select an entry in the list and click on the Properties button to modify an existing entry. The Site IPv6 MAF Match Entry (Edit) form opens.

11 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Action
- Source IP
- Source IP Mask
- Source Port Type
- Source Port ID
- Destination Port
- Destination Port Mask
- Next Header
- Flow Label

When you set the Action parameter to deny, you cannot distribute the policy to the managed device. Before setting the parameter to deny, set the parameter to permit, distribute the configuration to the managed devices, then reconfigure the parameter to deny.

12 Click on the OK button. The Site IPv6 MAF Match Entry (Create) or Site IPv6 MAF Match Entry (Edit) form closes.

13 Click on the MAC Entries tab button.

Note — MAC MAF functionality is supported on the 7750 SR, 7450 ESS, and 7710 SR Release 6.1 R4 or later.

14 Click on the Add button. The Site MAC MAF Match Entry (Create) form opens with the General tab displayed.

15 Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description

16 Click on the Filter Properties tab button.

17 Configure the parameters:

- Action
- Frame Type
- Source MAC
- Destination MAC
- Src Mask
- Dst Mask
- Dot1p
- Dot1p Mask
- CFM Opcode
- CFM Val 1
- CFM Val 2
- Service Id

18 Perform one of the following.

a If you set the Frame Type parameter to e802dot2LLC in step 17, configure the following parameters. Otherwise, go to step 19.

- DSAP
- DSAP Mask
- SSAP
- SSAP Mask

b If you set the Frame Type parameter to e802dot2SNAP in step 17, configure the following parameters. Otherwise, go to step 19.

- SNAP OUI
- SNAP PID

c If you set the Frame Type parameter to Ethernet II in step 17, configure the Ether Type parameter. Otherwise, go to step 19.

19 Click on the OK button to save the configuration and close the CFM MAC Filter Entry (Create) or CFM MAC Filter Entry (Edit) form.

20 Click on the OK button. A confirmation window appears.

21 Confirm the action.

22 Repeat for each site management access filter you want to create or modify.

Note — If the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed. You must first release the policy for distribution. When you switch the configuration mode to released, the policy is not distributed to existing local definitions. See Procedure 18-14 for more information about how to release a policy.

You must distribute policies to specific devices, as described in Procedure 18-14.

Procedure 18-2 To create or modify a CPM filter policy for a managed device

A device CPM module provides traffic management and queuing hardware for protecting the control plane. The device provides dedicated 10 Gb/s hardware protection for the control planes. You can create CPM filters for the following traffic management functions:

- Drop traffic
- Accept traffic
- Allocate dedicated hardware shaping queues for traffic directed to the control processors

Note 1 — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

Note 2 — The 7705 SAR does not support IPv6 CPM filters, Queue filters, or MAC CPM filters.

1 Choose Administration→Security→NE CPM Filter from the 5620 SAM main menu. The NE CPM Filter form opens.

2 Perform one of the following steps.

a Specify a filter to search for and edit and existing site management access filter. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The CPM Filter (Create) form opens.

3 Click on the General tab button.

4 Configure the parameters as required.

- Displayed Name
- Description
- Default Filter Action
- Administrative State
- IPv6 Administrative Status

Note — The 7705 SAR does not support IPv6 and MAC CPM filters.

5 Click on the IPv4 Entries tab button.

6 Perform one of the following steps.

a Click on the Add button to add a new filter entry.

b Click on an entry in the list and click on the Properties button to modify an existing entry.

The CPM IP Filter Entry (Create) form opens with the General tab displayed.

7 Configure the parameters.

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description

8 Click on the Filter Properties tab button.

9 Configure the parameters:

- Action
- Protocol
- Queue ID
- DSCP
- Source IP
- Source Mask
- Destination IP
- Destination Mask
- Destination Port
- Routing Instance
- Fragment
- IP Option
- IP Option Mask
- Option Present
- Multiple Option
- ICMP Code
- ICMP Type
- Source Port
- TCP Ack
- TCP Syn

The Queue ID parameter is configurable when the Action parameter is set to queue.

10 Click on the OK button. The new CPM IP filter entry appears in the list.

11 Click on the IPv6 Entries tab button.

12 Perform one of the following steps.

a Click on the Add button to add a new filter entry.

b Select an entry in the list and click on the Properties button to modify an existing entry.

The CPM IPv6 Filter Entry (Create) form opens with the General tab displayed.

13 Configure the parameters.

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description

14 Click on the Filter Properties tab button.

15 Configure the parameters:

- Action
- Next Header
- Queue ID
- DSCP
- Source IP
- Source Mask
- Destination IP
- Destination Mask
- Routing Instance
- Flow Label

The Queue ID parameter is configurable when the Action parameter is set to queue.

16 Click on the OK button. The new CPM IPv6 filter entry appears in the list.

17 Click on the MAC Entries tab button.

Note — MAC CPM filters are supported only on the 7750 SR and 7450 ESS, Release 6.1 R4 or later.

18 Perform one of the following steps.

a Click on the Add button to add a new MAC entry. The CPM MAC Filter Entry (Create) form opens with the General tab displayed.

b Select an entry from the list and click on the Properties button to modify an existing CPM MAC entry. The CPM MAC Filter Entry (Edit) form opens with the General tab displayed.

19 Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description

20 Click on the Filter Properties tab button.

21 Configure the parameters:

- Action
- Frame Type
- Source MAC
- Destination MAC
- Src Mask
- Dst Mask
- Dot1p
- Dot1p Mask
- CFM Opcode
- CFM Val 1
- CFM Val 2
- Service Id

22 Perform one of the following.

a If you set the Frame Type parameter to e802dot2LLC in step 21, configure the following parameters. Otherwise, go to step 24.

- DSAP
- DSAP Mask
- SSAP
- SSAP Mask

b If you set the Frame Type parameter to Ethernet II in step 21, configure the Ether Type parameter. Otherwise, go to step 24.

23 Click on the OK button to save the configuration and close the CFM MAC Filter Entry (Create) or CFM MAC Filter Entry (Edit) form.

24 Click on the Queues tab button.

25 Perform one of the following steps.

a Click on the Add button to add a new CPM filter queue. The CPM Filter Queue (Create) form opens with the General tab displayed.

b Click on an entry in the list and click on the Properties button to modify an existing CPM filter queue.

26 Configure the parameters.

- ID
- Displayed Name
- Description

27 Click on the CIR/PIR tab button.

28 Configure the parameters.

- CIR (kb/s)
- PIR (kb/s)
- MAX

Ensure that the CIR value is lower than the PIR value.

29 Click on the Burst Size tab button.

30 Configure the parameters.

- Committed Burst Size (KB)
- Maximum Burst Size (KB)

The parameters are configurable when the Default check box above each is deselected.

Ensure that the Committed Burst Size (KB) parameter value is lower than the Maximum Burst Size (KB) parameter value.

31 Click on the OK button. A dialog box appears.

32 Click on the OK button. The CPM IP Filter (Create) form reappears.

33 Repeat for each CPM filter that you want to create or modify.

34 Click on the Apply button to save the changes.

You must distribute policies to specific devices, as described in Procedure 18-14.

Procedure 18-3 To create or modify an NE DoS protection policy

Perform this procedure to control the amount of subscriber-based control-plane traffic that NE interfaces receive.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE DoS Protection from the 5620 SAM main menu. The NE DoS Protection form opens.

2 Perform one of the following.

a Create a policy.

i Click on the Create button. The NE DoS Protection (Create) form opens.

ii Configure the following parameters:

- Auto-Assign ID
- Policy ID

iii Click on the Apply button. The form displays additional buttons and the form name changes to NE DoS Protection (Edit).

b Modify an existing policy.

i Configure the filter criteria. A list of DoS protection policies is displayed.

ii Select a policy in the list and click on the Properties button. The NE DoS Protection (Edit) form opens.

3 Configure the following parameters:

- Description
- Packet Rate Limit (pps)
- Overall Rate Limit (pps)
- Out Profile Rate (pps)
- Receive Notification

4 Perform the following steps to configure CFM frame-rate limiting, if required.

i Click on the CFM Rate Limiting tab button.

ii Click on the Add button. The CfmRateLimiting (Create) form opens.

iii Configure the parameters:

- Policy ID
- Description
- Packet Rate Limit (pps)
- Level Set

iv Click on the Add button in the Op Code Set panel. The Select Property form opens.

Note — You must specify at least one OpCode value.

v Select one or more OpCodes in the list and click on the OK button. The OpCode entries are listed on the CfmRateLimiting (Create) form.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The CfmRateLimiting (Create) form closes.

5 Distribute the policy to NEs, as required, as described in Procedure 18-14.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The NE DoS Protection (Edit) form closes.

Procedure 18-4 To view NE DoS protection violations

1 Choose Administration→Security→NE System Security from the 5620 SAM main menu. The Select Site form opens.

2 Select a managed device in the list and click on the OK button. The NE System Security (Edit) form opens with the General tab displayed.

3 Click on the NE DoS Protection tab button.

4 Perform one of the following to view a specific violation type.

a Click on the Per Source Violations tab button to view a list of the violations that are associated with subscriber hosts.

b Click on the Link Specific Port Violations tab button to view a list of the violations at the port level. The following kinds of violations are listed:

- violations that exceed the Link Rate Limit (pps) parameter value specified for the NE
- violations that exceed the Port Overall Rate Limit (pps) parameter value specified for the NE.

c Click on the Network Interface Violations tab button to view a list of the violations for network interfaces that exceed the Overall Rate Limit (pps) parameter value specified in an associated NE DoS protection policy.

d Click on the SAP Interface Violations tab button to view a list of the violations for SAPs that exceed the Overall Rate Limit (pps) parameter value specified in an associated NE DoS protection policy.

5 Repeat step 4 as required to view another violation type.

6 Close the NE System Security (Edit) form.

Procedure 18-5 To create a user profile for managed device access

A site user profile specifies the commands or command groups that are permitted or denied on the managed device by the 5620 SAM.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE User Profiles from the 5620 SAM main menu. The NE User Profiles form opens.

2 Click on the Create button. The Site User Profile (Create) form opens.

3 From the General tab, configure the parameters.

- Displayed Name
- Description
- Default Profile Action
- LI Profile

Note — To configure the LI Profile parameter you must have LI privileges. For more information about LI, see chapter 31.

4 Click on the Apply button.

5 Click on the Entries tab button.

6 Click on:

a The Add button to add a new site entry.

b An entry in the table and click on the Properties button to modify an existing entry.

The Site User Profile Match Entry (Create) form opens when you create a new entry.

7 Configure the parameters.

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Action
- Match String

Specify the Match String parameter. A match string is a CLI command prefix, which defines the scope of the user profile. For example, when you set the match string to “config” and specify a deny action, this user profile cannot use any CLI commands that begin with the word “config”.

8 Click on the Apply button to save the changes. The site user profile match entry appears in the list form.

9 Verify the action.

10 Click on the OK button to close the form.

11 Repeat for each required site user profile.

You must distribute policies to specific devices, as described in Procedure 18-14.

Procedure 18-6 To configure a user account for access to a managed device

Perform this procedure to create a user account on a device for managed device access when the authentication servers are unavailable, or to specify the allowed types of device access, for example, Telnet, SNMPv3, FTP, or console.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens.

2 Click on the Create button. The Site User (Create) form opens with the General tab displayed.

3 Configure the parameters.

- User Name
- Additional ID
- Description
- Access
- Password
- Confirm Password
- Home Directory
- Restrict to Home
- Console Login Exec File
- Console Cannot Change Password
- Console New Password At Login

Note — For SNMP v2 managed NEs, you can create and update an SNMP user configuration policy when SNMP is not enabled for the Access parameter.

4 When a user has console permission, you can configure the parameters in the Console Profiles tab.

i Click on the Console Profiles tab button. The list of profiles numbered one through eight appears.

Each user can have up to eight profiles.

ii Click on the Select button beside Profile 1 and Profile 2 to 8 parameters. Profile 1 is automatically configured to use the system-generated default profile.

The Select Site User Profile form opens. Default profiles and the profiles created in Procedure 18-5 are listed.

iii Choose a profile from the list.

iv Click on the OK button. The profile name appears beside the profile number.

5 When a user has SNMPv3 permissions, you can configure the authentication parameters. Ensure that the SNMPv3 user and user group has been created on the managed device. If MD5 or SHA authentication and DES privacy is used, ensure the keys have been created and associated with the managed device and the SNMPv3 user group, as described in Procedure 13-1.

i Click on the SNMP v3 tab button.

ii Configure the parameters.

- Authentication Protocol
- Privacy Protocol
- New Authentication Password
- Confirm New Auth Password
- New Privacy Password
- Confirm New Privacy Password

iii Click on the OK button to save the changes.

iv Verify the action.

6 Click on the Apply button to save the changes.

7 Close the form.

You must distribute policies to specific devices, as described in Procedure 18-14.

Procedure 18-7 To create or modify a password policy

Perform this procedure to create a policy that specifies the rules to which a password must conform on one or more devices.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE Password Policy from the 5620 SAM main menu. The NE Password Policy form opens.

2 Click on the Create button. The Site Password Policy (Create) form opens.

3 Configure the parameters.

- ID
- Auto-Assign ID
- Name
- Description
- Complexity
- Lockout Time (minutes)
- Password Never Expires
- Maximum Attempts
- Maximum Attempts Time (minutes)
- Days Before Expiration
- Minimum Length
- Health Check
- Health Check Interval
- Authentication Order 1
- Exit On Reject
- Admin Password

If the password can expire, specify the expiration parameter to indicate the number of days that the password can be active before the old password expires and a new password must be set.

Use the Maximum Attempts and Maximum Attempts Time (minutes) parameters to specify the number of attempts allowed within a specified time.

If the maximum number of password attempts in the specified time is exceeded, set how long the account is locked out using the Lockout Time (minutes) parameter.

4 Specify the types and order of password authentication to be used to verify the user account password using the Authentication Order 1 through 3 parameters. Set the order from the most preferred method of authentication to the least preferred method of authentication.

5 Click on the OK button to save the changes.

You must distribute policies to specific devices, as described in Procedure 18-14.

Procedure 18-8 To create an NE RADIUS access policy

See the appropriate RADIUS documentation for more information about configuring RADIUS servers.

1 Choose Administration→Security→NE RADIUS Authentication from the 5620 SAM main menu. The NE RADIUS Authentication form opens.

2 Click on the Create button. The Site RADIUS Policy (Create) form opens.

3 Configure the parameters.

- Displayed Name
- Description
- Administrative State
- Enable Accounting
- Enable Authorization
- RADIUS Authorization Algorithm
- Retry Attempts
- Timeout (seconds)
- Authentication Port
- Source Address
- Accounting Port
- Enable User Template

Note — The Source Address parameter on the Site RADIUS Policy (Create) form is configurable but is not used. You must use the Source Address tab of the routing instance properties form for the device to specify the source address of the RADIUS server.

4 Click on the Servers tab button to configure a connection to the RADIUS servers. You can configure up to five RADIUS servers.

i Click on the Add button. The Site RADIUS Server (Create) form opens.

ii Configure the parameters.

- ID
- Displayed Name
- Description
- Address
- Secret

iii Click on the OK button to save the changes.

5 Click on the Apply button to save the changes.

You must distribute policies to specific devices, as described in Procedure 18-14.

Ensure that the authentication order uses RADIUS first. See Procedure 18-7 for more information.

Procedure 18-9 To create an NE TACACS+ access policy

See the appropriate TACACS+ documentation for more information about configuring TACACS+ servers.

See section 8.4 for a sample configuration.

1 Choose Administration→Security→NE TACACS+ Authentication from the 5620 SAM main menu. The NE TACACS+ Authentication form opens.

2 Click on the Create button. The Site TACACS+ Policy (Create) form opens with the General tab displayed.

3 Configure the parameters.

- Displayed Name
- Description
- Administrative State
- Enable Accounting
- Accounting Type
- Enable Authorization
- Timeout (seconds)
- Single Connection
- Source Address
- Enable User Template

Note — The Source Address parameter on the Site TACACS+ Policy (Create) form is configurable but is not used. You must use the Source Address tab of the routing instance properties form for the device to specify the source address of the TACACS+ server.

4 Click on the Servers tab button to configure a connection to the TACACS+ servers. You can configure up to 5 TACACS+ servers.

i Click on the Add button.

The Site TACACS+ Server (Create) form opens.

ii Configure the parameters.

- ID
- Displayed Name
- Description
- Address
- Secret Name

iii Click on the OK button to save the changes.

5 Click on the Apply button to save the changes.

You must distribute policies to specific devices, as described in Procedure 18-14.

Procedure 18-10 To configure NE system security

1 Choose Administration→Security→NE System Security from the 5620 SAM main menu. The Select Site form opens.

2 Select a managed device in the list and click on the OK button. The NE System Security (Edit) form opens with the General tab displayed.

3 Click on the Servers Configuration tab button to configure the type of servers that you want to configure on the managed device, for example, FTP servers.

4 Configure the parameters:

- Servers Enabled
- SSH

Note — The 7705 SAR may become temporarily unreachable when enabling SSH and starting the SSH server on the device.

5 Click on the CPM-Per-Peer-Queuing tab button to ensure that the managed device allocates a separate CPM hardware queue for the peer, for example, a BGP or T-LDP peer.

6 Configure the CPM-Per-Peer-Queueing parameter.

7 Click on the System User Template tab button. The default template is displayed.

8 Select the default template and click on the Properties button. The System User Template (Edit) form opens.

9 Configure the parameters.

- Access
- Home Directory
- Restricted to Home Directory
- Console Login Exec File

10 Click on the OK button. The System User Template (Edit) form closes.

11 Click on the NE DoS Protection tab button to configure global DoS functionality for the NE.

12 Configure the parameters:

- Link Rate Limit (pps)
- Port Overall Rate Limit (pps)
- Protection Administrative State

13 Click on the Faults tab button to view alarm information, as required.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The NE System Security (Edit) form closes.

You must distribute policies to specific devices, as described in Procedure 18-14.

Procedure 18-11 To create an OmniSwitch RADIUS or TACACS+ security policy

See the appropriate RADIUS or TACACS+ documentation for information about configuring RADIUS and TACACS+ servers.

1 Choose Administration→Security→NE AOS Security Authentication from the 5620 SAM main menu. The NE AOS Security Authentication form opens.

2 Click on the Create button. The Site AOS Security Policy (Create) form opens with the General tab displayed.

3 Configure the parameters.

- Displayed Name
- Description
- Protocol Name

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Perform one of the following:

a If you set the Protocol Name parameter to RADIUS in step 3, go to step 5.

b If you set the Protocol Name parameter to TACACS+ in step 3, go to step 8.

5 Configure the parameters.

- Ip Address
- Ip Address 2
- Time Out
- Retries
- Secret
- Authentication Port
- Account Port

6 Click on the Apply button to save the changes.

7 To configure multiple RADIUS servers, repeat steps 3 to 4 to add more RADIUS servers; otherwise go to step 11.

8 Configure the parameters:

- Ip Address
- Ip Address 2
- Time Out
- Secret
- Port

9 Click on the Apply button to save the changes.

10 To configure multiple TACACS+ servers, repeat steps 3 to 4 to add more TACACS+ servers; otherwise go to step 11.

11 Close the Site AOS Security Policy (Create) form.

You must distribute the security policies to specific devices, as described in Procedure 18-14.

Ensure that the authentication order uses RADIUS first. See Procedure 18-7 for more information.

Procedure 18-12 To create a subscriber authentication policy

The 5620 SAM provides security support for creating DHCP sessions on the 7450 ESS, 7750 SR, and 7710 SR. The 5620 SAM allows you to create a policy that uses RADIUS authentication to grant network access to a dynamic host. You can apply the policy to a VPLS or IES SAP, or to a VPRN or IES group interface. Authentication is not performed for statically provisioned hosts.

Perform this procedure to create a DHCP-based subscriber authentication policy that defines the parameters for dynamically created subscriber host sessions and authenticates the sessions. The 5620 SAM supports up to 32 subscriber authentication policies.

See chapter 68 for information about configuring a VPLS and chapter 70 for information about configuring an IES.

1 From the 5620 SAM main menu, choose Administration→Security→Subscriber Authentication Policy Manager. The Subscriber Authentication Policy Manager form opens.

2 Click on the Create button. The Subscriber Authentication Policy (Create) form opens with the General tab displayed.

3 Configure the parameters.

- Displayed Name
- Description
- Retry Attempts
- Timeout (seconds)
- Re-Authenticate when DHCP lease expired
- Accept CoA
- Access Algorithm
- RADIUS Attributes
- Source Address
- PPPoE Access Method
- Authentication Hold Down Time
- User Name Format
- Append To User Name
- Password
- Calling Station ID Type
- Port Type
- Port Type Value
- Port Prefix Type
- Port Prefix String
- Port Suffix Type
- Fallback Action

Note — The Calling Station ID Type parameter is configurable when the Calling Station ID option is enabled for the RADIUS Attributes parameter.

The Port Type parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter.

The Port Type Value parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter, and the Port Type parameter is set to Config.

The Port Prefix Type, Port Prefix String, and Port Suffix Type parameters are configurable when the NAS Port ID option is enabled for the RADIUS Attributes parameter.

4 Configure the Router Instance parameter. If you set the parameter value to VPRN, go to step 5. Otherwise, go to step 7.

Note — The Router Instance parameter is configurable for the 7710 SR, 7750 SR, and the 7450 ESS, Release 6.0 or later.

5 Configure a VPRN service as a virtual router instance for the subscriber authentication policy. Perform the following steps.

i Click on the Select button in the VPRN ID panel. The Select VPRN ID - Subscriber Authentication Policy list form opens.

ii Select a VPRN site from the list and click on the OK button. The Select VPRN ID - Subscriber Authentication Policy list form closes and the Subscriber Authentication Policy (Create) form refreshes with the VPRN service information.

Note — You must select a VPRN site before you add RADIUS servers in step 7.

6 If you want to configure PAP/CHAP user name re-writing, configure the following parameters:

- User Name Operation
- Domain Name

7 Click on the RADIUS Servers tab button, if required. Otherwise, go to step 12.

8 Click on the Add button. The RadiusEntry (Create) form opens with the General tab displayed.

9 Configure the parameters.

- ID
- Auto-Assign ID
- Description
- Server IP Address
- Port
- CoA Only
- Secret Name

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The RadiusEntry (Create) form closes and the Subscriber Authentication Policy (Create) form refreshes with the RADIUS server information displayed in a list in the RADIUS Servers tab.

12 Click on the Apply button. The Subscriber Authentication Policy (Create) form refreshes with additional buttons and tabs.

13 Click on the Distribute button to manually distribute the policy to the selected devices.

See Procedure 18-14 for information about distributing security policies. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — If the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed. You must first release the policy for distribution. When you switch the configuration mode to released, the policy is distributed to existing local definitions. See Procedure 18-14 for more information about how to release a policy.

14 Close the Subscriber Authentication Policy (Create) form. The Subscriber Authentication Policy Manager form refreshes with the policy information displayed in a list.

Procedure 18-13 To modify a security policy

1 Choose the appropriate policy from the Administration→Security→*option* 5620 SAM main menu. The appropriate form opens.

2 Set the filter criteria, if applicable. You can filter or local or global policies by using the Policy Scope parameter. When you set the parameter to Local, you can search on a specific managed device by clicking on the Select button beside the Local Node IP Address parameter.

3 Click on the Search button. A policy list opens.

4 Specify whether to modify the global or the local instance of the policy.

   a Local policies have a check mark for the Local column.

   b Global policies do not have a check mark for the Local column.

5 Choose a policy from the list.

6 Click on the Properties button.

7 Configure the policy parameters, as required.

   From either a local or global policy, you can click on the Local Definitions or Global Definitions tab button to view the local instances of policies or the global policy used to define the local instance.

8 Save the changes and close the file. You must distribute global policies to the managed devices. You do not distribute modified local policies.

Procedure 18-14 To distribute a security policy

1 Create policies, as described in Procedures 18-1 to 18-12.

2 Choose the appropriate policy from the Administration→Security→*option* 5620 SAM main menu. The appropriate form opens.

3 Set the filter criteria, if applicable.

4 Click on the Search button. A policy list opens.

5 When:

   a A management access filter is configured to deny access to managed devices, ensure the following:

      i List the applicable management access filters. A list of management access filters opens.

      ii Shut down the management access filter.

      iii Distribute the policies. Complete steps 6 to 14.

   b If no management access filter is configured, go to step 6.

6 Choose a policy from the list.

7 Click on the Properties button if you are distributing a CPM IP, NE DoS protection, or management access filter. The *Policy_Type*, Global (Edit) form opens.

8 When the policy is in draft configuration mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution by performing the following steps. Otherwise, go to step 9.

i Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears.

ii Click on the Yes button. The configuration mode of the policy is changed to Released.

Warning — When you change the configuration mode of a management access filter or CPM IP filter to released, the policy is not distributed to existing local definitions. When all other policies are changed to released, the policy is distributed to existing local definitions.

iii View the local policy, if necessary, by clicking on the Local Definitions tab button and double-clicking on the local policy in the list.

iv Close the local policy form.

9 Click on the Distribute button. The Distribute form opens.

10 Choose a row or rows from the Available Nodes list.

11 Click on the right arrow button. The chosen device or devices move to the Selected Nodes panel on the right side of the form.

12 Click on the Distribute button. CPM IP and management access filters require that you confirm the policy distribution. The policy is distributed to the device or devices.

13 Close the Distribute form. The *Policy_Type*, Global (Edit) form reappears.

14 Configure the distribution mode of the local definitions by performing the following steps.

i Click on the Distribution Mode button. The Distribution Mode - *Policy* form opens.

ii Configure the Distribution Mode parameter. The existing local definitions that are configured with the selected distribution mode are listed.

iii Choose one ore more rows from the Available Nodes list.

iv Click on the right arrow button. The chosen device or devices move to the Selected Nodes panel on the right side of the form.

v Depending on the distribution mode of the chosen device or devices, perform one of the following steps:

- Click on the Sync With Global button.
- Click on the Local Edit Only button.

vi Close the Distribution Mode - *Policy* form. The *Policy_Type*, Global (Edit) form reappears.

15 Turn up the management access filter if you performed step 5 a ii. Otherwise, go to step 16.

16 Close the *Policy_Type*, Global (Edit) form.

17 Close the policy manager form.

Procedure 18-15 To delete a security policy

Note 1 — When you delete site management access filter policies in which the Action parameter is set to deny, ensure that you edit the policy to set the parameter to permit before it is deleted, otherwise, the 5620 SAM may be isolated.

Note 2 — You cannot remove a site management access filter if the filter administrative state is up and the default action of the filter is set to deny or deny host unreachable.

Note 3 — If you attempt to delete an OmniSwitch RADIUS or TACACS+ security policy that has been applied to an authentication service, the 5620 SAM generates a deployment error. You must use the OmniSwitch CLI to delete the policy from the authentication service before you can delete the policy from the 5620 SAM.

1 Choose the appropriate policy from the Administration→Security→*option* 5620 SAM main menu. The appropriate form opens.

2 Set the filter criteria, if applicable.

3 Click on the Search button. A policy list opens.

4 Choose a policy from the list.

5 Click on the Delete button.

6 Click on the Yes button. The policy is deleted.

19 — Inventory management

19.1 Inventory management overview

The 5620 SAM client GUI provides multiple ways of generating inventory data about managed devices and the managed network. You can also use the 5620 SAM-O interface to generate inventory data. See the *5620 SAM-O OSS Interface Developer Guide* for more information.

Use the list, properties, and equipment management forms to generate inventories for:

- required data for SLA audits
- equipment, such as cards, needed for sparing
- installed and in-operation equipment
- vintages, CLEI codes, and identifications

You can generate inventory data based on:

- the entire managed network, which includes all 5620 SAM-managed devices
- a managed device

Figure 19-1 shows how to use the Manage Equipment form to filter and inventory data for all managed devices.

Figure 19-1 Generating inventory data for all managed devices

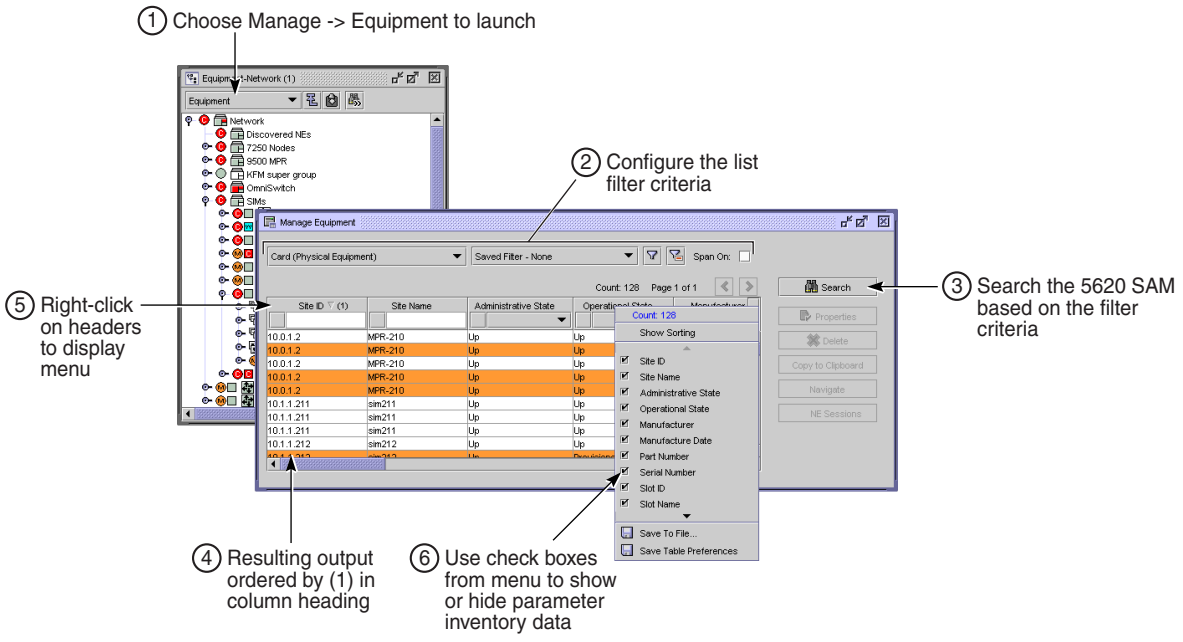
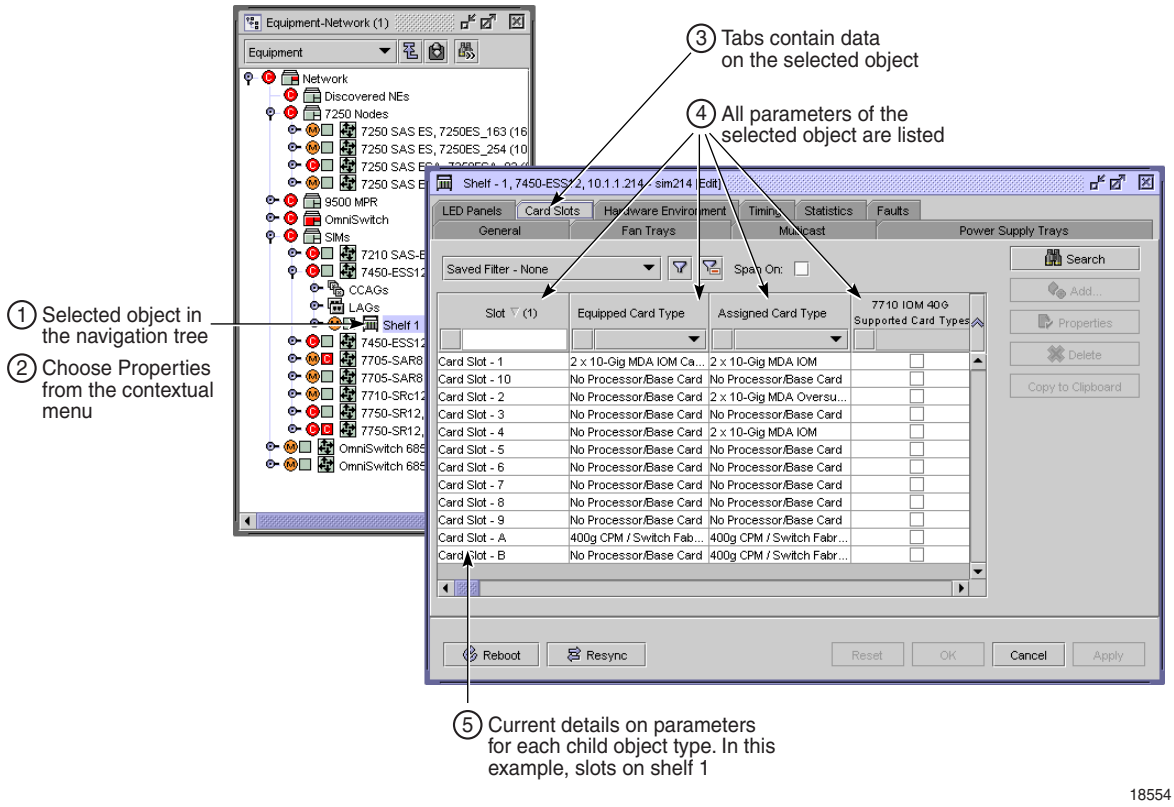


Figure 19-2 shows how to use the properties form for a network object, in this case a shelf on a managed device, to inventory data for the managed device.

Figure 19-2 Generating inventory data for a managed device



Save the data in CSV or HTML format. You can use the saved file for further processing on another platform; for example, as input to a back-office parts management system. Figure 19-3 shows the output of an inventory list saved in CSV format.

Figure 19-3 CSV inventory output

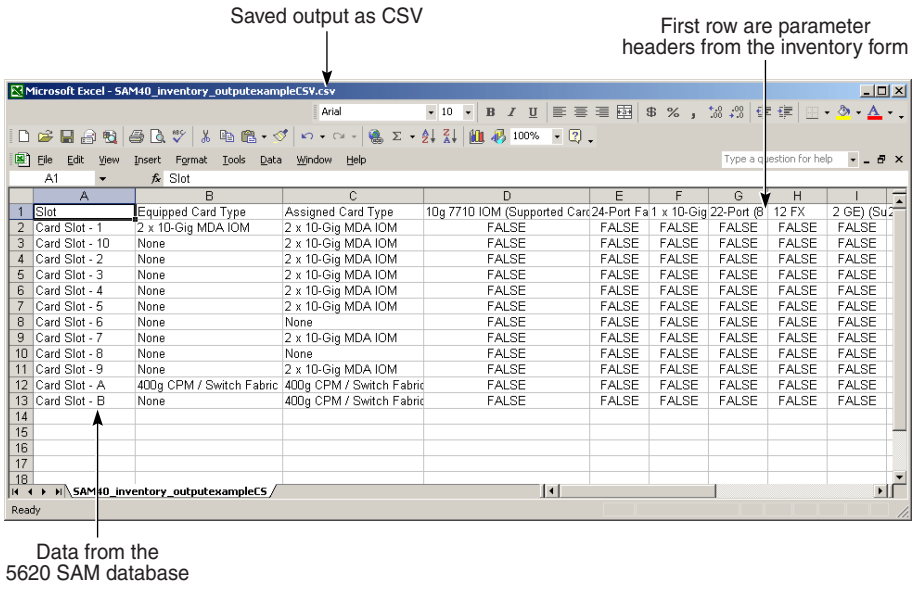
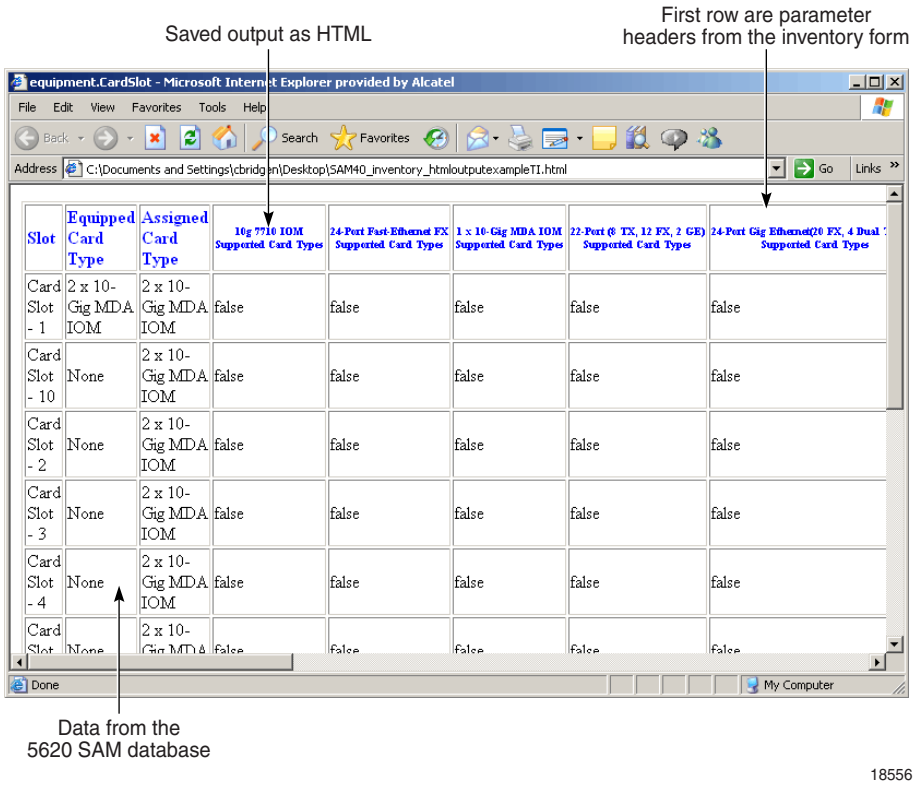


Figure 19-4 shows the output of an inventory list saved in HTML format.

Figure 19-4 HTML inventory output



19.2 Sample inventory management workflow

Figure 19-5 shows a sample inventory management workflow using the client GUI to generate a list of required spare parts, based on business needs.

Figure 19-5 Sample inventory management workflow

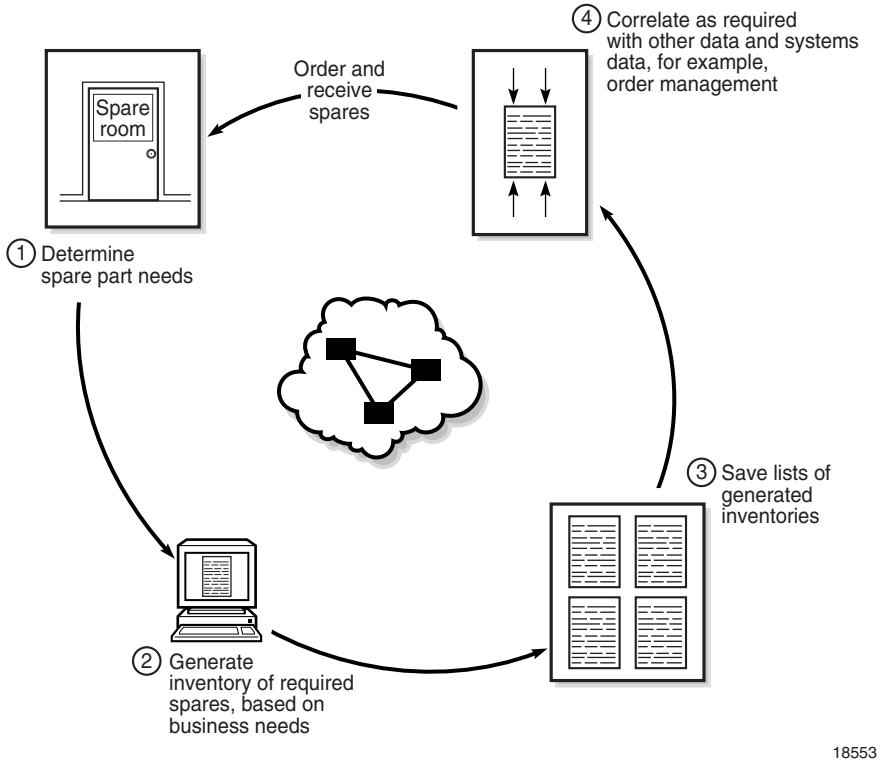


Table 19-1 lists the high-level tasks necessary to configure this sample.

Table 19-1 Sample inventory management workflow

Task	Description
1. Determine spare part needs.	Base spare part needs on business needs and future growth plans.
2. Generate inventories of required spares.	Choose the 5620 SAM client GUI Manage→Equipment→Equipment main menu option to open the Manage Equipment form. Filter the list form to list only those objects that you want; for example, cards of a certain type required for sparing. Generate multiple lists, based on business needs.
3. Save lists of required spares.	Use the 5620 SAM to save the lists in a format compatible with your back-office systems; for example, CSV or HTML. Move the lists to another system, as required by the back-office applications; for example, an order management or data management system.

(1 of 2)

Task	Description
4. Correlate lists with other data, as required.	Use the inventory data to provide inputs to other back-office systems, as required by business needs.

(2 of 2)

19.3 Workflow for inventory management

1 Determine inventory management needs.

2 Provide inventory management list requirements to NOC operators.

3 Generate inventory lists using 5620 SAM client GUI forms, such as list, properties, equipment window, and manage equipment forms.

4 Save inventory lists in the required formats.

5 Move inventory lists to other platforms for post-processing.

19.4 Inventory management procedures

Use the following procedures to perform inventory management tasks.

Procedure 19-1 To list and sort inventory data

1 Inventory can be listed and sorted for a device or for the entire network.

a To list and sort inventory for a device, perform steps 2 to 6.

b To list and sort inventory for the entire network, perform steps 7 to 11.

2 Choose Application→Equipment Window from the 5620 SAM main menu. The Equipment Window Filter form opens.

3 See Procedure 19-1 for more information about using the equipment window filter, or click on the OK button to close the equipment window filter form and access the Equipment Window form.

4 Choose a managed device from the Network Element drop-down menu.

5 Click on the applicable tab button.

6 Go to step 11.

7 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

8 Choose a network object from the object drop-down list.

Note — You can click on the Search button without creating additional filters.

9 Configure the filter criteria.

10 Click on the Search button. The list form displays the results of the inventory search.

11 Sort the results.

- **a** To count the number of items in the list, generate an inventory of data and right-click on the list heading. The Count shows the number of objects in the list.
- **b** To sort in ascending or descending order, click on the column heading. The arrow direction changes to indicate the order in which the data is sorted.
- **c** To move a column, click on the column, drag the column to the right or left, and drop the column in its new location.
- **d** To remove a column, right-click on the column heading and deselect the column in the contextual menu. The column disappears from the display.
- **e** To sort multiple columns, right-click on a column heading and choose Show Sorting from the contextual menu. The Show Sorting form opens. Choose the property or properties from the Available for Sorting panel and click on the right arrow button. The property or properties appear in the Used for Sorting panel. Click on the Sort Ascending or Sort Descending button, as required.

12 Save the inventory output by performing Procedure 19-2 or 19-3.

13 Close the form.

Procedure 19-2 To save inventory output in HTML format

1 Define the filter properties for the inventory search, and list and sort the output as described in Procedure 19-1.

2 Right-click on a column heading of the inventory output and choose Save to File from the contextual menu. The Save form opens.

3 Save the inventory output.

- **i** To choose a directory in which to save the listed information, use the Save In parameter.
- **ii** To create a filename, use the File Name parameter.
- **iii** Choose HTML Only from the Files of Type drop-down menu.
- **iv** Click on the Save button. The results of the inventory search are saved to the specified HTML file.

4 Close the form.

Procedure 19-3 To save inventory output in CSV format

1 Define the filter properties for the inventory search, and list and sort the output as described in Procedure 19-1.

2 Right-click on a column heading of the inventory output and choose Save to File from the contextual menu. The Save form opens.

3 Save the inventory output.

- **i** To choose a directory in which to save the listed information, use the Save In parameter.
- **ii** To create a filename, use the File Name parameter.
- **iii** Choose CSV Only from the Files of Type drop-down menu.
- **iv** Click on the Save button. The results of the inventory search are saved to the specified CSV file.

4 Close the form.

Procedure 19-4 To save a filter

See Procedure 2-36 for more information.

Procedure 19-5 To inventory CLEI codes for managed device objects

1 You can list CLEI codes for fan trays, power supply trays, flash memory, ports, card slots, cards, daughter card slots and daughter cards.

- **a** To view CLEI codes for a device, perform steps 2 to 7.
- **b** To view CLEI codes for the entire network, perform steps 8 to 13.

2 Choose Application→Equipment Window from the 5620 SAM main menu. The Equipment Window Filter and Equipment Window forms open.

3 See Procedure 16-1 for more information about using the Equipment Window filter, or click on the OK button to close the filter form and access the Equipment Window form.

4 Choose a managed device from the Network Element drop-down menu.

5 Click on the applicable tab button.

a Click on the Shelf tab button. Click on the following tab buttons to view information:

- Fan Trays
- Power Supply Trays
- Flash Memory

b Click on the Card Slots tab button. Click on the Inventory tab button to display the cards that are configured in the slots.

c Click on the Cards tab button. Click on the Inventory tab button to display the IOMs that are installed on, pre-provisioned, or provisioned for the node.

d Click on the Daughter Card Slots tab button. Click on the Inventory tab button to display the daughter card slots and daughter cards that are configured in the slots.

e Click on the Ports tab button. Click on the following tab buttons to view information:

- Physical Ports
- SONET Channels
- Link Aggregation Groups
- TDM Channels
- Multilink Bundles
- APS Groups

6 Sort the results to obtain a list of CLEI codes.

Right-click on a column heading and deselect all columns from the contextual menu, except for the object ID or object type and the CLEI code columns. The deselected columns disappear from the display.

7 Go to step 12.

8 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

9 Choose a network object from the object drop-down list.

10 Click on the Search button. The list form displays the results of the inventory search.

11 Sort the results to obtain a list of CLEI codes.

Right-click on the column heading and deselect all columns in the contextual menu, except for the site ID, object ID, and CLEI code columns. The deselected columns disappear from the display.

12 Save the CLEI code inventory output.

a To save the results in HTML format, perform steps 2 and 3 of Procedure 19-2.

b To save the results in CSV format, perform steps 2 and 3 of Procedure 19-3.

13 Close the form.

Procedure 19-6 To inventory card software versions for a managed device

1 Choose Application→Equipment Window from the 5620 SAM main menu. The Equipment Window Filter and Equipment Window forms open.

2 See Procedure 16-1 for more information about using the Equipment Window filter, or click on the OK button to close the filter form and access the Equipment Window form.

3 Choose a managed device from the Network Element drop-down menu.

4 Click on the Cards tab button. The Inventory tab is displayed.

5 Click on the Software tab button. The card software information is displayed for the selected managed device.

6 Right-click on a column heading and deselect all columns from the contextual menu, except for the Slot and Software Version column headings. The deselected columns disappear from the display.

7 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

8 Close the form.

Procedure 19-7 To inventory port types for a managed device

Perform this procedure to generate an inventory of port types, such as physical ports, SONET channels, link aggregation groups, terminations, TDM channels, protocols, multilink bundles, and APS groups.

1 Choose Application→Equipment Window from the 5620 SAM main menu. The Equipment Window Filter and Equipment Window forms open.

2 See Procedure 16-1 for more information about using the Equipment Window filter, or click on the OK button to close the filter form and access the Equipment Window form.

3 Choose a managed device from the Network Element drop-down menu.

4 Click on the Ports tab button. Click on the following tab buttons to view inventory information:

- Physical Ports
- SONET Channels
- Link Aggregation Groups
- TDM Channels
- Multilink Bundles
- APS Groups

5 To sort the inventory output, perform step 11 of Procedure 19-1.

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

7 Close the form.

Procedure 19-8 To inventory shelf data for a managed device

Perform this procedure to generate an inventory of shelf manufacturer information, part numbers, serial numbers, CLEI codes, and CLLI codes for the shelves of a managed device.

1 Choose Application→Equipment Window from the 5620 SAM main menu. The Equipment Window Filter and Equipment Window forms open.

2 See Procedure 16-1 for more information about using the Equipment Window filter, or click on the OK button to close the filter form and access the Equipment Window form.

3 Choose a managed device from the Network Element drop-down menu.

4 Click on the Shelf tab button.

5 Click on the General tab button. The shelf information is displayed.

6 Use screen capture software to record the screen image, or otherwise copy the shelf information to a file for further processing.

Note — You can generate an inventory of shelf data for the managed network, but not for an individual managed devices. See Procedure 19-16 for more information.

7 Close the form.

Procedure 19-9 To inventory all managed cards

You can inventory all managed cards in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Card (equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 Sort the results to obtain a list of card-specific codes. For example:

- Manufactured Date
- Part Number
- Serial Number
- CLEI Code

Right-click on the column heading and deselect all columns in the contextual menu that you do not want to view or save. The deselected columns disappear from the display.

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

7 Close the form.

Procedure 19-10 To inventory all managed fan trays

You can inventory all managed fan trays in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Fan Tray (equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 Sort the results to obtain a list of fan tray-specific codes. For example:

- Operational State
- Administrative State
- Device State
- CLEI Code

Right-click on the column heading and deselect all columns from the contextual menu that you do not want to view or save. The deselected columns disappear from the display.

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

7 Close the form.

Procedure 19-11 To inventory all managed flash memory

You can inventory all managed flash memory in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Flash Memory (equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 Sort the results to obtain a list of flash memory-specific codes. For example:

- Serial Number
- Firmware Revision
- Model Number
- Capacity
- Amount Used
- CLEI code

Right-click on the column heading and deselect all columns from the contextual menu that you do not want to view or save. The deselected columns disappear from the display.

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

7 Close the form.

Procedure 19-12 To inventory all managed physical links

You can inventory all managed physical links in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Physical Link (netw) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 Sort the results to obtain a list of physical link-specific codes. For example:

- Endpoint A Type
- Endpoint A Port
- Endpoint B Type
- Endpoint B Port

Right-click on the column heading and deselect all columns in the contextual menu that you do not want to view or save. The deselected columns disappear from the display.

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

7 Close the form.

Procedure 19-13 To inventory all managed ports

You can inventory all managed ports in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Port (equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 Sort the results to obtain a list of port-specific codes. For example:

- Name
- CLI Name
- MTU (bytes)
- CLEI Code
- State

Right-click on the column heading and deselect all columns in the contextual menu that you do not want to view or save. The deselected columns disappear from the display.

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

7 Close the form.

Procedure 19-14 To inventory all managed power supply trays

You can inventory all managed power supply trays in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Power Supply Tray (equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 Sort the results to obtain a list of power supply tray-specific codes. For example:

- Administrative State
- Operational State
- AC Voltage Status
- DC Voltage Status
- Assigned Type
- CLEI Code

Right-click on the column heading and deselect all columns in the contextual menu that you do not want to view or save. The deselected columns disappear from the display.

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

7 Close the form.

Procedure 19-15 To inventory all managed processors

You can inventory all managed processors in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Processor (equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 Sort the results to obtain a list of processor-specific codes. For example:

- Operational State
- Administrative State
- Device State
- CLEI Code
- Manufacturer
- Manufacture Date
- Part Number
- Serial Number

Right-click on the column heading and deselect all columns in the contextual menu that you do not want to view or save. The deselected columns disappear from the display.

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

7 Close the form.

Procedure 19-16 To inventory all managed shelves

You can inventory all managed shelves in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Shelf (equipment) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 Sort the results to obtain a list of shelf-specific codes. For example:

- Operational State
- Administrative State
- CLEI Code
- Manufacturer
- Manufacture Date
- CLLI Code
- Part Number
- Serial Number

Right-click on the column heading and deselect all columns in the contextual menu that you do not want to view or save. The deselected columns disappear from the display.

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

7 Close the form.

Procedure 19-17 To inventory all management ports

You can inventory all management ports in a network of managed devices.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Network Element (netw) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. The list form displays the results of the inventory search.

5 Sort the results to obtain a list of management port-specific codes. For example:

- System ID
- Management IP Address
- Location
- Chassis Type
- Sys Object ID
- Software Version
- Descriptor Version (software release)
- Resource Group ID

Right-click on the column heading and deselect all columns in the contextual menu that you do not want to view or save. The deselected columns disappear from the display.

6 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

7 Close the Manage Equipment form.

Procedure 19-18 To collect inventory data for network device SLA audits

You can create lists of inventory data to provide the specific summary information required for SLA audits. Ensure the following before you start:

- Inventory collection requirements differ based on SLA agreements. Ensure that the correct data is being collected for your SLA agreement.
- Perform inventory collection during a maintenance window, or during low network activity windows to ensure no impact to systems.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Collect the required SLA audit data.

a For card SLA audits, choose Card (equipment) from the object drop-down list.

b For shelf SLA audits, choose Shelf (equipment) from the object drop-down list.

c For power supply tray SLA audits, choose Power Supply Tray (equipment) from the object drop-down list.

3 Click on the Search button. The SLA audit data appears in the list.

4 Typically, only a subset of data is required for SLA audits. To display only the required information, perform the following:

i Left-click on the list column heading. The list contextual menu appears.

ii Ensure the information that you want displayed has a check mark. These typically include:

- Identification information, such as Site ID, Site Name, Slot ID, and Slot Name
- SLA audit and ordering information, such as Manufacture Date, Part Number, Serial Number, CLEI Code, and Card Type

iii Close the list contextual menu. Only the chosen information is displayed in the list.

iv Choose Save Table Preferences from the list contextual menu to save the refined list for future use. When a similar search from the same client GUI is performed, the refined list is shown by default.

v Confirm the action.

5 Save the inventory output.

a To save the output in an HTML file, perform steps 2 and 3 of Procedure 19-2.

b To save the output in a CSV file, perform steps 2 and 3 of Procedure 19-3.

6 Close the form.

20 — TCP enhanced authentication

20.1 TCP enhanced authentication overview

This chapter describes the 5620 SAM support of TCP enhanced authentication for NEs based on the MD5 encryption mechanism described in RFC2385. 5620 SAM TCP enhanced authentication allows the use of powerful algorithms for authenticating routing messages.

The 5620 SAM uses a TCP extension to enhance BGP and LDP security. TCP enhanced authentication is used for applications that require secure administrative access at both ends of a TCP connection. TCP peers update authentication keys during the lifetime of a connection.

A 5620 SAM operator with administrative privileges can create, delete, modify, and distribute TCP enhanced authentication components, and can perform an audit of a local key chain to compare it with the associated global key chain or other local key chains. The 5620 SAM TCP enhanced authentication components are called keys and key chains.

Global key chains are created in draft mode. This allows operators to verify that the key chain is correctly configured before they distribute it to the network elements. When the key chain is approved for distribution, you can change the global key chain to released mode, which also distributes the key chain to existing local definitions. The 5620 SAM saves the latest released version of the global key chain.

Caution — Alcatel-Lucent recommends that you use only the 5620 SAM to create keys and key chains. Do not create a key or key chain directly on a managed NE using another interface, for example, a CLI. The 5620 SAM cannot obtain a TCP key secret value from an NE during resynchronization, so it cannot specify the key for use on another NE.

If a local NE key chain and the associated global 5620 SAM key chain differ after a resynchronization, the 5620 SAM raises an alarm.

TCP keys and key chains

A key is a data structure that is used to authenticate TCP segments. One or more keys can be associated with a TCP connection. Each key contains an identifier, a shared secret, an algorithm identifier, and information that specifies when the key is valid for authenticating the inbound and outbound segments.

A key chain is a list of up to 64 keys that is associated with a TCP connection. Each key within a key chain contains an identifier that is unique within the key chain. You can use the 5620 SAM to distribute a global key chain to multiple NEs and assign a key to multiple BGP or LDP instances.

The 5620 SAM treats global and local key chain management as it does policy management; depending on the distribution mode configuration of a local key chain, when you modify a global key chain using the 5620 SAM, all local instances can be updated to ensure that all instances of the key chain in the network are synchronized. See chapter 43 for information about global and local policy instances, policy distribution and distribution modes, and local policy audits.

When the 5620 SAM attempts to synchronize the keys in a global key chain with the keys on an NE, the NE does not return the secret key value. After a key chain is deployed to an NE, the shared secret and the encryption algorithm cannot be modified. You can delete a key chain or key only when it is not in use by a protocol.

You can specify whether an NE uses a TCP key for sending packets, receiving packets, or both. Using keys that are configured for both, or send-receive, is general good practice because communication between NEs cannot be affected by assigning the wrong key type.

There are two classes of TCP keys:

- Active
- Eligible

Active keys

A key set contains one active key. An active key is a key that TCP uses to generate authentication information for outbound segments. You cannot delete the active key in a keychain.

Eligible keys

Each set of keys, called a key chain, contains zero or more eligible keys. An eligible key is a key that TCP uses to authenticate inbound segments.

20.2 Workflow to create a global key chain and local key

1. Create a global key chain that contains at least one key.
2. Distribute the key chain to NEs, as required.
3. Assign the key chain to a routing protocol, such as BGP or LDP.
4. Modify a key chain or key, if required. The modified object is automatically distributed to the NEs that have a local instance of the key chain.
5. Delete a key chain, as required.

20.3 TCP enhanced authentication menu

Table 20-1 lists the TCP enhanced authentication menu and the associated functions.

Table 20-1 5620 SAM TCP KeyChains menu

Menu option	Function
Administration→Security→TCP KeyChains	Create and manage TCP keys and key chains.

20.4 TCP enhanced authentication procedures

Use the following procedures to perform TCP enhanced authentication management functions.

Procedure 20-1 To create a global key chain

Perform the following procedure to create a global TCP key chain for distribution to NEs.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Click on the Create button. The KeyChain (Create) form opens.

3 Configure the parameters.

- Displayed Name
- Description
- Send Option
- Receive Option
- Admin State

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click the KeyChain Key tab button.

5 Click the Add button. The KeyChain Key (Create) form opens.

6 Configure the parameters:

- Key ID
- Auto-Assign ID
- Secret Key Algorithm
- Key
- Key Direction
- Admin State
- Begin Time
- End Time
- Tolerance

Caution — Alcatel recommends that you choose the Send-receive option for the Key Direction parameter to ensure bidirectional communication between NEs.

Note — The 5620 SAM generates a random default value for the Key parameter. For greater security, Alcatel-Lucent recommends that you accept this value rather than manually enter a value.

7 Click on the OK button. A dialog box appears.

8 Click the OK button. The key is added to the keychain and displayed on the KeyChain (Edit) form.

9 Click the OK button. The KeyChain (Edit) form closes.

10 Close the TCP KeyChains form.

Procedure 20-2 To distribute global key chains to NEs

Perform the following procedure to distribute one or more global TCP key chains to one or more NEs. When you distribute a global key chain, local key chain using the Sync With Global distribution mode allow the NE to receive the key chain.

Note — Local key chains using the Local Edit Only distribution mode do not allow the NE to receive the distribution of a global key chain. You must ensure that the distribution mode for the local key chain is set to Sync With Global if you want the NE to receive the distribution of a global key chain.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Configure the filter criteria and click on the Search button. A list of key chains is displayed.

3 Select one or more key chains in the list.

4 When the key chain is in draft configuration mode, the Distribution button is disabled and the key chain cannot be distributed to the network elements. You must first release the key chain for distribution by performing the following steps. Releasing the global key chain also distributes the key chain to existing local definitions. Otherwise, go to step 5.

   i Click on the Properties button. The Key Chain (Edit) form opens.

   ii Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears.

   iii Click on the Yes button. The configuration mode of the key chain is changed to Released.

Warning — When you switch the configuration mode of the global key chain to released, the key chain is distributed to existing local definitions.

iv View the local key chain, if necessary, by clicking on the Local Definitions tab button and double-clicking on the local key chain in the list.

v Close the Key Chain (Edit) form. The TCP KeyChains form reappears.

5 Click the Distribute button. The Distribute - KeyChain form opens.

6 Select one or more NEs in the Available Nodes list.

7 Click on the right-arrow button. The selected NEs move to the Selected Nodes list.

8 Click on the Distribute button. The 5620 SAM distributes the key chains to the NEs.

9 Close the Distribute - KeyChain form. The TCP KeyChains form reappears.

10 Configure the distribution mode of the local definitions by performing the following steps.

i Click on the Distribution Mode button. The Distribution Mode form opens.

ii Choose Sync With Global, Local Edit Only, or All from the Distribution Mode parameter drop-down menu. The sites that are configured with the selected distribution mode are listed.

iii Choose one ore more rows from the Available Nodes list.

iv Click on the right arrow button. The chosen site or sites move to the Selected Nodes panel on the right side of the form.

v Depending on the distribution mode of the chosen site or sites, perform one of the following steps:

- Click on the Sync With Global button.
- Click on the Local Edit Only button.

vi Close the Distribution Mode form. The TCP KeyChains form reappears.

11 Close the TCP KeyChains form.

Procedure 20-3 To verify the distribution of a global key chain to NEs

Perform the following procedure to view a list of the NEs to which the 5620 SAM has successfully distributed a specific TCP key chain.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Configure the filter criteria and click on the Search button. A list of key chains is displayed.

3 Select a key chain in the list.

4 Click on the Properties button. The KeyChain (Edit) form opens.

5 Click on the Local Definitions tab button. The NEs that have a local instance of the key chain are displayed in a list.

6 View the list of NEs to confirm that the key chain is distributed to the required NEs.

7 Close the KeyChain (Edit) form.

8 Close the TCP KeyChains form.

Procedure 20-4 To modify a key chain or key

Perform the following procedure to modify global or local TCP key chain or key parameters, or to add a key to an existing global or local key chain.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Perform one of the following actions.

a Modify a global key chain.

i Select Global from the Policy scope drop-down menu.

ii Configure the filter criteria and click on the Search button. A list of global key chains is displayed on the form.

b Modify a local key chain.

i Select Local from the Policy scope drop-down menu.

ii Click on the Select button to choose an NE. The Select a Network Element form opens.

iii Select an NE in the list and click on the OK button. The NE IP address is displayed in the Local Node IP Address field.

iv Click on the Search button. A list of key chains on the NE is displayed.

3 Select a key chain in the list and click on the Properties button. The KeyChain (Edit) form opens with the General tab displayed.

4 Configure the parameters, if required.

- Description
- Send Option
- Receive Option
- Admin State

5 Click the KeyChain Key tab button. The key chain keys are listed.

6 Modify a key, if required.

i Select a key in the list and click on the Properties button. The KeyChain Key (Edit) form opens.

ii Perform steps 6 to 8 of Procedure 20-1.

7 To add a new key to the key chain, perform steps 4 to 8 of Procedure 20-1.

8 Click the OK button. The KeyChain (Edit) form closes.

9 Close the TCP KeyChains form.

Procedure 20-5 To delete a key chain

Perform the following procedure to permanently remove a local or global TCP key chain.

Caution — Deleting a TCP key chain can be service-affecting. Ensure that you understand the implications of deleting the key chain before you proceed.

Note — You cannot delete a TCP key chain when the Admin State parameter for the key chain is set to In Service.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Perform one of the following actions.

a Delete a global key chain.

i Select Global from the Policy scope drop-down menu.

ii Configure the filter criteria and click on the Search button. A list of global key chains is displayed on the form.

b Delete a local key chain.

i Select Local from the Policy scope drop-down menu.

ii Click on the Select button to choose an NE. The Select a Network Element form opens.

iii Select an NE in the list and click on the OK button. The NE IP address is displayed in the Local Node IP Address field.

iv Click on the Search button. A list of key chains on the NE is displayed.

3 Select a key chain in the list and click on the Delete button. A dialog box appears.

4 Click on the OK button. A dialog box appears.

5 Click on the OK button. The 5620 SAM deletes the key chain and removes it from the list.

6 Close the TCP KeyChains form.

Procedure 20-6 To delete a key

Perform the following procedure to permanently remove a key from a local or global TCP key chain.

Caution — Deleting a TCP key can be service-affecting. Ensure that you understand the implications of deleting the key before you proceed.

Note — You cannot delete a TCP key when the Admin State parameter for the key is set to In Service.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Perform one of the following actions.

- **a** Delete a key from a global key chain.
  - **i** Select Global from the Policy scope drop-down menu.
  - **ii** Configure the filter criteria and click on the Search button. A list of global key chains is displayed on the form.
- **b** Delete a key from a local key chain.
  - **i** Select Local from the Policy scope drop-down menu.
  - **ii** Click on the Select button to choose an NE. The Select a Network Element form opens.
  - **iii** Select an NE in the list and click on the OK button. The NE IP address is displayed in the Local Node IP Address field.
  - **iv** Click on the Search button. A list of key chains on the NE is displayed.

3 Select a key chain in the list and click on the Properties button. The KeyChain (Edit) form opens with the General tab displayed.

4 Click the KeyChain Key tab button. The key chain keys are listed.

5 Select a key in the list and click on the Delete button. A dialog box appears.

6 Click on the OK button. The 5620 SAM deletes the key and removes it from the list.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The KeyChain (Edit) form closes.

9 Close the TCP KeyChains form.

Procedure 20-7 To identify differences between a global and local policy or two local key chains

Note 1 — You can cancel the local audit at any time by clicking on the Local Audit Off button on the KeyChain (Edit) form.

Note 2 — The 5620 SAM does not identify differences between the Begin Time and End Time properties of key chains.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Choose Local from the Policy scope drop-down menu.

3 Click on the Select button beside the Local Node IP Address parameter. The Select a Network Element form opens.

4 Choose a device from the list and click on the OK button. The Select a Network Element form closes and the TCP KeyChains form is updated with the network element IP address.

5 Click on the Search button. A list of local key chains is displayed.

6 Choose the local key chain that you want to compare with another key chain.

7 Click on the Properties button. The KeyChain (Edit) form opens.

8 Click on the Local Audit On button. The Local Audit form opens.

9 From the Policy scope drop-down menu:

- **a** Choose Global and go to step 10.
- **b** Choose Local and configure the Local Node IP Address parameter by using the Select button to choose a network element. The Select a Network Element form opens.
  - **i** Choose a network element and click on the OK button. The Select a Network Element form disappears, and the policy manager form reappears with a list of the local policies for the chosen network element in the bottom panel.
  - **ii** Go to step 10.

10 Click on the OK button. The Local Audit form closes.

11 View the differences between the key chains by clicking on the tab buttons that are highlighted with an arrow icon to indicate that differences exist on the forms. An arrow icon beside a property indicates that the property is modified. In lists, new entries are highlighted in pink and modified entries are highlighted in purple.

12 Close the local and global key chain (Edit) forms.

21 — NE maintenance

21.1 NE maintenance overview

The 5620 SAM includes NE maintenance functionality for supported devices that allows a system administrator to:

- define the 5620 SAM deployment and local device configuration-save conditions
- perform an on-demand or scheduled NE configuration backup
- restore a previous device configuration
- perform an on-demand or scheduled NE software upgrade; scheduled software upgrades are supported on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7210 SAS-E, 7450 ESS, 7750 SR, 7710 SR, 7705 SAR, and 9500 MPR.
- view the status of a deployment, backup, device configuration restore, device software upgrade, or accounting statistics retrieval operation in progress
- troubleshoot a failed deployment, backup or upgrade

A 5620 SAM operator with an administrator or network element software management scope of command role and can perform device configuration save, backup, or restore operations, and can create policies for scheduling backups and configuration saves.

A 5620 SAM operator can upgrade software or schedule a software upgrade on sites and routers that are within their span of control.

A 5620 SAM operator with lawful intercept management scope of command role can perform back up and restore operations for LI configuration on an NE. Back up data is saved only when the LI local save allowed parameter is set to True. See Procedure 12-9 for more information about configuring LI local save allowed.

Managing NE deployments

When you apply a device configuration change using the 5620 SAM—for example, by clicking on OK or Apply after changing a service parameter—the 5620 SAM deploys the configuration change to the device according to the 5620 SAM deployment policy. The 5620 SAM deployment policy also specifies when the device saves its configuration locally. The information in a deployment policy includes the following:

- the number and frequency of deployment retries that the 5620 SAM performs
- the conditions under which the 5620 SAM initiates a device configuration save, such as the frequency and level of saved configuration detail

In a lab or testing environment, it is sometimes necessary to disable 5620 SAM deployment. See the *5620 SAM-O OSS Interface Developer Guide* for information about disabling 5620 SAM deployment.

Managing NE backups and restores

A 5620 SAM backup policy specifies the conditions under which the 5620 SAM performs a device backup to ensure that the device configuration is not lost in the event of a failure. A default policy that is assigned to all managed devices is in place after 5620 SAM installation. You can create and configure multiple backup policies, and you can assign them to multiple NEs. You cannot delete a backup policy that is assigned to an NE. The information in a backup policy includes the following:

- the frequency of backups
- the files that a backup collects
- the type of file compression that the 5620 SAM uses
- the age and number of backup files that the 5620 SAM retains

The 5620 SAM stores the backed-up device configuration files in the 5620 SAM database for ease of tracking and retrieval. You can perform an on-demand export of backup files from the database to a file system, and can import NE backups from a file system to the 5620 SAM database.

You can configure the 5620 SAM to save device configuration backup files to the main-server file system, in addition to the 5620 SAM database, by editing a main-server configuration file. The saved files are synchronized between the primary and standby main servers in a redundant 5620 SAM deployment.

You can configure the 5620 SAM to do the following:

- automatically save device backups to a file system in addition to the database
- automatically delete device backup files after the associated NE is unmanaged

See chapter 5 for more information.

When a device configuration requires replacement, for example, because it becomes corrupted, you can restore a previously backed-up configuration. Unless otherwise specified, the 5620 SAM restores the most recent device configuration backup. See Procedures 21-4 and 21-7 for more information.

Managing NE software upgrades

When a new device software version is available, you can use the 5620 SAM to perform an on-demand NE software upgrade or schedule one using a software upgrade policy. You can create and configure multiple software upgrade policies and assign them to multiple NEs. You cannot delete a software upgrade policy that is assigned to an NE. The information in a software upgrade policy includes the following:

- the NE file location of the currently active device software
- the NE file location in which to store a backup copy of the current device software
- whether to activate the software after transferring it to the NE
- whether to reinitialize the NE after the upgrade
- whether the upgrade is an in-service software upgrade, or ISSU

During a software upgrade, the 5620 SAM performs checks to ensure that the new software is compatible with the device type and that the required files are present. The 5620 SAM does not initiate a device software upgrade unless the necessary conditions are in place. You can use the 5620 SAM to roll back a software upgrade to the previous version in the event of an upgrade failure.

Note — The 5620 SAM does not support a software upgrade or downgrade on a Telco, 7250 SAS, 7250 SAS-ES or 7250 SAS-ESA NE. You can use a software upgrade policy to upload a software image to the NE, but the upgrade or downgrade must be performed using a CLI. Contact your Alcatel-Lucent technical support representative for information about downgrades.

See Procedures 21-8 and 21-11 for more information.

ISSUs

An ISSU on a managed device that has dual CPMs allows the device to provide uninterrupted service during the upgrade process. A device software upgrade requires a CPM restart, which causes temporary device down time. When a device has dual CPMs, however, one CPM can remain active while the other restarts with the upgraded software. These alternate CPM restarts mean that the device remains in service during the upgrade. If an upgrade on a CPM fails, the CPM reports a failed state and raises an alarm. In-service software upgrades for devices are restricted to maintenance software releases.

You can specify that the 5620 SAM activates the new software image immediately after transferring it to an NE, or you can specify only the file transfer and manually activate the software image later. Manual software activation provides more control over an upgrade, which may be required, for example, when multiple NEs are involved.

NE file-system browsing

A 5620 SAM operator can browse the file system of a managed NE to list the contents of the compact flash devices. You can browse files for the 7450 ESS, 7750 SR, 7710 SR, 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, and 7705 SAR using simple FTP or a CLI session using SSH. The 5620 SAM GUI is used to browse the different types of files.

Browsing an NE file system using the 5620 SAM is a convenient way to confirm that operations such as the following occur as planned by verifying the sizes and time stamps of local NE files:

- NE configuration saves
- NE software image transfers and upgrades
- NE configuration restores
- NE accounting-statistics collection

FTP file browsing on an NE requires FTP user-account access on the NE. SSH file browsing requires console user-account access and the configuration of SSH security on the NE. See chapter 13 for information about enabling FTP or console access for an NE user account. See chapter 13 for information about configuring SSH on an NE.

Note — The 7705 SAR may become temporarily unreachable when enabling SSH and starting the SSH server on the device.

See Procedure 21-23 for information about browsing an NE file system using an FTP file browser. See Procedure 21-24 for information about browsing an NE file system using an SSH file browser.

Secure file transfers for site backups and upgrades

The 5620 SAM supports both secure and non-secure file transfers in backups, restores, and software upgrades. Secure file transfers using SSH2 are supported by the 7450 ESS, 7750 SR, 7705 SAR, 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, and 7710 SR. The device mediation policy determines whether FTP or SCP is used during file transfers. See chapter 13 for information about configuring SSH2.

Sample deployment policy configuration

The following example describes the configuration and operation of a 5620 SAM deployment policy. The example uses the default parameter values, which are appropriate for most applications. The Deployment Policy properties form contains the parameters listed in the example. See Procedure 21-1 for deployment configuration information.

Example details

The sample deployment policy specifies that after a configuration deployment failure, the 5620 SAM retries the deployment until it is successful. The policy also specifies that the 5620 SAM initiates a save of the device configuration to local storage after every configuration change. In order to conserve storage space, the device is configured to save the configuration information for only the device parameters that are not at their default values.

The deployment policy parameters and their values for the example are:

- Auto Save Scheme—Every Deployment
- Auto Save Threshold—0
- Scheduled Save Scheme—None
- Scheduled Save Interval—1 hour
- Save Details—disabled
- Retry Scheme—Retry Forever
- Retry Interval—5 minutes
- Retry Threshold—0

Sample backup/restore policy configuration

The following example describes a sample 5620 SAM backup/restore policy configuration and its operation using parameter values that are appropriate for most applications. The Backup Policy form contains the parameters listed in the example. See Procedure 21-3 for the configuration information.

Example details

The sample backup policy specifies that the 5620 SAM obtains the backup files by FTP from the device once every hour regardless of configuration activity, and after every 25 configuration changes. The policy also specifies that the 5620 SAM backs up the device configuration file and boot options file (BOF) only when a newer file is present, and uses gzip file compression. The 5620 SAM is to retain at most 30 backup versions, and purge versions that are more than 30 days old.

The backup policy parameters and their values are:

- Enable Backup—enabled
- Auto Reboot After Successful Restore—enabled
- Scheduled Backup Scheme—Every Scheduled Interval
- Scheduled Backup Interval—1 hour
- Scheduled Backup Sync Time — 00:00
- Scheduled Backup Threshold (operations)—5
- Auto Backup Scheme—Every Nth 5620 SAM Server Initiated Save
- Auto Backup Threshold (operations)—50
- CLI Config File Mode—New Version Only
- CLI Config Save Details—disabled
- CLI Debug Save Config File Mode—disabled
- Boot Option File Mode—New Version Only
- File Compression—GZIP
- Auto-Purge Scheme—By Age But Retain A Minimum Number Of Backups
- Number of Backups—30
- Maximum Backup Age (days)—30

Figure 21-1 5620 SAM backup process

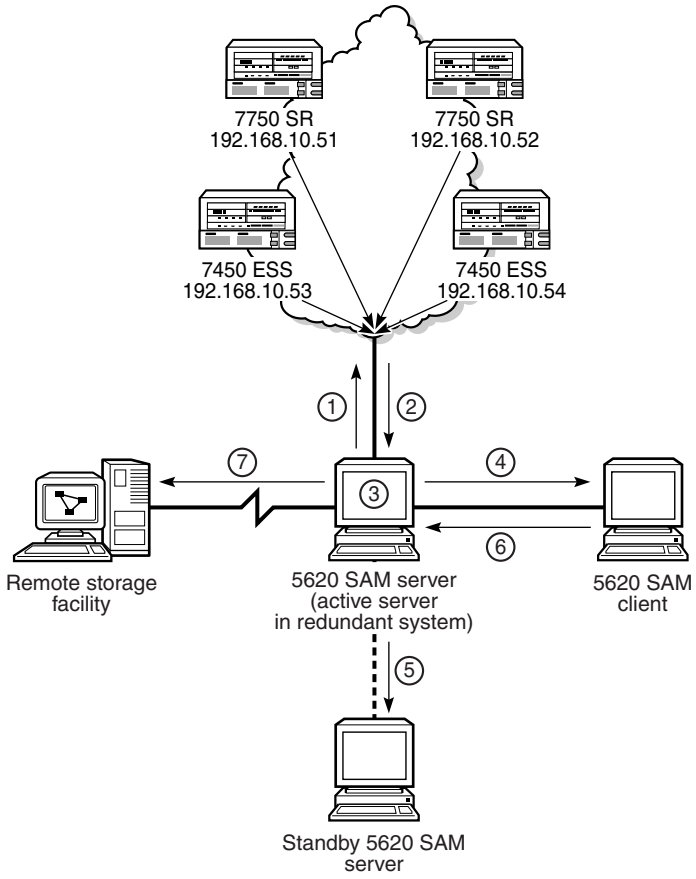


Figure 21-1 illustrates the activities of the 5620 SAM backup/restore process. The labels correspond to events in the following sequence:

1 At the interval specified—every hour in this example—the 5620 SAM issues an FTP or SCP request to all devices for a backup.

2 The devices use FTP or SCP to send the BOF and configuration files to the 5620 SAM server.

3 The 5620 SAM server stores the received files in the 5620 SAM database.

4 An operator using a 5620 SAM client uses the Backup/Restore Status tab of the Backup Policy form to view the backup status.

5 If the 5620 SAM system is a redundant configuration, the active server synchronizes the backed-up information with the standby server.

6 A 5620 SAM operator uses the Backup/Restore form to perform on-demand and scheduled device backups, restores, and configuration saves, as required.

7 A third-party application periodically sends a copy of the backup files from the 5620 SAM server to a remote storage facility for safekeeping.

21.2 Workflow for NE maintenance

1. For secure backups and upgrades, ensure that SSH2 is properly configured on the device and that the 5620 SAM mediation policy for the device is configured for secure FTP, or SCP. See chapter 12 for information about device commissioning. See chapter 13 for information about configuring a 5620 SAM mediation policy. Secure backups and upgrades are supported on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7450 ESS, 7710 SR, 7750 SR, and 7705 SAR.
2. Commission the managed devices using a CLI. See chapter 12 for information about device commissioning.
3. Configure the 5620 SAM deployment policy to specify how and when the 5620 SAM tries to send configuration changes from 5620 SAM clients to the managed devices.
4. Use the 5620 SAM to configure device backup policies. A device backup policy specifies how often the 5620 SAM backs up the device configuration.
5. Schedule device software upgrades, as required. Scheduled software upgrades are supported on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, 7710 SR, 7750 SR, 7705 SAR, and 9500 MPR.
   - **i** Create a 5620 SAM schedule. See chapter 74 for information about creating 5620 SAM schedules.
   - **ii** Create a software upgrade policy and create a 5620 SAM scheduled task for the upgrade activity.
   - **iii** Review the results and status of the scheduled upgrade and take the appropriate actions, as required, based on your company policies.
6. Perform on-demand NE configuration saves, backups, and restores as required.
7. View the status of configuration deployments, backups, restores, or upgrades using the appropriate management form and by viewing the contents of NE file systems by opening an FTP or SSH file browser from the 5620 SAM client GUI.
8. Troubleshoot failed configuration deployments, as required using the 5620 SAM alarm window and the Deployment form.

21.3 Workflow for a 7450 ESS, 7710 SR, or 7750 SR software upgrade

Caution — Before you perform an ISSU, review the appropriate device release notice for more information about the device software releases that support the ISSU. The software upgrade information in the device documentation takes precedence over this procedure.

1. Perform a preliminary check before you start the software upgrade.
   - **i** Manually verify the software image file checksums.
   - **ii** Verify that the device supports the new software.

iii Verify that there is sufficient space on the compact flash drive for the software image files.

iv For NEs with redundant CPMs, verify that the boot environments are synchronized by using the appropriate CLI command.

2 Download the software description file to a directory on a 5620 SAM client station.

3 Import the software description file.

4 Back up the device configuration. See Procedure 21-4.

5 Perform a scheduled software upgrade or an immediate software upgrade to transfer the software image files to each NE that you need to upgrade.

6 After the upgrade, verify whether the boot environment synchronization is successful.

7 Reboot the NE, if required.

Note 1 — Some device software upgrades do not require a reboot; for example, ISA-AA upgrades and ISSUs. See the device documentation for more information.

Note 2 — When you perform an ISSU, you can manually soft reset or hard reboot the IOMs after an upgrade. A soft reset results in minimal downtime, but has restricted support. See Procedure 21-9 for information about a manual soft reset. See Procedure 21-10 for information about a manual hard reboot.

Note 3 — For MDAs, CMAs, and MCMs in a 7710 SR, Release 7.0 or later, after an ISSU, the system determines what needs to be reset and performs the required resets automatically. Manual intervention is not required.

Note 4 — When the IOMs are not manually soft reset or hard rebooted, the device performs a soft reset, if supported, after 2 h; otherwise, the device performs a hard reboot after 2 h.

8 Verify whether the upgrade is successful, as described in Procedure 21-20.

9 Use the FTP or SSH file browser to verify whether the transferred files and configurations are on the device.

10 Remove obsolete software images from the device.

11 Fully resynchronize the NE using the 5620 SAM GUI. See chapter 13 for information about resynchronizing an NE.

12 Perform upgrade verification tests, as required.

21.4 Workflow for a 7250 SAS software upgrade

Caution — The software upgrade information in the device documentation takes precedence over this procedure. Before you perform a software upgrade, read the device documentation.

1. Perform a preliminary check before you start the software upgrade.
   - i. Verify that the device supports the new software.
   - ii. Verify that there is sufficient space on the compact flash drive for the software image files.
2. Download the software description file to a directory on a 5620 SAM client station.
3. Load the software description file.
4. Back up the device configuration using the script manager or CLI.
5. Start the upgrade procedure using the script manager. Perform a scheduled software upgrade or an immediate software upgrade to transfer the software image files to each NE that you need to upgrade.
6. Reboot the NE.
7. Verify whether the upgrade is successful.
8. Use the FTP or SSH file browser to verify whether the transferred files and configurations are on the device.
9. Remove obsolete software images from the device.
10. Fully resynchronize the NE using the 5620 SAM GUI.
11. Perform upgrade verification tests, as required.

21.5 Workflow for a 9500 MPR software upgrade

1. Create a 9500 MPR software upgrade policy; see Procedure 21-8 for more information. The software upgrade policy provides the 9500 MPR NE with information about where to obtain the new software image files during a software upgrade.
2. Download the 9500 MPR software description file to a directory on your 5620 SAM client; software description files have a .DSC file extension. A software description file identifies the files required to upgrade the 9500 MPR.

3 Import the software description file that you downloaded in step 2 to the 5620 SAM database. See Procedure 21-18 for more information.

Note — A prerequisite of the 9500 MPR software upgrade is that the .DSC file must be available on the machine which hosts the 5620 SAM client. Other software files do not need to be present on the client system. The mpr sw package can be on the client system or on a different ftp server than the client. If the ftp host is not on the client itself, then copy the image descriptor file (.DSC extension) onto the client system.

Because the 9500 MPR NE software upgrade uses FTP, the software image files must be available on an FTP server in a specific directory format. For example, assume the directory structure is R95MSS/2_2_1X. The sw version "2_2_1X" is found from the dsc file. An image directory name other than 2_2_1X (e.g., 2.2.1.X or 2.2.1_X) would not be accepted.

The path specified in the root directory field of the Software Upgrade policy form on the General tab must be the path that contains R95MSS/2_2_1X directory on the FTP server. For example, if R95MSS/2_2_1X is in the root directory, then the path is "/". If R95MSS/2_2_1X is in the /MPR/SW directory, then the path is "/MPR/SW".

4 Perform a scheduled software upgrade or an immediate software upgrade to transfer the software image files to each 9500 MPR that you need to upgrade. See Procedure 21-14 for more information about performing an immediate software upgrade. See Procedure 21-15 for more information about performing a scheduled software upgrade.

5 Activate the new software on each upgraded 9500 MPR NE. See Procedure 17-50 for more information about activating software on a 9500 MPR NE.

21.6 NE maintenance procedures

Use the following procedures to perform NE maintenance operations.

Procedure 21-1 To configure the 5620 SAM deployment policy

1 Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Deployment form opens with the Incomplete Deployments tab displayed.

2 Click on the Deployment Policy tab button.

3 Configure the parameters:

- Auto Save Scheme
- Auto Save Threshold
- Scheduled Save Scheme
- Scheduled Save Interval
- Save Details
- Retry Scheme
- Retry Interval
- Retry Threshold

4 Click on the OK button. A dialog box appears.

5 Click on the Yes button. The Deployment form closes.

Procedure 21-2 To troubleshoot a failed configuration deployment

The 5620 SAM continues to retry deployments after a failed or incomplete deployment attempt, based on the 5620 SAM deployment policy, as configured in Procedure 21-1. When there is a deployment error, a number of problems can occur, for example:

- The 5620 SAM database may lose synchronization with the device database.
- Configuration changes requested using the client GUI may clash with configuration changes, retries, and recovery applications developed by an OSS system using the 5620 SAM-O interface or by an operator using a CLI.

When a failed or incomplete deployment or a failed SNMP configuration request occurs, a Problems Encountered error display form appears automatically. This form displays error information about the failure(s).

Note 1 — The Request Id and Task Name fields appearing on the Problems Encountered error form can be used for troubleshooting using the Task Manager application.

Note 2 — The Problems Encountered error form can appear for non-deployment generated errors also.

For example, to view more information on a failed deployment, select a failed deployment entry, then click on the Properties button, or double-click on the failed deployment entry.

An error form opens which contains a View Affected Object button and a Details button.

Click on the Details button to view detailed diagnostic information about the failure(s).

Click on the View Affected Object button. A form displaying object properties opens. This form facilitates rapid navigation to the object which caused the failure for troubleshooting purposes.

Click on the Faults tab button. Alarm information related to the failure(s) is displayed.

A failure error message is not generated when the alarm is cleared or the failure entry is deleted.

Note 1 — If a deployment failure is associated with more than one 5620 SAM GUI, the Problems Encountered form and related forms appear only on the GUI from which the deployment was issued.

Note 2 — The automatically generated Problems Encountered form and related forms, are an additional tool to the following troubleshooting procedure.

The Deployment form displays failed configuration deployments and allows you to view information about failed deployments. Using this form, you can clear the deployment, override the error to force the configuration to be downloaded to the device, or suspend or resume deployment retries to a device.

1 Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Deployment form opens with the Incomplete Deployments tab displayed.

2 Review the deployment information. The State value indicates the cause of the deployment failure.

3 Select a deployment in the list and click on the Properties button. The properties form for the deployment opens. The objects that the deployment failed to modify are displayed in the Objects list.

4 Select an entry in the Objects list and click on the Properties button. The Object Change form that describes the attempted configuration change opens.

5 Select an entry in the Attributes list and click on the Properties button. The Attribute Change form opens and displays the following object attribute information for troubleshooting:

- the NE attribute that was to be modified
- the old, unmodified attribute value
- the new attribute value that the deployment failed to assign

6 Click on the Cancel button to close the Attribute Change form.

7 Click on the Cancel button to close the Object Change form.

8 Click on the Cancel button to close the deployment properties form.

9 Perform one of the following actions, depending on the result of the investigation into the failed deployment.

a Click on the Suspend Retries button to override the deployment policy setting and prevent further retries of the deployment. A dialog box appears; click on the Yes button.

b Click on the Resume Retries button to override a previous Suspend Retries action performed on the deployment. A dialog box appears; click on the Yes button.

c Click on the Clear button to clear the deployment. A dialog box appears; click on the Yes button. The deployment is cleared.

Note — Clearing a failed deployment may result in a loss of data synchronization between the 5620 SAM database and the NE. Alcatel-Lucent recommends that you resynchronize the NE objects associated with a failed deployment after you clear a failed NE deployment.

d Click on the Force Submit button to force the 5620 SAM to immediately resend the deployment to the NE. A dialog box appears; click on the Yes button.

10 Click on the Refresh button to update the list of failed deployments.

11 Take the appropriate action described in this procedure to troubleshoot other failed deployments, as required.

12 Close the Deployment form.

Procedure 21-3 To create a device backup policy

When the 5620 SAM performs a device configuration backup, it transfers files to itself from the device.

Note — The default backup policy is assigned automatically to all 5620 SAM-managed NEs that do not currently have an assigned backup policy.

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

2 Click on the Create button. The Backup Policy (Create) form opens.

3 Specify whether backup functionality is enabled.

a Enable the Enable Backup parameter.

b Disable the Enable Backup parameter. The remaining parameters on the form cannot be configured. Go to step 13.

4 Configure the following parameters:

- Policy ID
- Auto-Assign ID
- Name
- Policy Type

5 If you selected AOS Based Node policy type, go to step 7.

6 Specify whether to perform a reboot after the configuration is restored to the device by specifying the Auto Reboot After Successful Restore parameter.

Caution — When you use the 5620 SAM client GUI to restore a managed device configuration and you disable the Auto Reboot After Successful Restore parameter, there is a risk that the bof.cfg file may be overwritten in the following situations:

- when a user performs “bof save” using CLI on the managed device
- If there is a gap between a restore and a reboot, perform a “show bof” to ensure that another user has not performed a “bof save”.

7 You can schedule backups based on a time interval or on the number of NE configurations performed from the 5620 SAM server. Configure the backup triggering parameters:

- Scheduled Backup Scheme
- Scheduled Backup Interval
- Scheduled Backup Sync Time
- Scheduled Backup Threshold (operations)
- Auto Backup Scheme
- Auto Backup Threshold (operations)

8 Perform one of the following:

a If you selected SR Based Node policy type, go to step 9.

b If you selected AOS Based Node policy type, go to step 11.

c If you selected MPR Based Node policy type, go to step 12.

9 Configure the Backup Settings parameters:

- CLI Config File Mode
- CLI Config Save Details
- CLI Debug Save Config File Mode
- Boot Option File Mode
- File Compression

Note — In addition to enabling the CLI Debug Save Config File Mode parameter, you must specify the location of the debug configuration files in the 5620 SAM main server configuration. See chapter 5 for information about how to specify the location of the debug configuration files in the main server configuration.

10 Go to step 12.

11 Configure the AOS Backup Settings parameters:

- Save Certified Directory
- Save Network Directory
- File Compression

Note — The 5620 SAM can only backup configuration files stored in the certified directory. If you need to backup configuration files in the working directory, you must ensure that the files in the certified and working directories are identical. See Procedure 17-49 to perform a Certify or Certify and Synchro command before you backup the OmniSwitch configuration files.

12 Configure the parameters in the Backup Purging panel. Backup purging parameters allow you to specify the number of backup files kept. These settings allow you to eliminate manual monitoring and deletion of backup files. The purge criteria can be the number of files, the age of the files, or both.

- Auto-Purge Scheme
- Number of Backups
- Maximum Backup Age (days)

13 Click on the OK button to save the backup policy. The Backup Policy (Create) form closes.

14 Assign the policy to NEs as required.

i Select the new policy in the list and click on the Properties button. The Backup Policy (Edit) form opens.

ii Click on the Backup/Restore Policy Assignment tab button.

iii Select one or more NEs in the Unassigned Sites list and click on the right-pointing arrow to move them to the Assigned Sites list.

iv Click on the OK button. The Backup Policy (Edit) form closes and a dialog box appears.

v Click on the Yes button. The policy is assigned to the NEs.

15 Close the Backup/Restore form.

Procedure 21-4 To perform an immediate device backup, restore, or configuration save

When you start an immediate backup, you back up the device configuration based on the backup policy associated with the NE.

A device configuration restore operation uses the most recently backed-up device configuration file unless otherwise specified. See Procedure 21-7 for more information.

The following conditions must be present before you can perform a device configuration backup, restore, or configuration save:

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 8 for more information about scope of command roles.
- FTP or secure FTP is configured in the mediation policy for the NE. See chapter 13 for more information.
- The BOF persist parameter is set on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7450 ESS, 7750 SR, or 7710 SR. See chapter 12 for information about device commissioning.

Depending on the operation type, the Backup State or Restore State column displays the current state of the operation. The possible values are:

- Not Attempted - the operation is unattempted
- Saving Config - the device configuration is being saved on the device
- Transferring Files - a file transfer is in progress
- Success - the operation is complete and successful
- Failure - the operation is complete but unsuccessful
- CPM Sync and Pending Reboot - the device configuration is restored and the device is synchronizing the CPMs before it reboots
- CPM Sync and Pending Reboot Standby - the 5620 SAM is waiting for the reboot of the standby CPM
- Standby Reboot and Pending Redundant Switch-over - the 5620 SAM is waiting for the switchover to the standby CPM

Note — During a backup, if a device is unresponsive to the 5620 SAM because SNMP on the device is disabled, the Backup State column entry for the device does not immediately display the correct value of Failed. This latency is caused by the inability of the 5620 SAM to communicate with the unresponsive device. In such a situation, the Backup State column displays the initial value of Saving Config until three 10-minute SNMP polling periods, or 30 minutes, have elapsed, after which the Backup State changes to Failed if SNMP remains disabled.

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens.

2 Click on the Backup/Restore Status tab button. The managed devices are listed.

3 Select a device from the list and click on the Backup button, the Restore button, or the Save Config button, depending on the operation that you want to perform. A dialog box appears.

4 Click on the Yes button. The backup or restore operation starts, and the current backup or restore state for the device is indicated in the Backup State or Restore State column.

5 You can resynchronize an NE with the 5620 SAM database, if required, by clicking on the Resync button. See chapter 13 for information about resynchronizing an NE.

6 Close the Backup/Restore form.

Procedure 21-5 To import a device backup to the 5620 SAM database

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

2 Click on the Backup/Restore Status tab button.

3 Select the NE in the list for which you are importing a backup and click on the Properties button. The NE Backup/Restore Status form opens.

4 Click on the Import button. A file navigator form opens.

5 Use the form to specify the directory that contains the device backup and click on the OK button.

If the directory contains a backup for this NE, the 5620 SAM imports the backup files into the 5620 SAM database and the import is successful. Otherwise, a dialog box appears if the directory does not contain a backup from this NE, and the import fails. Click on the OK button to close the dialog box.

6 Close the NE Backup/Restore Status form.

7 Close the Backup/Restore form.

Procedure 21-6 To export a device backup to a file

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

2 Click on the Backup/Restore Status tab button.

3 Select the NE in the list for which you are exporting a backup and click on the Properties button. The NE Backup/Restore Status form opens.

4 Click on the Backups tab button. A list of backups for the NE is displayed.

5 Select a backup in the list and click on the Export button. A file navigator form opens.

6 Use the form to specify the directory that is to contain the exported device backup and click on the OK button. The NE configuration backup is saved to the specified directory.

7 Close the NE Backup/Restore Status form.

8 Close the Backup/Restore form.

Procedure 21-7 To restore a device configuration backup other than the most recent

You can choose to restore an older version of the device configuration to meet special network requirements.

Caution 1 — Older backups do not have the most recent network information. Restoring an older device configuration may be service-affecting.

Caution 2 — Ensure that you back up the current device configuration using Procedure 21-3 before you proceed.

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM menu. The Backup/Restore form opens.

2 Click on the Backup/Restore Status tab. The managed devices are listed.

3 Double-click on a device from the list. The NE Backup/Restore Status form for the selected device opens.

4 Click on the Backups tab button. A list of configuration backups for the selected device opens, ordered from the oldest to the most recent.

5 Select a backup in the list and click on the Restore button. A dialog box appears.

6 Click on the Yes button.

7 Click on the Resync button to ensure the latest network information is available, if required.

8 Close the Backup/Restore form.

Procedure 21-8 To create a software upgrade policy

Perform this procedure to create a policy that can be used to perform an immediate or scheduled device software image upgrade. Contact your Alcatel-Lucent technical support representative for information about downgrades.

You cannot create a software upgrade policy on the 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, or 7210 SAS-M24F2XFP [ETR].

1 Perform Procedure 21-18 to import the required device software image.

2 Ensure that the following conditions are present.

- Appropriate FTP accounts are configured and available on the devices.
- The device configuration files are backed up, as described in Procedures 21-3 and 21-4.

3 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

4 Click on the Create button. The Software Upgrade Policy (Create) form opens.

5 Configure the Policy Type parameter.

6 Perform one of the following.

a If you selected SR Based Node in step 5, go to step 7.

b If you selected AOS Based Node in step 5, go to step 10.

c If you selected MPR Node in step 5, go to step 11.

Note — If you are performing an MME software upgrade, see Procedure 15-1 in the *5620 SAM LTE ePC User Guide*.

7 Configure the following parameters:

- Auto-Assign ID
- Policy ID
- Name
- CFlash Image Root Path
- CFlash Backup Root Path

Note 1 — You can open an FTP or SSH file browser from this form to determine the values to use for the CFlash Image Root Path and CFlash Backup Root Path parameters. Click on the FTP File Browser or SSH File Browser button, as required. See Procedures 21-23 and 21-24 for more information.

Note 2 — By default, compact flash cf3 is used to store image and backup files. Some NE types do not support a cf3, for example the 7210 SAS supports only one compact flash designated as cf1. Ensure that you specify a supported compact flash for the NE type when you configure the CFlash Image Root Path and CFlash Backup Root Path parameters.

8 Perform one of the following actions, as required.

a To specify an out-of-service upgrade that activates the new software image after the download but does not reboot the NE, enable the Auto-Activate After Successful File Transfer parameter and ensure that the Auto-Reboot After Successful Activation parameter is disabled.

Note — You are not required to reboot for some NE software upgrades; for example ISA-AA upgrades. See the associated node documentation for additional information.

b To specify an out-of-service upgrade that includes rebooting the NE after activating the software, enable the Auto-Reboot After Successful Activation parameter. When you are downloading multiple images to multiple devices, Alcatel-Lucent recommends that you disable the Auto-Reboot After Successful Upgrade option to ensure that the new software properly transfers.

When you enable the Auto-Reboot After Successful Activation parameter, you are prompted to acknowledge the action because it is potentially service-affecting. Before you proceed, ensure that you understand the implications of automatically rebooting the NE after an upgrade.

The Auto-Reboot After Successful Activation parameter is configurable when the In Service Software Upgrade parameter is disabled.

Caution — When you use the 5620 SAM client GUI to perform a managed device software upgrade and you disable the Auto-Activate After Successful File Transfer and Auto-Reboot After Successful Activation parameters, there is a risk that the bof.cfg file may be overwritten in these situations:

- if a user performs 'bof save' using CLI on the managed device
- if there is a gap between the software upgrade and the reboot

Perform a 'show bof' to verify that the BOF has not been overwritten.

Note — You are not required to reboot for some NE software upgrades; for example ISA-AA upgrades. See the associated node documentation for additional information.

c To specify an in-service upgrade, select In Service Software Upgrade to upgrade a device with dual CPMs.

Note — An in-service software upgrade is supported only for a maintenance-release upgrade. For an upgrade to a new major release, you must perform an out-of-service upgrade.

Specifying an in-service software upgrade disables the Auto-Reboot After Successful Activation parameter.

9 Go to step 12.

10 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- Image Root Path
- Upgrade File Type

11 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- FTP User ID
- FTP Password
- FTP Server IP
- FTP Server Port
- Root Directory
- Forced Download

12 Click on the Apply button. The Software Upgrade Policy (Create) form refreshes with additional tab buttons and the form name changes to Software Upgrade Policy (Edit).

13 Assign the policy to NEs as required.

i Click on the Software Upgrade Policy Assignment tab button. The Software Upgrade Policy Filter (edit) form opens.

ii Configure the filter parameters, if required. Click on the OK button.

iii Select one or more NEs in the Unassigned Sites list and click on the right-pointing arrow to move them to the Assigned Sites list.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button. The policy is assigned to the NEs.

14 Close the Software Upgrade Policy (Edit) form. The new policy is displayed on the Software Upgrade form.

Procedure 21-9 To perform a soft reset of an IOM or IMM

Use this procedure to perform a manual soft reset of the following:

- IOM on a 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7450 ESS, or 7750 SR, Release 6.1 R4 or later
- IOM3 or IMM on a 7450 ESS, or 7750 SR, Release 8.0 R1 or later

Note — Soft reset is supported only under the following conditions:

- The IOM is operationally up.
- The IOM is supported.
- The MDAs are Ethernet MDAs but not HSMDAs, and are provisioned.

1 To select the IOM, in the equipment view of the 5620 SAM GUI select the Card Slot associated with an NE.

2 Right-click on the card slot and select Soft Reset from the contextual menu. A Warning form opens.

3 View the dependency information.

4 Select the I understand the implications of this action check box.

5 Click on the Yes button. The operational state of the IO card displays the soft reset status when the soft reset is in progress.

Procedure 21-10 To perform a hard reboot of an IOM

Use this procedure to perform a manual hard reboot of an IOM.

1 To select the IOM, in the equipment view of the 5620 SAM GUI select the Card Slot associated with an NE.

2 Right-click on the card slot and select Properties. The Card Slot form opens.

3 Click on the IO Card button tab button.

4 Click on the Reboot button. The operational state of the IO card displays the hard reboot status when the hard reboot is in progress.

5 Close the Card Slot form.

Procedure 21-11 To perform an immediate 7450 ESS, 7710 SR, or 7750 SR software upgrade

The following conditions must be true before you attempt a device software upgrade:

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 8 for more information about scope of command roles.
- The FTP or secure FTP must be configured in the mediation policy for the NE. See chapter 13 for more information.

Warning — Devices, such as the 7450 ESS and 7750 SR, may require a firmware upgrade before a device software upgrade. To avoid a service outage, ensure that the device firmware version supports the software upgrade. See the device software Release Notes to obtain information about firmware and software version compatibility and about the firmware upgrade procedures.

Caution 1 — Alcatel-Lucent recommends that you establish a physical console session on the device that you need to upgrade. The console session allows you to monitor the upgrade and recover the device if the upgrade fails.

Caution 2 — Before you perform a software upgrade, read the device documentation. The software upgrade information in the device documentation takes precedence over this procedure.

Caution 3 — Before you perform an ISSU, review the appropriate device release notice for more information about the device software releases that support the ISSU. See section 21.1 for more information about the ISSU.

Note — If you downgrade a device software image, you must unmanage and delete the device before you perform the downgrade, as described in Procedure 13-12. Contact your Alcatel-Lucent technical support representative for information about downgrades.

1 Perform a preliminary check before you start the software upgrade.

   i Manually verify the software image file checksums.

   ii Verify that the device supports the new software.

   iii Verify that the compact flash drive has sufficient space for the software image files.

   iv For NEs with redundant CPMs, verify that the boot environments are synchronized by using the appropriate CLI command.

2 Back up the device configuration. See Procedure 21-4.

3 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

4 Choose the appropriate software upgrade policy.

Note — The 5620 SAM performs an upgrade on each NE to which the software upgrade policy is assigned and performs each upgrade according to the policy configuration.

5 Click on the Software Images tab button.

6 Choose a software image in the list and click on the Import button. The Open window appears.

7 Navigate to the folder that contains the software image, choose the software image and click on the Open button.

Note — You upgrade a Release 8.0 R1 or later 7450 ESS, 7710 SR, or 7750 SR using a common software image. The Product Name field displays Alcatel-SR/ESS-7XXX to indicate that the software image is a common software image.

The 5620 SAM verifies that only the required files for the upgrade are present and then imports the files from the specified directory into the 5620 SAM database. An entry for the image appears in the list.

If the directory does not contain only the required files, a dialog box appears. Go to step 8. Otherwise, go to step 9.

8 Perform the following:

i Click on the OK button.

ii Copy or move files to ensure that the directory contains only the files required for the upgrade.

iii Go to step 6.

9 Click on the Upgrade Sites button. A list of NEs appears. The list is filtered to display only the device type that is appropriate for the specified software image.

Note — If you select a common software image in step 7, only the 7450 ESS, 7750 SR, and 7710 SR devices are listed.

10 Choose one or more NEs in the list.

11 Click on the OK button. The software upgrade starts.

12 Click on the Software Upgrade Status tab button to view the progress of the upgrade.

13 Reboot the NE if the Auto-Reboot After Successful Activation parameter is disabled in the software upgrade policy. Perform one of the following actions.

Note 1 — Some device software upgrades do not require a reboot; for example, ISA-AA upgrades and ISSUs. See the device documentation for more information.

Note 2 — When you perform an ISSU, you can manually soft reset or hard reboot the IOMs or IMMs after an upgrade. A soft reset results in minimal downtime, but has restricted support. See Procedure 21-9 to perform a manual soft reset, or Procedure 21-10 to perform a manual hard reboot.

Note 3 — For MDAs, CMAs, and MCMs in a 7710 SR, Release 7.0 or later, after an ISSU, the system performs the required resets automatically.

Note 4 — When the IOMs are not manually soft reset or hard rebooted, the device performs a soft reset, if supported, after 2 h; otherwise, the device performs a hard reboot after 2 h.

a Use a Telnet or SSH CLI session.

i Right-click on the NE and choose NE Session→Telnet Session or NE Session→SSH Session.

ii Enter the following at the command prompt:

```
admin reboot now ↵
```

The NE reboots.

b Use the 5620 SAM GUI.

i Choose Equipment from the 5620 SAM navigation tree drop-down menu.

ii Navigate to the NE shelf object. The path is Routing→NE→Shelf.

iii Right-click on the shelf object and choose Reboot. The NE reboots.

Caution — Rebooting an NE that is in service is service-affecting. Ensure that the reboot activity occurs during a scheduled maintenance window.

14 Verify whether the upgrade is successful, as described in Procedure 21-20.

15 Use the FTP or SSH file browser to verify whether the transferred files and configurations are on the managed device. See Procedure 21-23 for information about using an FTP file browser. See Procedure 21-24 for information about using an SSH file browser.

16 Fully resynchronize the NE using the 5620 SAM GUI. See chapter 13 for information about resynchronizing an NE.

17 Perform upgrade verification tests, as required.

Procedure 21-12 To perform an immediate 7250 SAS software upgrade

The following conditions must be true before you attempt a device software upgrade:

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 8 for more information about scope of command roles.
- The FTP or secure FTP must be configured in the mediation policy for the NE. See chapter 13 for more information.

Caution 1 — Alcatel-Lucent recommends that you establish a physical console session on the device that you need to upgrade. The console session allows you to monitor the upgrade and recover the device in the event of an upgrade failure.

Caution 2 — Before you perform a software upgrade, read the device documentation. The software upgrade information in the device documentation takes precedence over this procedure.

Note — If you downgrade a device software image, you must unmanage and delete the device before you perform the downgrade, as described in Procedure 13-12. Contact your Alcatel-Lucent technical support representative for information about downgrades.

1 Perform a preliminary check before you begin the software upgrade.

   i Verify that the device supports the new software.

   ii Verify that the compact flash drive has sufficient space for the software image files.

2 Download the software description file to a directory on a 5620 SAM client station.

3 Load the software description file from step 2 into the TFTP server. See Procedure 21-18 for more information.

4 Back up the device configuration using the 5620 SAM Script Manager.

5 Start the upgrade procedure using the 5620 SAM Script Manager. Code 21-1 is an example of an upgrade script.

Code 21-1: 7250 SAS upgrade script example

```
#*
<velocityProperties>
  <tab><name>BiNOS Upgrade</name><tooltip>BiNOS Upgrade
Info</tooltip>
    <group><name>BiNOS Version</name><tooltip>BiNOS
Version</tooltip>
      <uiOrder>0</uiOrder>
      <property>
        <name>binos_version</name>
        <uiName>BiNOS Version:</uiName>
        <type>ComboBox</type>
        <default>BiNOS-7250-ES_v2_0_R7.0.Z</default>
        <uiOrder>0</uiOrder>
        <list>
          <item><name>BiNOS 7250ES Release
2.0-R5.2</name><value>BiNOS-7250-ES_v2_0_R5.2.Z</value></item>
          <item><name>BiNOS 7250ES Release
2.0-R6.1</name><value>BiNOS-7250-ES_v2_0_R6.1.Z</value></item>
          <item><name>BiNOS 7250ES Release
2.0-R7.0</name><value>BiNOS-7250-ES_v2_0_R7.0.Z</value></item>
        </list><tooltip>BiNOS Version</tooltip>
        <runtime>true</runtime>
      </property>
    </group>
  </tab>
</velocityProperties>
*#
config boot
   application $binos_version
   device local
   exit
dir Boot
config boot
```

```
show
exit
```

6 Reboot the NE.

7 Verify whether the upgrade is successful, as described in Procedure 21-20.

8 Use the FTP or SSH file browser to verify that the transferred files and configurations are on the device. See Procedure 21-23 for information about using an FTP file browser. See Procedure 21-24 for information about using an SSH file browser.

9 Remove obsolete software images from the device.

10 Fully resynchronize the NE using the 5620 SAM GUI. See chapter 13 for information about resynchronizing an NE.

11 Perform upgrade verification tests, as required.

Procedure 21-13 To perform an immediate OmniSwitch software upgrade

The directory structure that stores the image and configuration files is divided into two parts:

- The certified directory contains files that have been certified by an authorized user as the default files for the switch.
- The working directory contains files that may or may not be modified from the certified directory. The working directory is a holding place for new files. Files in the working directory must be tested before you commit them to the certified directory.

The following conditions must be present before you can perform a device software upgrade:

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 8 for more information about scope of command roles.
- FTP is configured in the mediation policy for the NE. See chapter 13 for more information.

Caution — Alcatel-Lucent recommends that you establish a physical console session on the device that you need to upgrade. The console session allows you to monitor the upgrade and recover the device in the event of an upgrade failure.

Warning — An OmniSwitch may require a firmware upgrade before a device software upgrade. To avoid a service outage, ensure that the device firmware version supports the software upgrade. See the device software Release Notes to obtain information about firmware and software version compatibility.

Perform the following procedure to perform an immediate software upgrade of an OmniSwitch. You can perform the following types of software upgrades:

- Image file
- Boot files
- FPGA files (OS 6855 only)

Note 1 — To perform an ISSU, which is supported only on the OS 9700E and OS 9800E, Release 6.4.2 R1, use the software upgrade window only.

Note 2 — The OS 9700E and OS 9800E NEs support standard software upgrades as described above, in addition to ISSU, with CMM images running on these NEs, and with minimal interruption of data traffic. Currently on OmniSwitch systems the introduction of new images necessitates a system reload which disrupts all data traffic during the reload process. As is the case for a CMM Takeover on current OS 9700E and OS 9800E based systems, data traffic loss should be limited to Layer 3 base traffic and no loss of Layer 2 data traffic should occur. Standard procedures can be used for a normal upgrade or an ISSU.

Note 3 — The operational restrictions and requirements are:

- Only OS 9700E and OS 9800E NEs CMM images have the ability to be upgraded.
- The following CMM images are ISSU capable: Jbase.img, Jsecu.img, Jadvrout.img and Jos.img.
- The OS 9700E and OS 9800E NE platforms must bet fully synchronized and certified.
- Target images must be loaded to the /flash/issu directory.
- Sufficient flash memory must be available for upgrade images.
- The CMM software build must be in the same major build tree branch, differing only in the build number (6.4.1.*.R01)
- NEs running an ‘R##’ build, such as 6.4.1.123.R01 do not support ISSU patches. The NE must first be upgraded to an ‘S##’ build such as 6.4.1.123.S01.

See Procedure 21-11 to perform an immediate software upgrade on a SR or ESS NE.

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

2 Perform one of the following:

a If you need to upgrade the image files or the image and boot files, go to step 3.

b If you need to upgrade the boot files, go to step 18.

c If you need to upgrade the FPGA files, go to step 32.

3 Choose the appropriate software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

4 Click on the Software Images tab button.

5 Click on the AOS Software tab button.

6 Choose a software image in the list.

7 Click on the Transfer to Sites button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected software image.

8 Choose one or more NEs in the list.

9 Click on the OK button. The selected software image file is uploaded to the working directory of the selected NEs.

10 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Wait until the files have been successfully transferred before going to step 11.

11 Click on the Reload working Sites button. A list of NEs opens.

12 Choose one or more NEs in the list.

13 Click on the OK button. The selected NEs reboots using the new software image that was uploaded to the working directory.

Caution — Rebooting an NE that is in service is service-affecting. Ensure that the reboot activity occurs during a maintenance window.

Note — Alcatel-Lucent recommends monitoring the switch to ensure that the reboot completes successfully.

14 Click on the Certify Sites button. A list of NEs opens.

Note — Only software that has been thoroughly validated as viable and reliable software should be copied to the certified directory. After you copy the software to the certified directory, you cannot recover a previous version of the image or configuration files.

15 Choose one or more NEs in the list.

16 Click on the OK button. The software image stored in the NE working directory is copied to the certified directory. The working directory and the certified directory are synchronized so that the same files are in both directories.

17 Perform one of the following:

a If you need to upgrade the boot files, go to step 26.

b If you need to upgrade the FPGA files, go to step 34.

c If you are only upgrading the image files, go to step 39.

18 Choose the appropriate software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

19 Click on the Software Images tab button.

20 Click on the AOS Software tab button.

21 Choose a software image in the list.

22 Click on the Transfer to Sites button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected software image.

23 Choose one or more NEs in the list.

24 Click on the OK button. The boot files are uploaded to the root directory of the selected NEs.

25 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Wait until the files have been successfully transferred before going to step 26.

26 Click on the Upgrade Boot files button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected files.

27 Choose one or more NEs in the list.

28 Click on the OK button. The boot files are upgraded on the selected NEs.

29 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Wait until the files have been successfully transferred before going to step 30.

30 Click on the Delete boot files button.

31 Perform one of the following:

a If you need to upgrade the FPGA files, go to step 34.

b If you do not need to upgrade the FPGA files, go to step 39.

32 Click on the Software Images tab button.

33 Click on the AOS Software tab button.

34 Choose a software image in the list.

35 Click on the Upgrade FPGA files button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected file type.

36 Choose one or more NEs in the list.

37 Click on the OK button. The selected FPGA files are uploaded to the root directory of the selected NEs.

38 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. After the FPGA files are successfully transferred, the selected NEs are rebooted.

39 Verify the upgrade success, as described in Procedure 21-20.

40 Close the Software Upgrade form.

Procedure 21-14 To perform an immediate 9500 MPR software upgrade

Perform the following procedure to download 9500 MPR software to one or more 9500 MPRs. After a successful software upgrade, perform Procedure 17-50 to activate the software on the 9500 MPR NE.

The 9500 MPR software is stored in two banks on a compact flash card:

- The committed bank contains the software that is currently running.
- The standby bank contains downloaded software that has not been activated or software that was active before the current committed software.

Note — A 9500 MPR that has never been upgraded only displays the committed bank. The standby bank does not appear until new software is downloaded for the first time.

You need a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package before you can perform a 9500 MPR software download. See chapter 8 for more information about scope of command roles.

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

2 Choose the appropriate software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

3 Click on the Software Images tab button.

4 Click on the MPR 9500 Software Images tab button.

5 Choose a software image file in the list. The image descriptor file has a .DSC file extension and must be present on the client system. Other software files do not need to be present on the client system.

6 Click on the Upgrade Sites button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected software image.

7 Choose one or more NEs in the list.

8 Click on the OK button. The software upgrade starts.

9 Click on the Software Upgrade Status tab button to view the status of the upgrade as it progresses. Verify that the files are successfully transferred before you go to step 10.

10 Close the Software Upgrade form.

Procedure 21-15 To schedule a software upgrade

Perform this procedure to schedule a device software upgrade on one or more managed NEs according to a software upgrade policy and a 5620 SAM schedule. See Procedure 21-11 for information about creating a software upgrade policy. See chapter 74 for information about creating schedules.

1 Perform Procedure 21-18 to import the required device software image.

2 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

3 Select the appropriate software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

4 Click on the Software Images tab button.

5 Select a software image in the list and click on the Schedule Upgrades button. The Select Sites form opens.

6 Choose an NE in the list and click on the OK button. You can choose multiple NEs. The Select Schedule form opens.

Note 1 — If no schedules are listed, you can create one for the upgrade. You cannot proceed unless a schedule is available. See chapter 74 for information about creating 5620 SAM schedules.

Note 2 — You cannot use a schedule in which the Ongoing parameter is enabled.

7 Select a schedule in the list and click on the OK button. A dialog box appears.

8 Click on the Yes button. The 5620 SAM schedules the upgrade.

9 Close the Software Upgrade form.

Procedure 21-16 To manage scheduled software upgrades

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

2 Click on the Software Upgrade Status tab button.

3 Click on the Scheduled Task button. The Scheduled Task form opens.

4 Configure the filter criteria and click on the Search button. A list of scheduled tasks is displayed.

5 Choose a scheduled software upgrade entry.

6 To view the scheduled task configuration, click on the Properties button. The Software Upgrade Scheduled Task form opens.

7 Administratively enable or disable the scheduled software upgrade, if required, by configuring the Administrative State parameter.

8 Click on the Properties button in the Schedule panel to view the schedule information, if required.

9 Click on the Properties button in the Task panel to view the 5620 SAM task information, if required.

10 Close the Software Upgrade Scheduled Task form. The Scheduled Task form reappears.

11 Click on the Task Action button and choose the appropriate option to turn up, shut down, or execute the task, if required.

12 Click on the Delete button to remove the scheduled task from the 5620 SAM, if required.

Note 1 — You cannot delete a scheduled task that is operationally enabled. Click on the Task Action button and choose Shut Down from the menu to operationally disable the scheduled task before you delete it.

Note 2 — The 5620 SAM does not delete a scheduled task after it runs; you must delete it manually. You cannot reuse a completed scheduled task.

13 Close the Scheduled Task form. The Software Upgrade form reappears.

14 Close the Software Upgrade form.

Procedure 21-17 To activate a device software image

Perform this procedure to activate a previously downloaded device software image on an NE. When the 5620 SAM activates an NE software image, it does the following:

- Updates the BOF with the new software image location
- Backs up the original boot.ldr at the location specified by the CFlash Backup Root Path parameter
- Replaces the currently active boot.ldr file with the new one
- Forces a "boot env synch" and a "config synch" on NEs that have redundant CPMs

Note 1 — If the BOF update fails, then the original boot.ldr file is put in place to align with the BOF specification.

Note 2 — The 5620 SAM ensures that the software image is present on the NE and valid for the device before it updates the BOF.

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

2 Click on the Software Upgrade Status tab button. A list of NEs is displayed.

3 Choose an NE in the list.

4 Click on the Software Images tab button. A list of software images on the selected NE is displayed.

5 Select a software image in the list and click on the Activate button. A dialog box appears.

6 Click on the Yes button. The software image is activated.

7 Verify the activation success, as described in Procedure 21-20.

8 Close the Software Upgrade form.

Procedure 21-18 To import device software image or description files to the 5620 SAM database

Perform this procedure to import a set of device software files or 9500 MPR software description files into the 5620 SAM database for use during device software upgrades.

1 Make the new device software files available to the 5620 SAM.

i If the device software files are compressed in an archive, for example, a TiMOS ZIP file, extract the files from the archive.

Note — Depending on the device type and version, the compressed files in a device software archive do not extract to a flat directory structure.

ii Copy or move the files to a directory that is accessible to the 5620 SAM.

Note 1 — The directory must contain a valid and complete set of device software files, and must not contain other files or subdirectories.

Note 2 — Alcatel-Lucent recommends that all OmniSwitch software image files, including any optional and boot files, are available in the specified directory for importing to the 5620 SAM database.

Note 3 — 9500 MPR NEs require only the software description (.DSC) files to be available for importing into the 5620 SAM database.

2 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

3 Click on the Software Images tab button.

4 Click on the appropriate tab button for the type of NE that you need to upgrade.

5 Click on the Import button. The Open window appears.

6 Navigate to folder that contains the software image, choose the software image, and click on the Open button. The software image appears in the list.

Note — You upgrade a Release 8.0 R1 or later 7450 ESS, 7710 SR, or 7750 SR using a common software image. The Product Name field displays Alcatel-SR/ESS-7XXX to indicate that the software image is a common software image.

The 5620 SAM verifies that only the required files are present and then imports the files from the specified directory into the 5620 SAM database. An entry for the image appears in the list.

If the directory does not contain only the required files, a dialog box appears. Go to step 7. Otherwise, go to step 8.

7 Perform the following:

i Click on the OK button.

ii Copy or move files, as required, to ensure that the directory contains only the files required for the upgrade.

iii Go to step 5.

8 Close the Software Upgrade form.

Procedure 21-19 To export a device software image from the 5620 SAM database to a file system

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

2 Click on the Software Images tab button.

3 Perform one of the following:

a To export SR device software images, go to step 4

b To export OmniSwitch software images click on the AOS Software tab button. Go to step 4.

4 Choose an image from the displayed list.

5 Click on the Export button. A file navigator form opens.

6 Use the form to specify the directory that is to contain the exported software image and click on the OK button. The software image is saved to files in the specified directory.

7 Close the Software Upgrade form.

Procedure 21-20 To view the deployment, backup/restore, or software upgrade status of an NE

1 Perform one of the following actions.

a Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu to view deployment status. The Deployment form opens with the Incomplete Deployments tab displayed.

i Double-click on a deployment in the list. The deployment properties form opens.

ii View the deployment status.

b Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu to view the backup or restore status. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

i Click on the Backup/Restore Status tab button. The Restore State column of the backup or restore is: Transferring Files, Pending, Reboot, CPM Sync and Reboot, Success, Not Attempted, Save Config, or Failure. The timestamp is also displayed.

ii Double-click on a row in the list to display information about the backup or restore operation. You can click on the General, Backups, Configuration Saves, and Faults tab buttons.

Note — When you click on the Backups tab button, the date and time in the Config File Version column corresponds to the date and time for the Last Boot Cfg Version on the NE.

c Choose Administration→NE Maintenance→Software Upgrade to view the software upgrade status. The Software Upgrade form opens.

i Click on the Software Upgrade Status tab button. A list of NEs displayed.

ii Double-click on an NE in the list to view information about the upgrade. The Software Upgrade Status form opens.

iii Close the Software Upgrade Status form.

2 Close the form.

Procedure 21-21 To view the accounting statistics collection status of an NE

1 Choose Tools→Statistics→Accounting Retrieval Status from the 5620 SAM menu. The Accounting Retrieval Status form opens with a list of managed NEs displayed.

2 Select an NE in the list and click on the Properties button. The Accounting Retrieval Status (View) form opens.

3 View the statistics collection information for the NE.

4 Close the Accounting Retrieval Status (View) form.

5 Close the Accounting Retrieval Status form.

Procedure 21-22 To view the trap metrics information

1 Choose Tools→Statistics→Trap Metrics Information from the 5620 SAM main menu. The Trap Metrics Information form opens and lists the NEs that generated the most traps during the last collection interval. The collection interval is indicated by the Start Collection Period and End Collection Period values at the top of the form.

Note — The number of displayed NEs is limited by the metrics configuration in the nms-server.xml file.

2 Click on the Search button to refresh the trap metrics information. The list and collection interval values are updated.

3 Close the Trap Metrics Information form.

Procedure 21-23 To view an NE file system using an FTP file browser

Perform this procedure to browse and list the files on a managed NE. You require FTP user-account privileges on the NE for access to the NE file system. See chapter 12 for information about enabling FTP access for an NE user account.

1 Initiate an FTP file browser session.

a Use the 5620 SAM main menu.

i Choose Tools→NE Sessions→FTP File Browser. The FTP File Browser form opens.

ii Enter the IP address of the NE that you want to browse in the field at the top of the form.

iii Press Enter or click on the Connect button. The Enter the Username and Password form opens.

Note — When you use the 5620 SAM main menu to open a file-browser session, you are not restricted to the original NE; you can use the same form to connect to other NEs. This is useful when several NEs are to be browsed in succession.

b Use the Software Upgrade Policy form.

i Choose Administration→NE Maintenance→Software Upgrade. The Software Upgrade form opens with the Software Policy tab displayed.

ii Select a policy in the list and click on the Properties button. The Software Upgrade Policy (Edit) form opens.

iii Click on the FTP File Browser button. The FTP File Browser form opens.

iv Enter the IP address of the NE that you want to browse in the field at the top of the form.

v Press Enter or click on the Connect button. The Enter the Username and Password form opens.

c Use the contextual menu for an NE.

i Select an NE icon in the 5620 SAM network navigation tree or topology map.

ii Right-click on the NE icon and choose NE Sessions→File Browser from the contextual menu. The FTP File Browser form opens, then displays the Enter the Username and Password form.

d Use the properties form of an NE.

i Select an NE icon in the 5620 SAM network navigation tree or topology map.

ii Right-click on the NE icon and choose Properties from the contextual menu. The Network Element (Edit) form opens.

iii Click on the File Browser button. The FTP File Browser form opens, then displays the Enter the Username and Password form.

e Use the topology view of a service.

i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

ii Configure the filter criteria.

iii Choose a service from the list.

iv Click on the Topology View button. A Topology View dialog box appears.

v Click on the Yes button. The Service Topology map opens.

vi Right-click on a managed device and choose NE Sessions→File Browser from the contextual menu. The FTP File Browser form opens to display the Enter the Username and Password form.

Note — You can open a file browser session on only one managed device at a time.

f Use the Components tab of a service management form.

i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

ii Configure the filter criteria.

iii Choose a service from the list.

iv Click on the Properties button.

v The *Service* (Edit) form opens.

where *Service* is the type of service selected

vi Click on the Components tab button.

vii Right-click on a service site and choose NE Sessions→File Browser from the contextual menu. The FTP File Browser form opens to display the Enter the Username and Password form.

Note — You can open a file browser session on only one service site at a time.

g Use the Sites tab of a service.

i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

ii Configure the filter criteria.

iii Choose a service from the list.

iv Click on the Properties button.

v The *Service* (Edit) form opens.

where *Service* is the type of service selected

vi Click on the Sites tab button.

vii Choose a site from the list.

viii Click on the NE Sessions button and choose File Browser from the contextual menu. The FTP File Browser form opens to display the Enter the Username and Password form.

Note — You can open a file browser session to only one service site at a time.

h Use the NE alarm contextual menu.

i Select an NE alarm in the 5620 SAM alarm window.

ii Right-click on the alarm and choose NE Sessions→File Browser. The FTP File Browser form opens, then displays the Enter the Username and Password form.

Note — When you use the 5620 SAM main menu or the Software Upgrade form to open a file-browser session, you are not restricted to the original NE; you can use the same form to connect to other NEs. This is useful when several NEs are to be browsed in succession.

2 Enter the user name and password of a user account with FTP access privileges on the NE and click on the OK button or press Enter. If the NE accepts the credentials, the form lists the contents of the NE.

<DIR> in the Type column indicates a directory. The file path to the current directory is displayed in the Path field.

Note — On an NE with redundant CPMs, the form lists the contents of the cf3 device on the active CPM.

You can browse the cf3 device on the standby CPM by specifying cf3-B:\ in the Path field.

3 If the login attempt fails with the supplied credentials, a dialog box appears. Click on the OK button to close the dialog box, check the credentials and repeat step 2.

4 Sort the list entries by a specific attribute, if required, by clicking on the column heading for the attribute. Clicking again on the column heading reverses the sort order.

5 Reorder the columns, if required, by clicking on a column heading and dragging the column to a new position.

6 Navigate the file system as required. Perform one of the following actions to open a directory and list the contents.

a Double-click on the directory row in the list.

b Select the directory row and press <CTRL>O.

c Type the path to the directory in the Path field and click on the Go button or press Enter.

7 If you opened the browser using the 5620 SAM main menu, you can browse another NE file system using the same form, if required.

i Click on the Disconnect button to end the browsing session.

ii Go to step 1 a ii.

8 Close the FTP File Browser form.

Procedure 21-24 To view an NE file system using an SSH file browser

Perform this procedure to browse and list the contents of a managed NE using a secure file browser. You require console and SSH user-account privileges on the NE for access to the NE file system, and an SSH server must be configured on the NE. See chapter 12 for information about enabling console or SSH access for an NE user account. See chapter 13 for information about configuring an SSH server for an NE.

1 Initiate an SSH file browser session.

a Use the 5620 SAM main menu.

i Choose Tools→NE Sessions→SSH File Browser. The SSH File Browser form opens.

ii Enter the IP address of the NE that you want to browse in the field at the top of the form.

iii Press Enter or click on the Connect button. The Enter the Username and Password form opens.

b Use the Software Upgrade Policy form.

i Choose Administration→NE Maintenance→Software Upgrade. The Software Upgrade form opens with the Software Policy tab displayed.

ii Select a policy in the list and click on the Properties button. The Software Upgrade Policy (Edit) form opens.

iii Click on the SSH File Browser button. The SSH File Browser form opens.

iv Enter the IP address of the NE that you want to browse in the field at the top of the form.

v Press Enter or click on the Connect button. The Enter the Username and Password form opens.

c Use the contextual menu for an NE.

i Select an NE icon in the 5620 SAM network navigation tree or topology map.

ii Right-click on the NE icon and choose NE Sessions→File Browser from the contextual menu. The SSH File Browser form opens, then displays the Enter the Username and Password form.

d Use the properties form of an NE.

i Select an NE icon in the 5620 SAM network navigation tree or topology map.

ii Right-click on the NE icon and choose Properties from the contextual menu. The Network Element (Edit) form opens.

iii Click on the File Browser button. The SSH File Browser form opens, then displays the Enter the Username and Password form.

e Use the NE alarm contextual menu.

i Select an NE alarm in the 5620 SAM alarm window.

ii Right-click on the alarm and choose NE Sessions→File Browser. The SSH File Browser form opens, then displays the Enter the Username and Password form.

Note — When you use the 5620 SAM main menu or the Software Upgrade form to open a file-browser session, you are not restricted to the original NE; you can use the same form to connect to other NEs. This is useful when several NEs are to be browsed in succession.

2 Enter the user name and password of a user account with FTP and SSH access privileges on the NE and click on the OK button or press Enter. If the NE accepts the credentials, the form lists the contents of the NE.

<DIR> in the Type column indicates a directory. The file path to the current directory is displayed in the Path field.

Note — On an NE with redundant CPMs, the form lists the contents of the cf3 device on the active CPM.

You can browse the cf3 device on the standby CPM by specifying cf3-B:\ in the Path field.

3 If the login attempt fails with the supplied credentials, a dialog box appears. Click on the OK button to close the dialog box, check the credentials and repeat step 2.

4 Sort the list entries by a specific attribute, if required, by clicking on the column heading for the attribute. Clicking again on the column heading reverses the sort order.

5 Reorder the columns, if required, by clicking on a column heading and dragging the column to a new position.

6 Navigate the file system as required. Perform one of the following actions to open a directory and list the contents.

a Double-click on the directory row in the list.

b Select the directory row and press <CTRL>O.

c Type the path to the directory in the Path field and click on the Go button or press Enter.

7 If you opened the browser using the 5620 SAM main menu or from the Software Upgrade form, you can browse another NE file system using the same form, if required.

i Click on the Disconnect button to end the browsing session.

ii Go to step 1 a ii.

8 Close the SSH File Browser form.

22 — Card migration

22.1 Card migration management overview

Release 6.1 R1 or later of the 7450 ESS and 7750 SR support the IOM 3. You can use a 5620 SAM GUI utility called the Card Migration Event Manager to facilitate the transition to an IOM 3 on one or more NEs. The Card Migration Event Manager transfers the existing IOM and MDA configurations to new modules with minimal service interruption.

The 5620 SAM Card Migration Event Manager can do the following:

- Upgrade from an IOM 1 or IOM 2 to an IOM3 while retaining the same MDAs.
- Upgrade from one MDA type to a newer MDA type that has compatible features.
- Upgrade an IOM and the associated MDAs in one operation.

You can perform an immediate migration, or preconfigure one or more migration events for later execution. A migration event can include an NE reboot to put the new hardware configuration into effect immediately after the migration. You can upgrade multiple IOMs and MDAs in one operation to limit the number of required NE reboots to one.

During a migration event, the 5620 SAM identifies the configured objects that are bound to the IOM or MDA, deletes the objects, and then creates the objects on the new IOM or MDA. The old and new configurations are saved in the 5620 SAM database until the migration completes successfully. The 5620 SAM preserves the statistics data and alarm information that is associated with each object.

Restrictions

The following restrictions apply to 5620 SAM card migration event management:

- **General**
  - Only the 5620 SAM admin user, or a user with an assigned administrator scope of command role, can create, modify, or execute a migration event.
  - The migration functions are not available to 5620 SAM OSS clients.
  - You may need to re-enable SNMP on an NE after the NE reboots following a migration event.
- **IOM-specific**
  - An IOM downgrade, for example, a migration from an IOM 3 to an IOM 2, is not supported.
- **MDA-specific:**
  - You cannot migrate an empty MDA slot to an MDA.
  - MDA migration is limited to MDAs of the same physical transmission type; for example, migration from a SONET MDA to an Ethernet MDA is not supported.
  - You cannot upgrade an MDA that is integrated with an IOM, for example, an IMM.
  - For MDAs, you can migrate only to an MDA of similar capacity that has the same or a greater number of ports.

The 5620 SAM raises an alarm during a migration event if a target NE is unreachable. After a migration event, the 5620 SAM raises an alarm to indicate migration success or failure.

Table 22-1 lists the supported MDA migration types.

Table 22-1 Supported MDA migration types

Current MDA	MDAs supported by migration
10 x 1-Gig Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
5 x 1-Gig Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
1 x 10-Gig Ethernet	4 x 10Gig Extended Performance XFP 2 x 10Gig Extended Performance XFP 1 x 10Gig Extended Performance SFP
20 x 100 Ethernet Fx	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
20 x 10/100/1000 Ethernet Tx	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
2 x 10-Gig Ethernet XFP	2 x 10Gig Extended Performance XFP 4 x 10Gig Extended Performance XFP
20 x 10/100/1000 Ethernet SFP	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
1 x 10-gig Ethernet XFP	4 x 10GigExtended Performance XFP 2 x 10Gig Extended Performance XFP 1 x 10Gig Extended Performance XFP
5 x 10/100/1000	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
10 x 10/100/1000 Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
60 x 10/100 Ethernet	48 x 10/100/1000 Ethernet Extended Performance TX

22.2 Workflow to manage card migration

The following is the sequence of high-level actions required to manage card migration.

1 Use the 5620 SAM to back up the device configuration of each target NE.

Note — When you attempt a migration on an NE that does not have a recent configuration backup in the 5620 SAM database, the 5620 SAM raises an alarm and the migration fails.

A recent configuration backup is a backup that occurs after the latest configuration save on the NE.

See chapter 21 for information about performing NE backups.

2 Specify the target NEs for the migration.

3 Specify the IOMs to upgrade on the target NEs.

4 Specify the MDAs to upgrade on the target IOMs.

5 Perform one of the following.

a Execute the migration event immediately.

b Save the migration event for later execution.

6 Check to ensure that each task in the migration event is successful.

7 Execute the saved migration event, if required.

8 Check to ensure that each task in the saved migration event is successful.

22.3 Card migration management procedures

Use the following procedures to perform card migration event management tasks.

Procedure 22-1 To create a card migration event

1 Choose Tools→Card Migration Event Manager from the 5620 SAM main menu. The Card Migration Event Manager form opens.

2 Click on the Create button. The Card Migration Event (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Description
- Additional Information
- Auto Reboot

4 Click on the NE Migration Candidates tab button.

5 Click on the Add button. The Select Network Elements - Card Migration Event form opens.

6 Select one or more NEs in the list and click on the OK button. The Select Network Elements - Card Migration Event form closes and the NEs are listed on the Card Migration Event (Create) form.

7 Select one or more NEs in the list and click on the Properties button. The Network Element Migration Candidates form opens.

8 Configure the Auto Reboot parameter.

9 Click on the Ok button. The Network Element Migration Candidates form closes, and a dialog box appears.

10 Click on the OK button.

11 Click on the Card Migration Candidates tab button.

12 Click on the Add button. The Select Cards - Card Migration Event form opens.

13 Select one or more cards in the list and click on the OK button. The Select Cards - Card Migration Event form closes and the cards are listed on the Card Migration Event (Create) form.

14 Select one or more cards in the list and click on the Properties button. The Migration Details (Create) form opens.

15 Configure the New Type parameter in the IOM panel, if required.

16 Configure the New Type parameter in the MDA 1 panel, if required.

17 Configure the New Type parameter in the MDA 2 panel, if required.

18 Click on the OK button. The Migration Details (Create) form closes, and a dialog box appears.

19 Click on the OK button.

20 To execute the migration event immediately, perform the following steps. Otherwise, you can execute the migration later by performing Procedure 22-2.

i Use the 5620 SAM to back up the device configuration of each target NE.

Note — When you attempt a migration on an NE that does not have a recent configuration backup in the 5620 SAM database, the 5620 SAM raises an alarm and the migration fails.

A recent configuration backup is a backup that occurs after the latest configuration save on the NE.

See chapter 21 for information about performing NE backups.

ii Click on the Apply button. The 5620 SAM saves the card migration event configuration.

iii Click on the General tab to display the Status indicator.

iv Click on the Initiate Migration button. A dialog box appears.

v Click on the Yes button. The 5620 SAM starts to migrate the specified cards.

vi Monitor the card migration as it progresses by viewing the Status indicator on the form. The status can be one of the following:

- Awaiting manual reboot to complete migration
- Failed - Latest configuration not available
- Failed - Unable to migrate configuration
- Failed - Unable to reboot network element
- Failed - Unable to transfer migrated configuration
- Migration completed
- Not Started
- Rebooted network element
- Started
- Swap failed
- Swap failed on some network elements

21 Click on the OK button. The Card Migration Event (Create) form closes.

22 Close the Card Migration Event Manager form.

Procedure 22-2 To execute a saved card migration event

1 Use the 5620 SAM to back up the device configuration of each target NE.

Note — When you attempt a migration on an NE that does not have a recent configuration backup in the 5620 SAM database, the 5620 SAM raises an alarm and the migration fails.

A recent configuration backup is a backup that occurs after the latest configuration save on the NE.

See chapter 21 for information about performing NE backups.

2 Choose Tools→Card Migration Event Manager from the 5620 SAM main menu. The Card Migration Event Manager form opens.

3 Configure the filter criteria and click on the Search button. A list of card migration events is displayed.

4 Select a card migration event and click on the Properties button. The Card Migration Event (Edit) form opens with the General tab displayed.

5 Click on the Initiate Migration button. A dialog box appears.

6 Click on the Yes button. The 5620 SAM starts to migrate the specified cards.

7 Monitor the card migration as it progresses by viewing the Status indicator on the form. The status can be one of the following:

- Awaiting manual reboot to complete migration
- Failed - Latest configuration not available
- Failed - Unable to migrate configuration
- Failed - Unable to reboot network element
- Failed - Unable to transfer migrated configuration
- Migration completed
- Not Started
- Rebooted network element
- Started
- Swap failed
- Swap failed on some network elements

8 Click on the OK button. The Card Migration Event (Create) form closes.

9 Close the Card Migration Event Manager form.

Procedure 22-3 To delete a card migration event

1 Choose Tools→Card Migration Event Manager from the 5620 SAM main menu. The Card Migration Event Manager form opens.

2 Configure the filter criteria and click on the Search button. A list of card migration events is displayed.

3 Select a card migration event and click on the Delete button. A dialog box appears.

4 Click on the Yes button. The 5620 SAM deletes the card migration event.

5 Close the Card Migration Event Manager form.

23 — TCA

23.1 TCA overview

You can create policies to raise 5620 SAM alarms based on managed-object utilization. When the utilization of an object such as an interface reaches a specified threshold, the 5620 SAM alerts GUI operators using a threshold-crossing alarm, or TCA, based on policy specifications.

A TCA policy includes the following:

- the direction of traffic flow to monitor
- the objects that are associated with the policy
- rules that define properties such as the rising and falling thresholds, and the alarm severity

Note — A TCA is not self-clearing. The 5620 SAM clears a TCA only when the TCA policy contains a falling-threshold rule in addition to a rising-threshold rule, and the alarm severity in the falling-threshold rule is set to cleared.

To enable TCA on an object, you must enable collection of performance statistics on the object. To determine whether object utilization exceeds a TCA policy threshold, the 5620 SAM compares the utilization value at each statistics collection to the threshold values in the associated TCA policy.

The 5620 SAM TCA function raises an alarm when a utilization threshold is initially crossed. Rather than raise a new alarm for each successive threshold-crossing event associated with a TCA policy, the 5620 SAM changes the severity of the initial alarm based on the rules defined in the policy.

In the 5620 SAM client GUI, you can associate a TCA policy with a managed object from the TCA policy configuration form, or from the object properties form. You can associate one TCA policy with multiple objects.

TCA configuration example

The following example describes the 5620 SAM configuration required to raise a TCA, adjust the alarm severity, and clear the alarm, based on the following utilization specifications:

- Raise a minor alarm if utilization is between 60% and 69%.
- Change the alarm severity to major if utilization rises to between 70% and 79%.
- Change the alarm severity to critical if utilization rises to 80% or higher.
- Change the alarm severity to major if utilization falls below 80%.
- Change the alarm severity to minor if utilization falls below 70%.
- Clear the alarm if utilization falls below 60%.

The following are the TCA rules and associated parameter values required to implement the example alarm behavior:

Rule to raise minor alarm for 60% or higher utilization:

- Alarm Severity—minor
- Threshold (%)—60
- Threshold Direction—Rising Above

Rule to change alarm severity to major for 70% or higher utilization:

- Alarm Severity—major
- Threshold (%)—70
- Threshold Direction—Rising Above

Rule to change alarm severity to critical for 80% or higher utilization:

- Alarm Severity—critical
- Threshold (%)—80
- Threshold Direction—Rising Above

Rule to change alarm severity to major if utilization falls below 80%:

- Alarm Severity—major
- Threshold (%)—80
- Threshold Direction—Falling Below

Rule to change alarm severity to minor if utilization falls below 70%:

- Alarm Severity—minor
- Threshold (%)—70
- Threshold Direction—Falling Below

Rule to clear alarm if utilization falls below 60%:

- Alarm Severity—cleared
- Threshold (%)—60
- Threshold Direction—Falling Below

23.2 Workflow to configure TCA

1 Enable performance statistics collection on the object that is to be monitored. For example, Table 23-1 lists the port statistics policy objects required to enable TCA on a network interface or physical link.

Table 23-1 Port statistics policy objects for TCA

Statistics policy type	MIB	MIB entry	Monitored class
NE MIB	IF-MIB	ifEntry	—
Specific MIB	IF-MIB	ifEntry	equipment.PhysicalPort

2 Create a TCA policy and apply it to one or more managed objects.

3 Apply the TCA policy to additional objects later, if required, using the object properties forms.

23.3 TCA management procedures

The following procedures describe how to manage TCA policies.

Procedure 23-1 To create a TCA policy

Perform this procedure to create a TCA policy for monitoring object utilization.

1 Choose Tools→TCA Policies from the 5620 SAM main menu. The Manage TCA Policies form opens.

2 Click on the Create button. The UtilizationTCA (Create) form opens.

3 Configure the parameters:

- Policy ID
- Auto-Assign ID
- Displayed Name
- Flow Direction

4 Click on the Rules tab button.

5 Click on the Create button. The UtilizationTCARule (Create) form opens.

6 Configure the parameters:

- Rule ID
- Auto-Assign ID
- Displayed Name
- Alarm Severity
- Threshold (%)
- Threshold Direction

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The UtilizationTCARule (Create) form closes, and the rule is listed on the UtilizationTCA (Create) form.

9 Repeat steps 5 to 8 to create another rule, if required.

Note — You cannot create two rules that have the same Threshold (%) and Threshold Direction values.

10 Click on the Apply button. A dialog box appears.

11 Click on the Yes button. The form name changes to UtilizationTCA (Edit).

12 To apply the TCA policy to one or more objects, perform the following steps.

i Click on the Monitored Objects tab button.

ii Click on the Add button. The Select Interface Stats (Physical Equipment) for UtilizationTCA (Edit) form opens.

iii Select an object from the Select Object Type drop-down list and click on the Search button. A list of objects is displayed.

iv Select one or more objects in the list and click on the OK button. The Select Interface Stats (Physical Equipment) for UtilizationTCA (Edit) form closes, and the object is listed on the UtilizationTCA (Edit) form.

v Click on the Apply button. A dialog box appears.

vi Click on the Yes button.

13 Close the UtilizationTCA (Edit) form.

14 Close the Manage TCA Policies form.

Procedure 23-2 To apply a TCA policy to objects using the object properties forms

Perform this procedure to apply an existing TCA policy to one or more objects from the object properties form.

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Select an object, for example, Port or Physical Link, from the Select Object Type drop-down list, and click on the Search button. A list of objects is displayed.

3 Select one or more objects in the list and click on the Properties button. The properties form for the object opens.

4 If the object is a Physical Link, perform the following steps.

i Click on the Endpoint A TCA tab button.

ii Click on the Add button. The Select UtilizationTCA form opens.

iii Select a TCA policy in the list and click on the OK button. The TCA policy is listed on the object properties form.

iv Click on the Endpoint B TCA tab button.

v Click on the Add button. The Select UtilizationTCA form opens.

vi Select a TCA policy in the list and click on the OK button. The TCA policy is listed on the object properties form.

vii Go to step 8.

5 Click on the TCA tab button.

6 Click on the Add button. The Select UtilizationTCA form opens.

7 Select a TCA policy in the list and click on the OK button. The TCA policy is listed on the object properties form.

8 Close the object properties form.

9 Close the Manage Equipment form.

Procedure 23-3 To delete a TCA policy

Perform this procedure to delete a TCA policy.

1 Choose Tools→TCA Policies from the 5620 SAM main menu. The Manage TCA Policies form opens.

2 Click on the Search button. A list of TCA policies is displayed.

3 Select one or more TCA policies in the list and click on the Delete button. The 5620 SAM deletes the TCA policies.

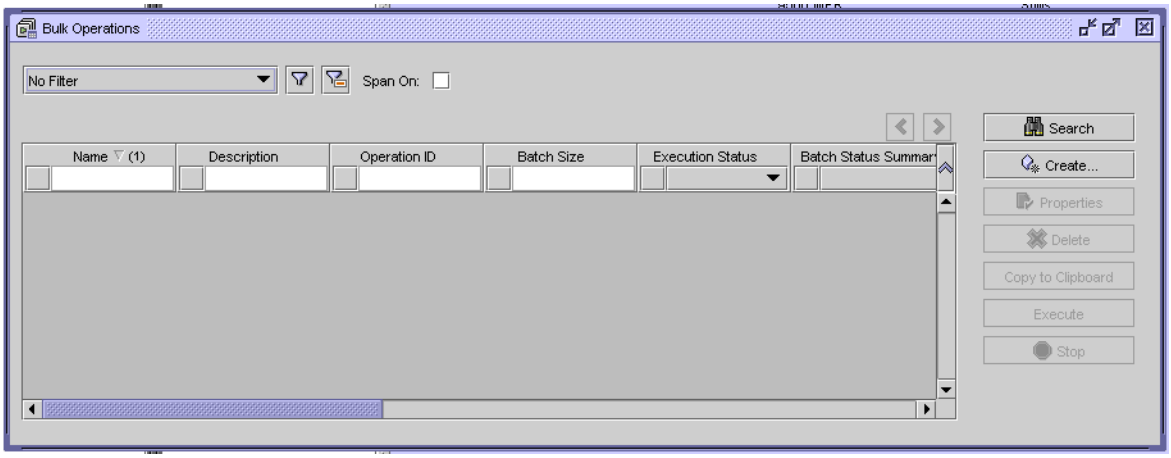
4 Close the Manage TCA Policies form.

24 — Bulk operations

24.1 Bulk operations overview

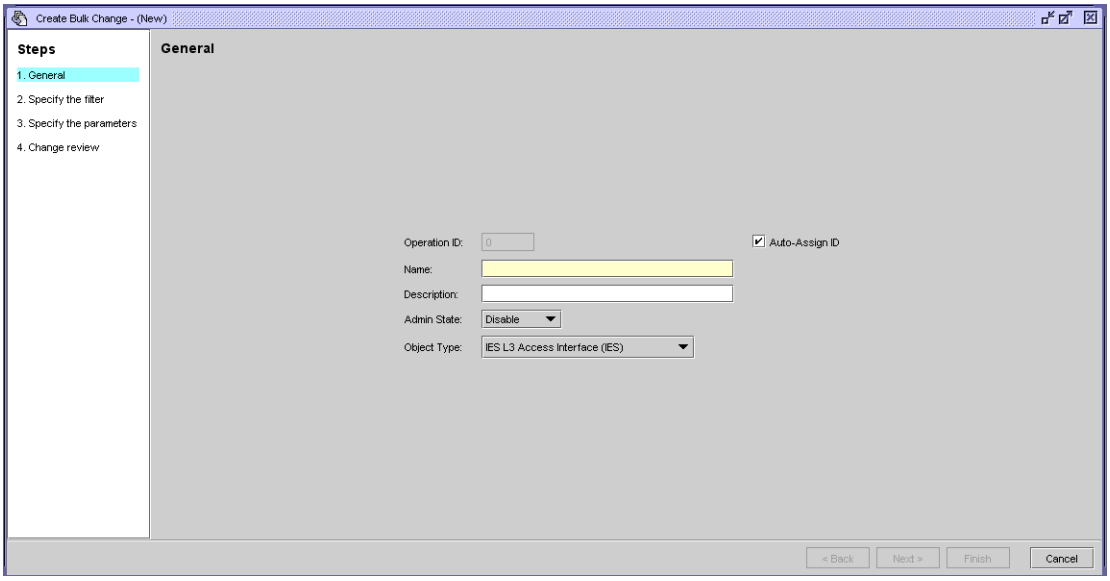
The 5620 SAM bulk operations function allows you to create bulk changes to modify a large amount of information. Bulk changes may be deployed to NEs or restricted to the 5620 SAM. You can create a bulk change using the Bulk Operations form, as shown in Figure 24-1.

Figure 24-1 Bulk Operations form



Creating a bulk change opens the Create Bulk Change form, as shown in Figure 24-2.

Figure 24-2 Create Bulk Change form



You specify the objects that the bulk change is to modify by setting filter and attribute definitions. Figure 24-3 shows the Specify the filter form.

Figure 24-3 Specify the filter form

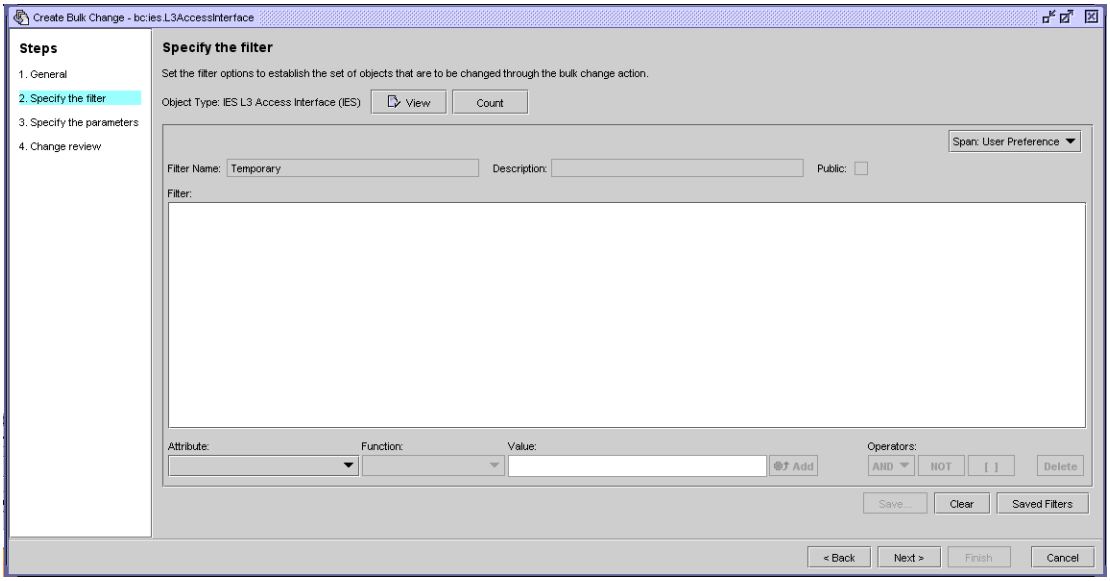
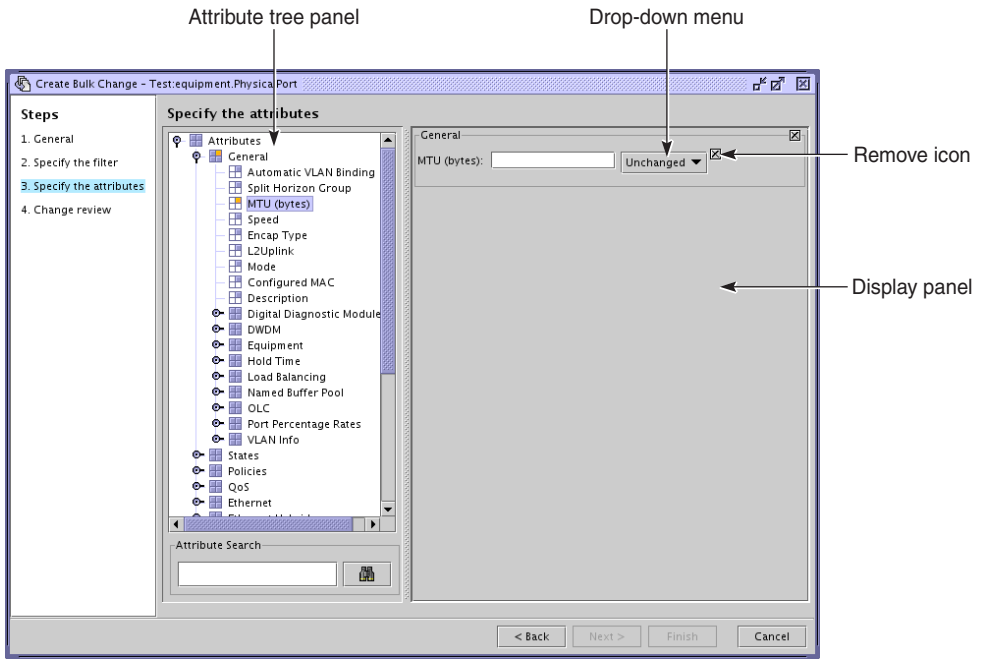


Figure 24-4 shows the Specify the attributes form.

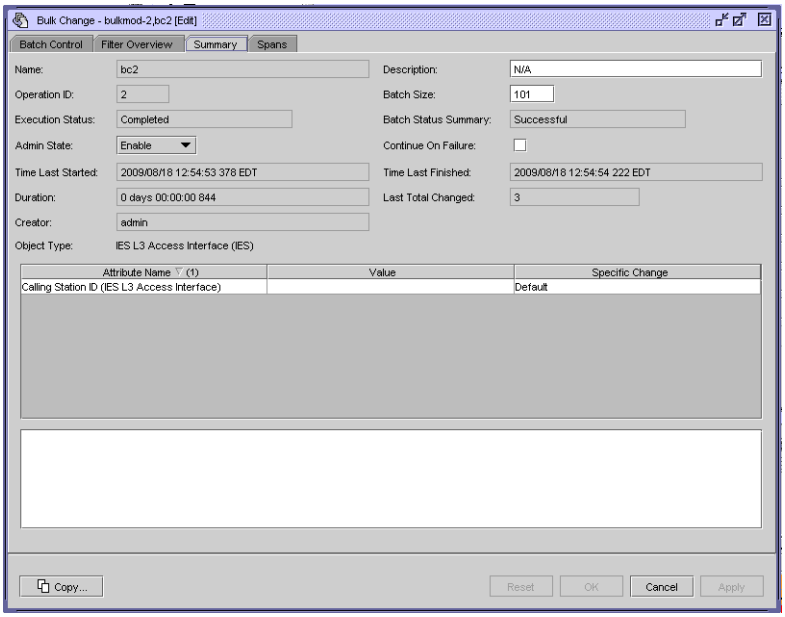
Figure 24-4 Specify the attributes form



20506

After you create a bulk change, you can modify it and generate batches using the Bulk Change configuration form, as shown in Figure 24-5.

Figure 24-5 Bulk Change configuration form



A bulk change can contain thousands of target objects. These objects, referred to as batch items, are grouped into batches for efficient bulk change execution. An operator can execute an entire bulk change or individual batches.

You should regenerate batches each time you execute a bulk change to ensure that each target object that matches the bulk change filter is modified.

If one or more of the batch items fail to change during a bulk change operation, the Batch Status and the Batch Status Summary parameters help identify the items. You can also use the Task Manager to view information about a batch.

24.2 Workflow to manage bulk operations

1. Create a bulk change.
2. Modify the bulk change, if required.
3. Generate batches for the bulk change.
4. Execute one or more batches in the bulk change.
5. View the bulk change execution results.

24.3 Bulk operations procedures

Use the following procedures to manage the 5620 SAM bulk operations.

Procedure 24-1 To create a bulk change

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Open the Create Bulk Change form by performing one of the following steps.

   a Click on the Create button.

   b To create a bulk change by copying values from an existing bulk change, perform the following steps.

      i Configure the filter criteria and click on the Search button. A list of bulk operations appears.

      ii Choose the bulk change from the list and click on the Properties button. The Bulk Change configuration form opens.

      iii Click on the Copy button.

3 Configure the parameters, if required:

   - Operation ID
   - Auto-Assign ID
   - Name
   - Description
   - Admin State
   - Object Type

   The Operation ID parameter is configurable when the Auto-Assign ID parameter is disabled.

4 Click on the Next button. The Specify the filter form opens.

5 Configure the filter criteria, as required. Creating a filter that contains the attributes that you want to change can limit the number of objects generated for the bulk change.

6 Click on the Count button to determine the number of network objects that are affected based on the filter.

7 Click on the View button to list the target objects. The Filtered List form opens.

8 Click on the Search button. A list of target objects is displayed.

9 Click on the Next button. The Specify the attributes form opens.

10 Double-click on the attribute or attribute group in the attribute tree panel that you want to include in the bulk change. The attribute or attribute group appears in the display panel.

11 If you included an attribute or attribute group that you want to exclude from the bulk change, you can remove it by clicking on the Remove icon in the display panel.

12 Perform one of the following on each listed attribute, as required.

a Enter a value in the attribute field. The drop-down menu changes from Unchanged to Set, which means that the attribute changes to the new value when you execute the bulk change.

b Choose Default from the drop-down menu to specify that the attribute is to change to the default value when you execute the bulk change.

c Choose Clear from the drop-down menu. Depending on the object type, the attribute value is cleared or set to the default value when you execute the bulk change.

13 Click on the Next button. The Change review form opens.

14 Configure the parameters, if required:

- Batch Size
- Continue on Failure
- Admin State

15 Click on the Finish button.

16 Click on the Close button. The Create Bulk Change form closes.

Procedure 24-2 To modify a bulk change

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change from the list and click on the Properties button. The Bulk Change configuration form opens with the Batch Control tab displayed.

4 Click on the Summary tab button.

5 Modify the attributes, if required:

- Description
- Batch Size
- Admin State
- Continue on Failure

6 Click on the Spans tab button and specify a span, if required.

7 Click on the OK button. The Bulk Change configuration form closes.

8 Close the Bulk Operations form.

Procedure 24-3 To execute a bulk change

Note 1 — You can only execute one bulk change at a time. All other bulk changes are queued.

Note 2 — You can only generate batches for one bulk change at a time.

Note 3 — You cannot generate batches when a bulk change is executing.

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change from the list and perform one of the following.

a If the bulk change contains batches, click on the Execute button to execute all of the batches.

Note — Changes made to the network after the batches were generated are not affected by the bulk change batches.

b If the bulk change does not contain batches, or you want to regenerate the batches, perform the following.

i Click on the Properties button. The Bulk Change configuration form opens.

ii If the Generate Batches button is dimmed, perform the following:

- Click on the Summary tab button.
- Set the Admin State parameter to Enable.
- Click on the Batch Summary tab.

iii Click on the Generate Batches button. The batches are generated and listed on the form.

iv To execute only specific batches, choose one or more batches from the list and click on the Execute Selected button.

v To execute all of the batches, click on the Execute All button.

A dialog box appears. You can modify the bulk change confirmation message behavior from the User Preferences form.

4 Click on the Yes button. The 5620 SAM executes the bulk change.

Procedure 24-4 To enable or disable the display of bulk change confirmation messages

Perform this procedure to specify whether the 5620 SAM displays a confirmation message when an operator initiates a bulk change operation.

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Enable Confirmation for Bulk Change Actions parameter.

3 Click on the OK button. The User Preferences form closes.

Procedure 24-5 To view executed batch information

Note — You can also use the 5620 SAM Task Manager to view information about a batch.

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change from the list and click on the Properties button. The Bulk Change configuration form opens with the Batch Control tab displayed.

4 Choose a batch from the list.

5 Click on the Properties button. The Bulk Change Batch configuration form opens with the General tab displayed. View general information about the executed batch.

6 Click on the Batch Items tab button.

7 Click on the Search button. A list of items that were changed in the batch appears with the status of each batch item.

8 To view the parameters for each batch item, choose a batch item from the list and click on the Properties button.

9 Close all of the forms.

Procedure 24-6 To stop one or more bulk changes

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Perform one of the following:

- **a** Choose one or more bulk change to stop from the list.
- **b** Choose one or more batches to stop by performing the following:
  - **i** Choose a bulk change from the list.
  - **ii** Click on the Properties button. A Bulk Change configuration form opens with the Batch Control tab displayed.
  - **iii** Choose one or more batches from the list.

4 Click on the Stop button. A dialog box appears.

5 Click on the Yes button. The bulk change execution stops.

6 Close the forms.

Procedure 24-7 To delete a bulk change

1 Choose Tools→Bulk Operations from the 5620 SAM main menu. The Bulk Operations form opens.

2 Configure the filter criteria and click on the Search button. A list of bulk operations appears.

3 Choose the bulk change that you want to delete from the list and click on the Delete button. A dialog box appears.

4 Click on the Yes button. The bulk changes is removed from the 5620 SAM.

25 — Object life cycle

25.1 Object life cycle overview

The OLC state specifies whether an object is in maintenance or in-service mode to filter alarms in the Alarms Window. Alarms are generated for objects and services regardless of the OLC State parameter setting. The parameter setting is not sent to the objects or services.

You can set the OLC state for the following objects and services:

- network element
- card slot
- daughter card
- port
- LAG
- composite service
- service
- site

Caution — Changing the OLC state can affect 5620 SAM performance and can take more than ten minutes to complete.

Setting the OLC state

The default value of the OLC state for network elements can be specified in the discovery rules. See chapter 13 for more information about configuring the default OLC state for network elements. The OLC state default value of a child object is inherited from the parent object. The default value of the OLC state for composite services and services can be specified using the nms-server.xml file.

Caution — Unauthorized modification of the nms-server.xml file can seriously affect network management and 5620 SAM performance. Contact your Alcatel-Lucent representative for information about file modification.

When the OLC state of an NE is set to the maintenance mode, all children equipment such as access interfaces, card slots, daughter cards, and ports are set to maintenance mode. The sites on the NE are set to the maintenance mode.

When the OLC state of a composite service or service is set to the maintenance mode, the following related objects are changed:

- sites on which the services reside
- access interfaces (SAPs, L2 and L3 access interfaces)
- SDP Bindings (mesh, mirror and spoke bindings)

When the OLC state of a composite service or services is changed to in service, access interfaces and sites may not change to in service if they belong to equipment objects that are set to maintenance.

See chapter 17 for information about setting the OLC state for network and equipment objects. See chapters 67, 68, 70, 71, 65, 69 and 72 for more information about setting the OLC state for specific services and sites. See the *5620 SAM Parameter Guide* for information about how to configure the OLC State parameter.

The OLC state for child object is inherited from the parent object. The OLC state of the parent object must be in service to change the OLC State parameter of the child object. You can change the OLC state parameter of the parent object regardless of the OLC state of the child object. However, when a child object has more than one parent object and the OLC state of one parent is set to maintenance, the child object is set to maintenance. The OLC state for a child object cannot be changed if one of the parent OLC states is set to maintenance.

Discovery rules allow the operator to set the default OLC state for the node during discovery. See chapter 13 for information about setting the OLC state during discovery.

You must add the OLC state property to manually created service templates, as described in Procedure 25-5.

25.2 Workflow to set OLC states

1. Determine if you need to change the default setting of the OLC state.
   - i. Set discovery rules to set the node default OLC state.
   - ii. Set the OLC state for composite services and services.
2. Set the OLC state for specific nodes, cards, ports, LAGs, services and alarms.
   - i. Set the OLC state using Administration→OLC.
   - ii. Set the OLC state from an object configuration form.
3. View the OLC state:
   - i. From the Alarm Window, using the OLC filter button.
   - ii. Choose Administration→OLC.
   - iii. From the manage services and manage equipment windows.
   - iv. From an object configuration form.

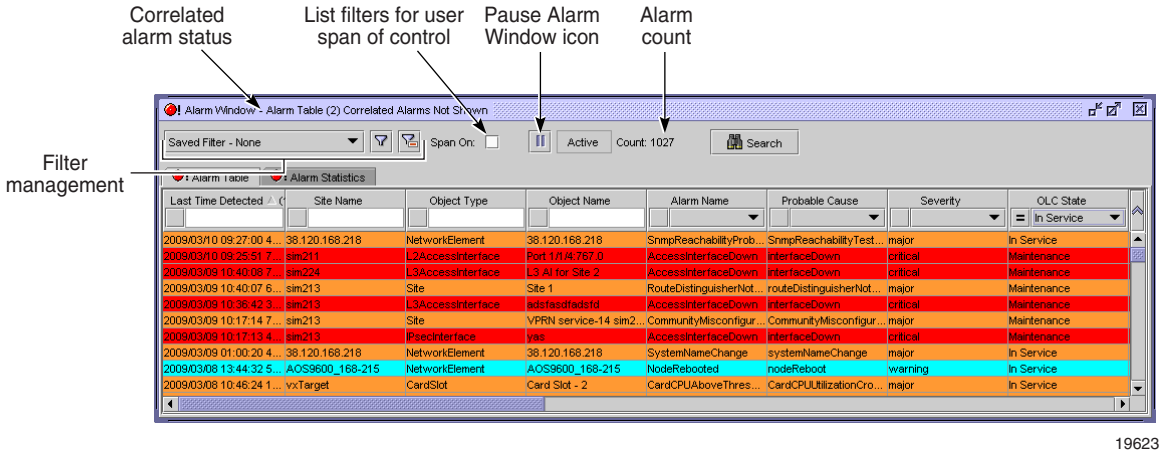
25.3 Setting the OLC state procedures

Use the following procedures to perform OLC management tasks.

Procedure 25-1 To view the OLC state of all network alarms using the dynamic alarm list

The dynamic alarm list Alarm Window allows you to monitor incoming faults from the devices and 5620 SAM software. This feature is most useful when monitoring the network. Figure 25-1 shows the dynamic alarm list Alarm Window.

Figure 25-1 Dynamic alarm list Alarm Window - Alarm Table



19623

1 Click on the filter icon in the Alarm Window. A filter window opens.

Note — You can open and view up to six Alarm Windows. This is useful when you need to view multiple filtered incoming network alarms.

2 Choose OLC State from the Attribute drop-down menu.

3 Configure the filter form to search for alarms. See chapter 2 for more information about creating search filters.

4 To assign the OLC State to the alarm. See Procedure 25-4 for more information.

5 Handle the alarms according to your fault management policies. See the *5620 SAM Troubleshooting Guide* for information about troubleshooting using alarm information guidelines.

Procedure 25-2 To view the OLC state of network equipment or a service

1 Choose Administration→OLC from the 5620 SAM main menu. An OLC form appears.

2 Choose a type of service or object from the object drop-down menu:

- Network Element (network) to view a list of NEs
- Card Slot (physical equipment) to view a list of cards
- Daughter Card Slot (physical equipment) to view a list of daughter cards
- Physical Port (physical equipment) to view a list ports
- LAG (LAG) to view a list of LAG ports
- Composite Service (Service Management) to view a list of composite services
- Service (Service Management) to view a list of services
- Site (Service Management) to view a list of sites

3 Choose In Service or Maintenance in the OLC State filter properties using the drop-down menu.

4 Click on the Search button. A list of objects or services appears based on the search filter.

Procedure 25-3 To change the OLC state of equipment or a service

Caution — Changing the OLC state can affect 5620 SAM performance and can take up to ten or more minutes to complete. Changing the OLC state of a parent object changes the OLC state of the child objects.

Note — One JMS message is sent to identify that the OLC state of a parent object has changed.

1 Choose Administration→OLC from the 5620 SAM main menu. An OLC form appears.

2 Choose a type of service or object from the object drop-down menu:

- Network Element (Network) to view a list of NEs
- Card Slot (Physical Equipment) to view a list of cards
- Daughter Card Slot (Physical Equipment) to view a list of daughter cards
- Physical Port (Physical Equipment) to view a list ports
- LAG (LAG) to view a list of LAG ports
- Composite Service (Service Management) to view a list of composite services
- Service (Service Management) to view a list of services
- Site (Service Management) to view a list of sites

3 Configure the filter criteria.

4 Click on the Search button. A list of equipment objects or services appears based on the search filter.

5 Select an object in the list. You can select multiple objects.

6 Click on the OLC State button, a drop-down menu appears.

7 Choose Maintenance or In Service from the drop-down menu. The OLC state of the object changes in the filtered list panel.

8 Close the OLC form.

Procedure 25-4 To change the OLC state from the Alarm Window

1 Click on the Alarm Table tab button in the Alarm Window. The dynamic list of incoming network alarms appears.

2 If required, click on the filter icon to create a filtered list of alarms. See chapter 2 for more information about creating search filters.

3 Select an alarm in the list. You can select multiple alarms.

4 Right-click on the alarm, a drop-down menu appears.

5 Choose Assign OLC State. An OLC State Assignment window opens.

6 Choose Maintenance or In service from the drop-down menu.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The OLC State Assignment window closes.

Procedure 25-5 To add the OLC state to a template using the GUI builder

Some service objects have an OLC state property. You cannot configure the OLC state property during the configuration of the service object. For 5620 SAM-created service templates, the OLC state property is automatically added to the template. For manually created service templates, the OLC state property is not added to the template. Perform the following procedure to add the OLC state property to a manually created template.

1 Perform steps 1 to 5 in Procedure 4-6 to open the GUI builder.

2 Perform step 15 in Procedure 4-6 to create a combo box component and enter olcState for the Name combo box component attribute.

3 Enter the value “maintenance” for the List combo box component attribute.

4 Enter the value “inService” for the List combo box component attribute.

5 Enter the value “maintenance” or “inService” for the Default combo box component attribute.

6 Save and close the GUI builder and Script editor windows.

26 — Auto-provision

26.1 Auto-provision overview

Auto-provision provides a way to reuse a proven configuration and apply the configuration to multiple NEs of the same type. This functionality is useful when a large number of similar NEs must be configured. Auto-provision reduces configuration errors and the time to configure each NE. Auto-provision takes advantage of the validations that are executed for every 5620 SAM configuration. When you configure a source NE from a 5620 SAM, the need to troubleshoot configuration problems is reduced.

After a source NE is configured and backed up, an operator can import the source script to the source profile. Alternatively, an operator can add the source script manually to the source profile. From the source profile, a target template can be generated. An operator can import the target template, enter any required changes and deploy the configuration template on a target NE. To ensure that the CLI syntax remains intact, the target NE must be the same type of NE, version, and chassis type as the source NE. For example, a source configuration from a 7705 SAR, version 2.0 device can only be deployed to a 7705 SAR, version 2.0 device.

Auto-provision extends configuration to an adjacent 7750 SR to ensure a prompt and reliable exchange of traffic between the devices. When the configuration profile is successfully deployed to a 7705 SAR target device, the operator can generate configuration modules to configure interactions between the target device and the adjacent devices. An operator can make minor changes to some of the attributes on the configuration modules and deploy the configuration modules to create objects on the selected 7750 SR. When modules are configured, the operator can deploy the modules to configure the connection. A VLL service site is created on the 7705 SAR and the adjacent 7750 SR. The 5620 SAM automatically creates SAPs and SDP bindings.

The 5620 SAM supports the generation of SAP and SDP configuration modules. Configuration between the 7705 SAR and the adjacent 7750 SR requires the following:

- Base configuration of the 7750 SR is complete and the 7705 SAR is auto-provisioned.
- Interface-level configuration is sent to the adjacent 7750 SR.
- The uplink port of the auto-provisioned 7705 SAR is configured to communicate with the network interface of the 7750 SR. Only Ethernet network interfaces are supported.
- The 7750 SR must be able to communicate with the adjacent 7705 SAR.
- A LDP interface is created on the same interface.
- A MPLS interface is created when MPLS is enabled. Choose either RSVP hop by hop or TE.
- MLPPP is configured on the 7750 SR when MLPPP is configured on the adjacent 7705 SAR.
- A LSP is configured between the 7750 SR and the 7705 SAR.
- An Ethernet, TDM or ATM endpoint is created on the 7750 SR that corresponds to the SAP on the 7705 SAR.

The velocity script generator parses a validated source NE configuration so that the NE is compatible with the velocity script management tool that is available in the 5620 SAM. After the layers are identified, the velocity script generator identifies attributes that require configuration before they can be applied to a target NE. Table 26-1 lists the layers that are identified by the velocity script generator. An operator can add, remove, modify, or hide any of the attributes that are listed. The layers must be configured to deploy together.

Table 26-1 Layers and attributes identified by the velocity script generator

Layer	Attributes
Base Equipment layer	SNMP packet size and daughter cards
Channelization layer	SONET SDH paths and channel groups
Policies layer	QoS and ACL related policies
Routing layer	Routing interface configurations and static routes
Routing Protocols layer	Routing Protocol configurations
MPLS layer	Targeted LDP, MPLS interfaces, and LSPs
Service layer	VLL services including Apipe, Cpipe, Epipe, Ipipe, VPRN, SAP, and SDP bindings

Warning — Scripts that are modified and saved must be applied to devices with the same vendor and version.

Access to the script management is controlled by the administration, script management and script execution scope of command roles. Access to auto-provision is controlled by the auto config permissions that are defined in the scope of command roles. Users that are assigned the administration or script management role can create, modify, delete, and execute scripts. Users that are assigned the script execution role can view and run scripts, view and save results, configure script targets and sources, and view historical results.

In addition to the scope of command access roles and profiles, access to the script manager is further defined by span of control. Span of control profiles determine where a user can apply scope of command access roles and profiles. For example, a user may have privileges to execute scripts. However, a span of control profile defines the scripts that the user can execute.

Auto-provision requires a Mobile Services Package license key to operate. See chapter 2 for more information about obtaining and installing software license keys.

26.2 Workflow to configure network devices using auto-provision

1 Determine the NE configuration that you need to use for the source.

2 Import a source configuration file from the router, or create a source file by performing a backup of the source configuration and naming the backup file a unique name. You can save the backup file to, for example, a USB drive, CD, and e-mail.

3 Import the source file into the auto-provision profiles manager tool.

4 Generate a template from the source script.

5 Use the GUI builder to customize attributes in the source template.

6 Export the source template to a file.

7 Create a target profile.

8 Import the source template into the auto-provision profiles manager tool.

9 Enter changes to the source script according to the network requirements.

10 Create a target template using the source script.

11 Apply the target template to a unprovisioned NE. This step is typically executed on a remote device.

Typically, steps 1 to 6 are performed on one 5620 SAM, and steps 7 to 11 are performed on another 5620 SAM. Steps 1 to 6 are typically performed in a lab or testing environment.

26.3 Auto-provision procedures

Use the following procedures to perform auto-provision.

Procedure 26-1 To configure a source template

1 Choose Tools→Auto-Provision Profiles from the 5620 SAM main menu. The Auto-Provision Profile Manager form opens.

2 Choose Auto-Config Source Node Profile (Automatic Configuration) from the drop-down menu.

3 Click on the Create button. The Auto-Config Source Node Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Script ID
- Name
- Description
- Network Element Type
- Network Element Version Information

5 Click on the Select button beside the Source Node Name parameter. The Select Source Node Auto-Config Source Node Profile form opens.

6 Choose a source NE from the list and click on the OK button. The Select Source Node Auto-Config Source Node Profile form closes. The following source NE information is displayed:

- Name
- Management IP Address
- System ID (Loopback IP Address)
- Chassis Type
- Software Version

7 Click on the Apply button. The Backup State parameter displays the status of the last backup operation on the NE, and the Script tab is available.

8 Create a backup file of the source NE and import the configuration script by performing one of the following:

a Back up and import from the router.

i Click on the Backup button. The Backup State parameter displays the status of the backup. When the status is Success, go to step ii.

ii Click on the Attach Source Node Config button. The backed-up script is attached to the source profile and can be viewed from the Script tab button.

b Back up and import the device configuration to a file.

i See Procedure 21-4 for information about saving a 7705 SAR configuration to a backup file.

ii Click on the Script tab button and click on the Create button. A Script Editor window opens.

iii Choose File→Import from the Editor menu. The Import dialog box appears.

iv Scroll to the location of the backup file that you previously created and saved.

v Click on the Import button. The script appears in the Script Editor workspace.

vi Choose File→Save and Close from the Editor menu. The Script Editor form closes.

Warning 1 — Scripts that are not correctly applied or created can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define the user responsibilities for script usage, and ensure that scripts are verified before they are executed on devices in a live network.

Warning 2 — Before you run a script, you need read, write, and execute permissions for the following folders:

- *install_dir*/client/nms/bin folder on Solaris
- *install_dir*/client/nms/bin/clientCache folder in Windows

where *install_directory* is the 5620 SAM client installation location which is typically /opt/5620sam/client on Solaris or C:\5620sam\client on Windows.

vii Choose File→Save and Close from the Editor menu. The Script Editor form closes and the Auto-Config Source Node Profile (Edit) form reappears. The script appears in the list.

9 Click on the Generate Template button.

Template generation can take several minutes to complete depending on the size of the source configuration file and server resource usage. After the process is complete, the Template tab is available.

10 Click on the Template tab. The newly created template appears in the list.

11 Choose a template and click on the Properties button. The script appears in the Script Editor workspace.

12 See Procedure 4-6 for more information about using the GUI builder tool to generate and customize a UI.

13 Choose File→Save from the Editor menu and close the GUI Builder window. The Script Editor window reappears.

14 Choose File→Export from the Editor menu. The Export dialog box appears.

15 Scroll to the location where you need to save the text file and enter a file name.

16 Click on the Export button. The Script Editor window reappears.

17 Close the Script Editor window. A dialog box appears if you entered any changes to the script.

18 Click on the OK button to save the changes to the script.

19 Close the Auto-Config Source Node Profile (Edit) window.

Procedure 26-2 To configure a target template

1 Choose Tools→Auto-Provision Profiles from the 5620 SAM main menu. The Auto-Provision Profile Manager form opens.

Note — Before you can apply a source configuration to a target NE, you must configure and export the source configuration. See Procedure 26-1 for more information about configuring and exporting a source template.

2 Choose Auto-Config Target Node Profile (Automatic Configuration) from the drop-down menu.

3 Click on the Create button. The Auto-Config Target Node Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Script ID
- Name
- Description
- Network Element Type
- Network Element Version Information

5 Click on the Apply button. The Template and Targeted Nodes tabs are available.

6 Click on the Template tab button and click on the Add button. A Script Editor window opens.

7 Choose File→Import from the Editor menu. The Import dialog box appears.

8 Scroll to the location of the file that you exported in Procedure 26-1.

9 Click on the Import button. The script appears in the Script Manager Editor workspace.

10 See Procedure 4-6 for more information about using the GUI builder tool to generate and customize a UI.

11 Choose File→Save from the Editor menu and close the GUI builder window.

12 Choose File→Save and Close from the Editor menu. The Script Editor form closes and the Auto-Config Target Node Profile (Edit) form reappears displaying the template.

13 Close the Auto-Provision Target Node Profile (Edit) window. To apply the source template to a target NE; go to Procedure 26-3.

Procedure 26-3 To apply a target template to an unprovisioned NE

1 Choose Equipment from the drop-down menu on the navigation tree.

Note — You can also access the Auto-Provision Managed Node Wizard from the equipment properties configuration form.

2 Right-click on the target device in the navigation tree and choose Auto-Provision from the drop-down menu. The Auto-Provision Managed Node Wizard form appears with the Profile step displayed.

Note — When a device has been previously configured, the Auto-Provision option is greyed out for the device.

3 Click on the Select button beside the Script ID parameter. A Select Template Name (Profile) - Auto-Provisioning window opens displaying a list of templates.

4 Choose the target template that you configured in Procedure 26-2.

5 Click on the OK button. The Auto-Provision Managed Node Wizard reappears.

6 Perform one of the following:

a Enable the Adjacent NE Managed parameter when the adjacent node is managed by the 5620 SAM. Go to step 9.

b Disable the Adjacent NE Managed parameter when the adjacent node is not managed by the 5620 SAM.

7 Click on the Next button. The Adjacent Node step is displayed.

8 Configure the Adjacent Site ID parameter. Go to step 13.

9 Click on the Next button. The Adjacent 7750 Node step is displayed.

10 Click on the Select button beside the Name parameter. A Select Adjacent NE - Auto-Provision Site window opens with a list of NEs.

11 Choose an NE from the list.

12 Click on the OK button. The Auto-Provision Managed Node Wizard reappears with the information about the displayed NE.

13 Click on the Finish button. A dialog box appears prompting you to deploy the script and generate configuration modules for the adjacent device.

14 Click on the OK button. The 5620 SAM prompts you to view the newly created auto-provision configuration.

15 Enable the View the newly created Auto-Provisioning parameter to display the auto-provision configuration after you close the form, if required.

16 Click on the Close button. The Auto-Provision-Site (Edit) window opens displaying the provisioning for the adjacent device.

17 Click on the Deploy Profile button. A Target Configuration window opens displaying the target NE, and the configurable parameters.

18 Configure the parameters, as required.

19 Click on the NE to which you need to deploy the configuration profile.

20 Click on the Execute button. View the status of the auto-provisioning in the Detailed Status/Error panel. After the NE is configured using the configuration profile, the status of the NE changes to configured.

21 Click on the Modules tab button.

Note — You must deploy the 7750 SR configuration modules after the 7705 SAR auto-provisioning is successfully deployed and resynchronized.

22 Click on the Generate Modules button to prompt the 5620 SAM to display the interactions between the target device and the adjacent device.

23 Click on the Properties button of a generated module to configure all of the modules that were created. The default values for some of the modules are usable. However, for other modules such as SAP modules, the operator must select a port on the 7750 SR before performing step 24.

24 Click on the Deploy Modules button to configure the connection.

25 Click on the Service Associations tab button to view the modified services.

26 Close the Target Configuration window.

Network management

27 — NE routing and forwarding

27.1 NE routing and forwarding overview

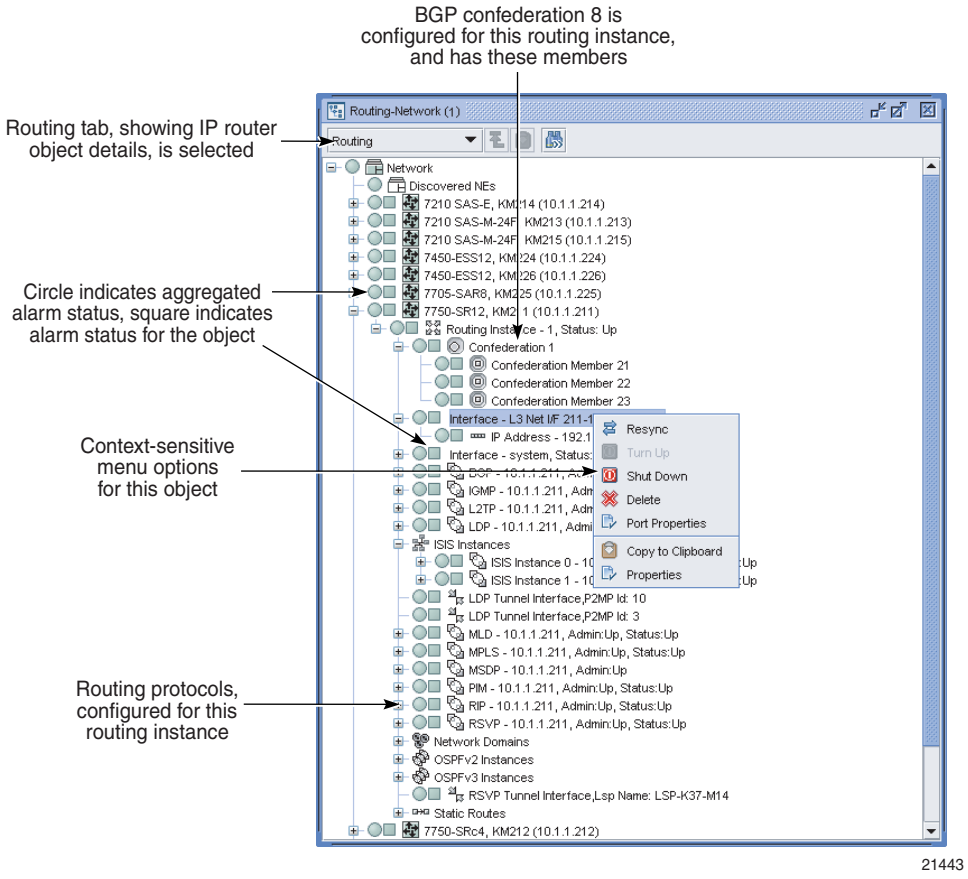
The 5620 SAM allows you to view and configure the routing and forwarding parameters on NEs. You can use the Routing view in the 5620 SAM GUI navigation tree to manage these functions on each managed NE.

Note 1 — For the 7250 SAS-ES and 7250 SAS-ESA, the 5620 SAM supports only the viewing, not the configuration, of routing instances and L3 interfaces. The 7250 SAS-ES and 7250 SAS-ESA must be configured using the CLI before they can be managed by the 5620 SAM.

Note 2 — For an OmniSwitch, the 5620 SAM supports viewing the status of routing protocols that are enabled using the CLI. The 5620 SAM also supports the configuration and management of routing instances, L3 interfaces, and static routes.

Figure 27-1 shows the routing objects in the network view of the navigation tree.

Figure 27-1 Routing objects



L3 network interfaces

An L3 network interface is a logical IP object that is defined on a physical port, such as an Ethernet port. An L3 interface:

- associates an IP address and subnet mask with a physical port or channel
- has a physical port or channel cabled to another device
- requires QoS policy configuration
- requires routing protocol configuration

The physical connection of one device to another device is through a port or channel. However, the L3 interface determines its IP connectivity. The L3 interface passes both routing information and IP traffic.

The system interface is associated with a network entity, such as a specific device, not a specific interface. The system interface is also referred to as the loopback interface. The system interface is associated during the configuration of the following entities:

- the termination point of service tunnels
- the hops when configuring MPLS paths and LSPs
- the addresses on a target device for BGP and LDP peering

The system interface is used to preserve connectivity when an interface fails or is removed. A system interface must have an IP address and a 32-bit subnet mask. The system interface is used as the device identifier by higher-level protocols such as OSPF and BGP. See chapter 28 for more information about routing protocols.

DoS protection

The 7750 SR-7, 7750 SR-12, 7450 ESS-7, and 7450 ESS-12, Release 6.0 R1 or later, support the use of DoS protection on network interfaces.

In a subscriber aggregation network, an NE typically receives few control-plane packets from a specific subscriber. If one or more subscribers generate excessive control-plane traffic, DoS protection policies can help to ensure that NEs do not become overburdened by these unwanted packets.

You can use the 5620 SAM to create DoS protection policies and apply them to L3 network interfaces. A DoS protection policy limits the number of control-plane protocol packets that are received each second from a subscriber host, and optionally logs a violation notification if a policy limit is exceeded. The interface drops the excessive packets before they are queued or processed by the NE. You can use the NE System Security form to view the violations for a specific NE.

You can apply DoS protection policies to control the following on L3 network interfaces:

- the control-plane packet arrival rate per subscriber host
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically assigns a default DoS protection policy to each L3 network interface. The default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified.

You can also apply DoS protection policies to certain L2 and L3 access interfaces. See the appropriate service chapter for information about applying DoS protection policies to access interfaces.

You can configure global DoS protection on an NE using the NE System Security form. Global DoS protection controls the arrival rate for unprovisioned link-layer protocol packets from CE devices. See Procedure 18-10 for more information.

See Procedure 18-3 for information about configuring NE DoS protection policies. See Procedure 27-6 for information about applying an NE DoS protection policy to an L3 network interface.

Routing protocols

When you configure a device, you configure the routing protocols used and the topology of packet handling between different devices in the network.

Networks can be grouped into areas. An area is a collection of network segments within an AS that have been administratively assigned to the same group. Area topology is concealed from the rest of the AS. This means a significant reduction in routing traffic. Routing in the AS takes place on two levels, depending on whether the source and destination of a packet reside in:

- the same area, known as intra-area routing
- different areas, knows as inter-area routing

In intra-area routing, the packet is routed based on information found within the area; no routing information from outside the area is used. This protects intra-area routing from the injection of bad routing information. Two devices, which are not area border routers, and belonging to the same area, have identical topological databases.

Devices that are aware of more than one area are called area border routers. In this case, all devices in an AS do not have an identical topological database. An area border router has a separate topological database for each area it is connected to. ASs share routing information, such as routes to each destination and information about the route or AS path, with other ASs using BGP.

Routing tables contain lists of next hops, reachable addresses, and associated path cost metrics to each device. Routing protocols use the information and path parameters to compile a network topology. The information about routes that is used to update routing tables can be modified using routing policies.

LLDP

Link Layer Discovery Protocol is a not a routing protocol, but instead, a neighbor-discovery protocol. As such, it is configured in a different manner than the standard routing protocols. LLDP allows a network access device to advertise its identity and capabilities to other stations attached to the same physical IEEE 801 LAN. It also permits information that the devices discover about peer devices to be stored. LLDP is only applicable for devices using Ethernet connectivity.

When LLDP is enabled on a device, it sends and receives LLDP messages on all of the physical interfaces that are enabled for LLDP transmission. These messages are sent periodically to ensure that information is accurate. These messages are stored on the local device for a configurable amount of time, and after this time has expired, the information is discarded.

5620 SAM uses the information stored in the applicable LLDP tables on the node to automatically discover the physical topology in the network. You can use this information to examine the L1/L2 topology and perform appropriate diagnostics and troubleshooting.

In LLDP, a single LLDP Protocol Data Unit is transmitted in a single Ethernet frame. The basic LLDP PDU consists of a header, followed by a variable number of information elements known as TLVs that each include fields for Type, Length, and Value. Type identifies what kind of information is being sent. Length indicates the length of the information string. Value is the actual information sent. Each LLDP PDU includes three mandatory TLVs followed by optional TLVs.

Mandatory TLVs include:

- Chassis ID: this represent the chassis identification of the device transmitting the LLDP frame
- Port ID: this represents the identification of the specific port transmitting the LLDP frame
- TTL: this represents the length of time the receive frame shall be valid

Optional TLVs include:

- Port Description: this represents the description of the port
- System Name: this is the administratively-assigned name of the device
- System Description: this is a textual description of the device
- System Capabilities: this identifies the capabilities of the device and its function (such as router, switch, repeater, etc.)

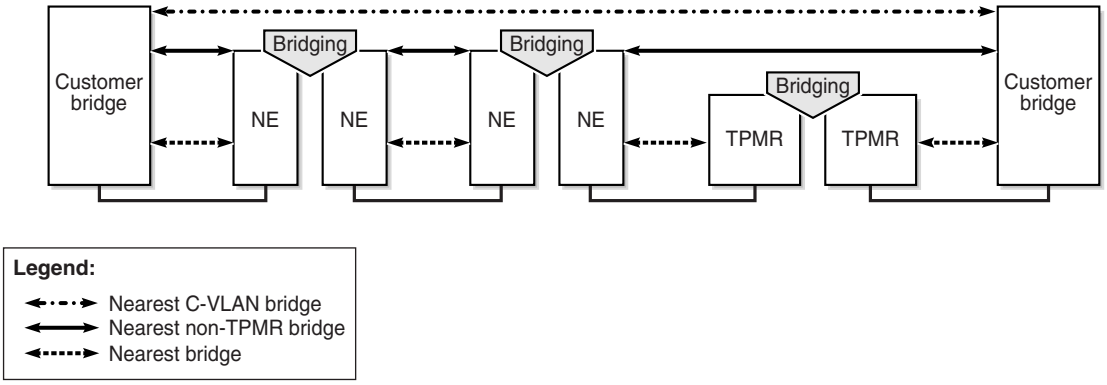
LLDP also supports multiple transmission scopes. The destination MAC address in the LLDP PDU determines how a frame is propagated through the network, thereby determining the LLDP message scope. Table 27-1 identifies a set of destination MAC address and describes the different transmission scopes associated with each address.

Table 27-1 MAC Addresses and transmission scopes

Name	Value	Purpose
Nearest Bridge	01-80-C2-00-00-0E	Propagation constrained to a single physical link
Nearest non-TPMR bridge	01-80-C2-00-00-03	Propagation constrained by all bridges other than TPMR; intended for use within provider bridged networks
Nearest Customer Bridge	01-80-C2-00-00-00	Propagation constrained by customer bridges

This information is also presented graphically in Figure 27-2.

Figure 27-2 LLDP Multiple Transmission Scopes



To enable LLDP, you must configure the protocol at both the system level and at the port level. This is best done using the equipment navigation tree. Table 27-2 lists the procedures required to implement LLDP.

Table 27-2 LLDP configuration procedures list

Procedure	See
To enable LLDP on a router	LLDP in section 17.4 and perform Procedure 17-47
To configure Ethernet ports	Procedure 17-61
To configure OmniSwitch Ethernet ports	Procedure 17-62

You can also use the physical topology map to view and edit various LLDP parameters and interconnections. By default, the physical map displays the topology based on the nearest-bridge LLDP scope. In addition, after the physical topology of a network has been discovered, you can create a reference checkpoint which is basically a snapshot of the topology at a specific time. Any subsequent deviations from this checkpoint can then be displayed. See "Physical topology map" in section 4.1 for more information.

Routing policies

Routing policies, also known as route redistribution policies, control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination.

Note — The 5620 SAM supports the distribution of policies on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, 7750 SR, 7710 SR, Release 6.0 or earlier Telco devices, on the 7705 SAR, Release 1.0 or later, and on the 7250 SAS and 7250 SAS-ES, before Release 2.0.

There are no default routing policies. Each policy must be created and applied to an object, a routing protocol, or the forwarding table. Each set of rules that is associated with controlling routes are called routing policy statement entries on the client GUI.

Use routing policies:

- to control routing protocols, such as BGP, to allow routes from another protocol, such as OSPF, into the routing table, which allows the routing table to redistribute packets into other protocols
- to control the import and export of learned active routes of a protocol
- to modify the characteristics of a route, for example, to change the community values of BGP AS path attributes
- to prevent the routes for specific customers from being added to routing tables
- to control BGP route flapping

Routing policy statements and routing policy statement entries are compared against incoming route packets in the following sequence.

1 The routing packets arrive.

2 The first routing policy is analyzed.

3 Each entry in the routing policy statement is analyzed.

If a match is found based on the first routing policy statement entry, the specified action is performed. You can use the Action parameter to specify the continued evaluation of route policy entries, or additional policy statements.

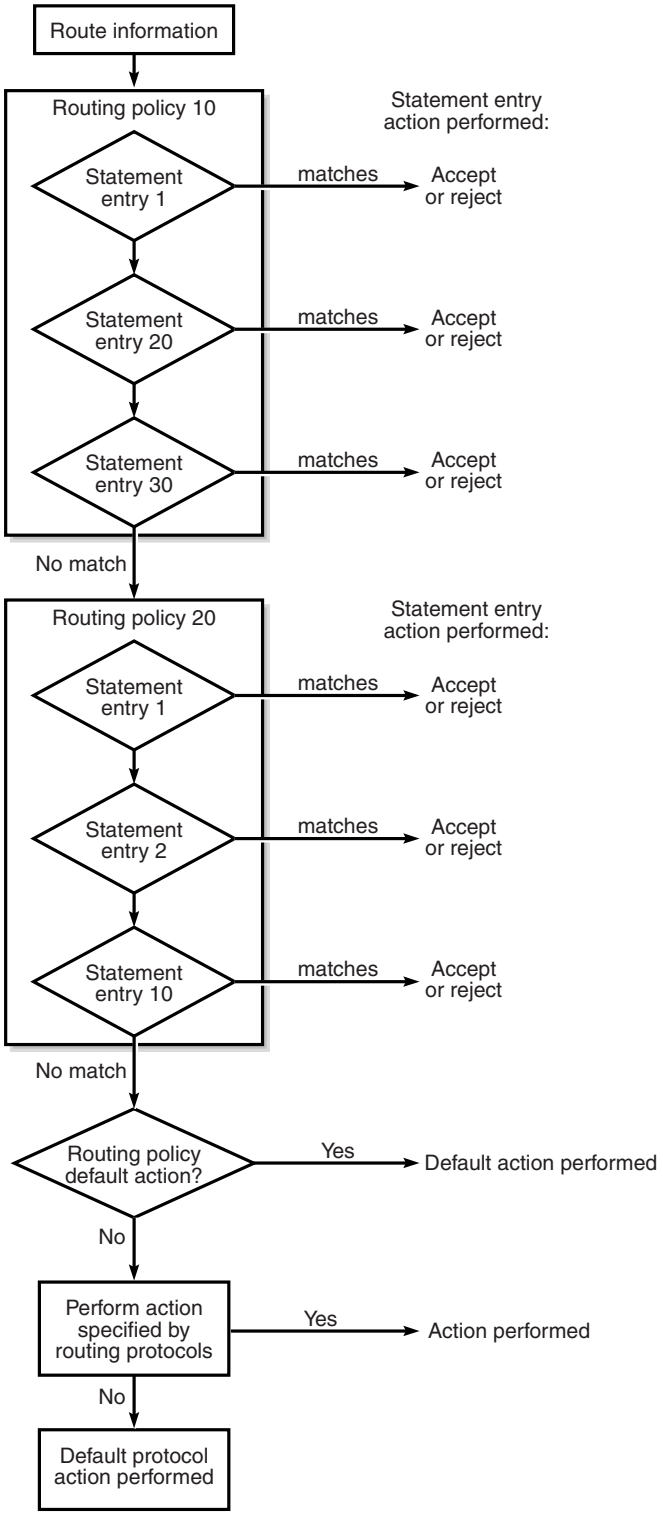
4 If no match is found, the packet is compared against the second routing policy statement entry. If a match is found based on the second routing policy statement entry, the specified action is performed.

5 If no match is found, the packet is compared sequentially against all remaining routing policy statements and routing policy statement entries. If a match is found, the specified action is performed.

6 If the packet does not match any routing policy statements or entries, the default action is performed.

Figure 27-3 shows how routes are analyzed using routing policies.

Figure 27-3 Routing policy analysis workflow



To ensure routing configuration flexibility, the following routing policies can be configured as separate policies or can be cross-referenced to form a framework of policies depending on the network requirements:

- Policy Statement
- Prefix List
- Community
- Damping
- AS Path

Policies that are cross-referenced are distributed together. For example a Policy Statement can reference the Prefix List policy by matching the From Criteria and the To Criteria for each policy type.

Careful planning is essential to implement route policies that can affect the flow of routing information or packets traversing managed devices. Before configuring and applying a route policy, consider the following:

- Develop an overall plan and strategy to accomplish your intended routing actions
- Analyze the effect of what happens to a packet that meets the specified criteria in a routing policy statement entry to ensure the proper action is executed and that no routing loops are created
- when possible, redistribute from a less router protocol to a greater routing protocol, for example from RIP to OSPF
- redistribute exported routes at a single device, when possible

When no action or default action in a routing policy is matched on a packet, then the routing protocols determine the default action for the packet. The action can be specified for the protocol. If the action is not specified, there are default routing protocol import and export actions performed, as described in Table 27-3.

Table 27-3 Default routing protocol actions

Protocol	Default import route action	Default export route options
BGP	All routes from BGP peers are accepted and forwarded to the BGP route selection process.	All active internal BGP routes are advertised to BGP peers. All non-BGP learned routes are not advertised to BGP peers.
IS-IS	IS-IS route acceptance cannot be configured. All IS-IS routes are accepted from IS-IS neighbors.	All internal IS-IS routes are advertised to all IS-IS neighbors. All non-IS-IS learned routes are not advertised to IS-IS neighbors.
OSPF	OSPF route acceptance cannot be configured. All OSPF routes are accepted from OSPF neighbors.	All OSPF routes are advertised to all OSPF neighbors. All non-OSPF learned routes are not advertised to OSPF neighbors.
RIP	All RIP-learned routes are accepted from RIP peers.	All non-RIP learned routes are not advertised to RIP peers.

For importing routing, RIP and BGP learned routes can be altered using routing protocols. For example, for devices learning about routes from BGP, you can create an import route policy that can limit the number and types of routes accepted and added to the routing tables.

For exporting routes, some default behaviors exist:

- internally learned routes are redistributed using the same protocol
- externally learned routes are not automatically advertised to all neighbors or peers

In the case of externally learned routes, you can create an export policy to determine how the routes are advertised, for example, configuring something learned by BGP to be redistributed using OSPF. This is useful in cases:

- where legacy equipment does not support a specific protocol
- when companies merge and they use different routing protocols on the devices

Network Address Translation

Network Address Translation, or NAT, is function that rewrites address information in IP packets that travel between private and public networks. NAT is a widely accepted method of effectively extending the available public IPv4 address space, because multiple end users can share one IP address. NAT can also provide security by preventing an internal IP address, such as an end-user address, from entering a public network.

NAT translates internal, or private, host IP address and TCP port values to external, or public, values. When NAT receives a packet from an internal host, it replaces the source address information in the packet with public address information, and forwards the packet to the destination. NAT assigns private IP addresses and ports dynamically using values from an allocated pool, but can also use values that are statically assigned to internal hosts, depending on the type of NAT depl.oyment.

You can use the 5620 SAM to configure NAT on a Release 8.0 or later 7750 SR in chassis mode B or higher. 5620 SAM NAT support includes the following:

- policy-based management
- subscriber-specific implementation
- configurable port usage limits per subscriber, address range, or policy
- reserved port ranges for specified forwarding classes that are exempt from port usage limits
- configurable protocol timeout periods for efficient resource management

The 5620 SAM supports the following NAT deployment types:

- L2-aware—Hosts of the same subscriber can share a private address, and are assigned public addresses from a pool in a base routing instance.
- large-scale—Each host can have a unique static or dynamic private address, and is assigned a public address from a pool in a VPRN routing instance.

The NAT configuration on a routing instance includes the following:

- one or more NAT address pools that are associated with local ISA-NAT groups
- a NAT policy, which specifies port ranges and operational parameters

- host address match criteria
- one or more NAT destinations

An ISA-NAT group is a logical group of redundant MDAs that forward NAT packets. A NAT policy associates an address pool with an ISA-NAT group and defines general NAT properties. See chapter 15 for an ISA-NAT group overview, and chapter 17 for ISA-NAT group configuration information. See chapter 43 for information about creating and configuring NAT policies.

A 5620 SAM operator assigns port ranges in an address pool configuration. Port ranges specify the number of ports allocated to a subscriber for mapping to host sessions. When all ports for a subscriber are consumed, further port assignments do not occur and host sessions are refused. This helps to prevent the swamping of NAT by an event such as a virus attack or multiple peer-to-peer file transfers. You can override a port-range limit by configuring a range of reserved ports that are assigned based on the traffic forwarding class.

Note — The 5620 SAM does not allow the use of ports 0 to 1023, which are called the well-known ports or privileged ports, in a NAT configuration.

To ensure fair and timely NAT resource allocation to hosts, you can specify timeout values in a NAT policy for protocols such as ICMP, TCP, and UDP. NAT ends a host session after the timeout period, for example, when TCP handshaking takes an unreasonable amount of time.

The NAT drain function is a mechanism that is used to gracefully remove the host sessions associated with an address range in a NAT address pool. When an address range is in the draining state, NAT drops new session requests for the address range. After an existing session associated with a draining address range closes, a new session for the same host is created using a different address range. The drain function removes an address range only when there are no sessions associated with the address range. See chapter 17 for information about using the NAT drain function.

You can view general NAT statistics, for example, address-pool allocation and session counts for different protocols on the Statistics tab of an ISA-NAT group member properties form.

Note — The 5620 SAM does not record detailed NAT session information such as duration or packet counts. You can obtain this information only by directly requesting it from a participating NE.

L2-aware NAT

In L2-aware NAT, a NAT policy is associated with a subscriber profile that is applied to an IES SAP. The NAT policy specifies an address pool on the base routing instance. When DHCP assigns a private IP address that is in an L2-aware NAT address range, NAT assigns a public IP address to the host packets. See chapter 70 for information about configuring NAT in an IES.

Note 1 — A NAT configuration on a base routing instance applies to each IES site on the NE.

Note 2 — A NAT policy that is specified in a subscriber profile redirects all IPv4 traffic for the subscriber to NAT.

Large-scale NAT

Large-scale NAT is used when each host in a customer VPRN service has a unique private IP address and requires a unique public IP address, for example, in mobile network deployments. Large-scale NAT is used between routing instances. A customer VPRN routing instance provides host access and forwards packets through NAT to a VPRN or through an IES to an NE routing instance, which provides public network access.

A VPRN routing instance requires an ACL IP filter or static route to direct host traffic through the NAT function, and uses an address pool in the VPRN routing instance. You can configure large-scale NAT to statically and dynamically assign private addresses. See chapter 71 for information about configuring NAT in a VPRN service. See "Static port forwarding" in this section for more information about configuring NAT to use static private addresses.

Static port forwarding

In a large-scale NAT deployment, you can configure NAT to assign static private addresses to subscriber hosts using static port forwarding. Static port forwarding ensures that an internal host uses the same private IP address and port each time they connect to the network. You can use the 5620 SAM to configure static port forwarding for TCP and UDP independently.

For VPRN services, static port forwarding is configurable on the VPRN routing instance. For IES, static port forwarding is configurable on the NE routing instance. See chapter 71 for information about configuring static port forwarding in a VPRN service. See chapter 70 for information about configuring static port forwarding in an IES.

Cflowd

The 5620 SAM supports the configuration of Cflowd on Release 8.0 and later of the 7710 SR, 7750 SR-7 and 7750 SR-12, and on the 7450 ESS in mixed mode. Cflowd is a traffic-sampling function that collects statistical data based on traffic flows. A flow is a series of packets in a user session. Cflowd data is typically used to monitor network-usage trends and detect security threats. You can use the 5620 SAM to configure Cflowd for the following:

- traffic that passes through an L3 network interface
- traffic that is redirected to Cflowd using an ACL IP filter
- AA traffic

You must enable Cflowd globally on an NE before you can configure Cflowd collectors. You can create multiple Cflowd collectors on an NE. Each collector is deleted when Cflowd is disabled.

AA Cflowd is configurable on an ISA-AA group, and supports basic Cflowd sampling as well as TCP performance data collection for AA applications and application groups. Each ISA-AA group supports one Cflowd instance.

See chapter 17 for information about enabling and configuring global Cflowd on an NE, and for information about enabling and configuring AA Cflowd on an ISA-AA group.

27.2 Workflow to configure NE routing and forwarding

1 Use the CLI to configure or verify these parameters:

- system address (system ID)
- router ID

See the *7750 SR OS Router Guide* for more information about the parameters.

2 Configure L3 interfaces. The L3 interfaces are associated with network ports. There are network and system interfaces.

i Assign names.

ii Associate IP addresses.

iii Specify the interface as a network or system interface.

iv Associate a network port with the L3 interface.

v Configure the appropriate routing protocols on the interfaces, as required. The supported protocols are BGP, MPLS, RIP, LDP, OSPFv2, OSPFv3, IS-IS, and RSVP.

See chapter 28 for more information about routing protocol configuration and parameters.

vi Enable the multicast routing types on the interfaces as required. The supported types are PIM, IGMP, and MLD.

See chapter 28 for more information about multicast configuration and parameters.

vii Enable bridging on the interfaces as required. The 5620 SAM supports bridging on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco and OmniSwitch devices.

See chapter 28 for more information about bridging configuration and parameters.

viii Assign a DoS protection policy to the interface, if required.

ix Assign an IES or network interface to a virtual router as a VRRP instance.

See chapter 36 for more information about VRRP configuration and parameters.

3 Cable the network ports on the devices to the network ports on other devices.

4 Configure these key device parameters using the 5620 SAM:

- BGP, MPLS, RIP, LDP, OSPF, IS-IS, and RSVP
  Enable routing protocols on the device, as required. If you plan to create signaled LSPs, then you must enable MPLS, and RSVP or LDP.
- IP address ranges for use by services, such as IES and VPLS
  Reserve IP addresses to provide a mechanism to reserve one or more address ranges for services. When services are defined, the address must be in the range specified as a service prefix. Addresses in the range of a service prefix can be allocated to a network port unless set to exclusive. Then, the address range is exclusively reserved for services.
- device-wide AS settings

5 Use the 5620 SAM to create static routes as required.

6 Use the 5620 SAM to configure a routing policy.

i Configure AS path expressions, as required.

ii Configure community lists, as required.

iii Configure damping parameters to control BGP route flapping, as required.

iv Configure prefix lists, as required.

7 Configure an AS and confederations for BGP (optional).

Configuring confederations is optional and should only be implemented to reduce the IBGP mesh inside an AS. An AS can be logically divided into smaller groupings called sub-confederations. See chapter 28 for more information about BGP configuration.

8 Use the 5620 SAM to create MPLS administrative groups and assign the groups to MPLS interfaces and LSPs paths as required.

9 Configure NAT on the base routing instance, if required. See "Network Address Translation" in this chapter for more information.

27.3 NE routing and forwarding configuration procedures

The following procedures describe how to configure routing.

Procedure 27-1 To configure a routing instance

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→Router→Routing Instance.

3 If you are configuring a VRF routing instance on an OS 9700E or OS 9800E, go to step 4, otherwise go to step 6.

4 Right-click on the OS 9700E or OS 9800E, and choose Create VRF Instance. The Routing Instance (Create) form opens.

5 Configure the VRF Name parameter. Click on the Apply button. The Routing Instance (Edit) form opens. Go to step 8.

6 Right-click on the routing instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

7 Configure the Administrative State parameter.

8 Click on the Protocols tab button.

9 Configure the applicable parameters:

- BGP Enabled
- MPLS Enabled
- OPSF v2 Enabled
- RIP Enabled
- L2TP Enabled
- LDP Enabled
- OPSF v3 Enabled
- IS-IS Enabled

The supported protocols are displayed in the navigation tree as sub-items in the routing instance. Click on the Properties button to configure the routing protocols. See chapter 28 for more information about routing protocol configuration using the GUI.

Note — SNMPv3 must be used to manage OS 9700E and OS 9800E NEs, when configuring a VRF routing instance.

10 Click on the Edit Routing Policies button. A Routing Policy Manager (Edit) window opens.

11 Click on the Show Policy button. A Routing Policy Show Policy window opens with the General tab displayed.

12 Click on the Ok button. A CLI display is initiated.

13 View the policy.

14 Click on the Close button. The Routing Policy Show Policy window closes.

15 Click on the Multicast tab button.

Multicast is not configurable for the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7450 ESS.

16 Configure the parameters:

- PIM Enabled
- IGMP Enabled
- MLD Enabled
- MSDP Enabled

The supported multicast protocols are displayed in the navigation tree as sub-items in the routing instance. Click on the Properties button to configure the routing protocols. See chapter 28 for more information about multicast protocol configuration using the GUI.

17 Click on the Routing tab button.

18 Configure the parameters:

- Router ID
- Maximum Number of Equal Cost Routes
- Autonomous System
- Confederation Autonomous System
- LDP Shortcut Enabled
- Enforce Maximum Number of Multicast Routes

Autonomous System, Confederation Autonomous System and Enforce Maximum Number of Multicast Routes parameters are not configurable in the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7450 ESS.

When you select the Enforce Maximum Number of Multicast Routes parameter, the following configurable parameters appear:

- Maximum Number of Multicast Routes
- Log Only
- Threshold (%)

See chapter 28 for more information about AS and confederation parameters for BGP using the GUI.

19 Configure the parameters:

- Single SFM Overload Admin State
- Hold-Off Time (seconds)

The Hold-Off Time (seconds) parameter and read-only attributes Overload State, Overload Start, and Overload Duration are only displayed when the Single SFM Overload Admin State parameter is set to Up.

20 Configure a Multicast Path Management Info Policy, if required.

i Click on the Select button beside the Name parameter. The Select Ingress Info Policy form is displayed.

ii Choose the required policy from the list and click OK. The Select Ingress Info Policy form closes and the policy name is displayed in the Name field.

Note — The Mcast Path Mgmt Channels tab displays data on the operational channels after actual traffic from a specific multicast source for a specific multicast group passes through the virtual router. You must click on the Search button to refresh the data. See chapter 43 for a listing of the displayed operational channel parameters.

21 Click on the Interfaces tab button. See Procedure 27-4 for more information about creating additional L3 interfaces.

22 Click on the Address tab button.

23 Configure IP address parameters for L3 interfaces.

i Choose an address in the list.

ii Click on the Properties button.

The IP Address form opens.

iii Configure the parameters:

- IP Address
- Prefix Length
- Broadcast Address Format

iv Click on the OK button. The IP Address form closes and the Routing Instance form reappears.

Note — The IP Address, Prefix Length, and Broadcast Address Format cannot be changed for the System interface.

24 Click on the Static Routes tab button to view a list of static routes and to add static routes. See Procedure 27-17 for more information.

25 To configure NAT on the routing instance, click on the NAT Configuration tab button. Otherwise, go to step 37.

Note — NAT configuration is supported only on a Release 8.0 or later 7750 SR-7 or 7750 SR-12 in chassis mode B or higher.

26 Click on the Add button. The NAT Configuration (Create) form opens with the General tab displayed.

27 Click on the Select button to choose a NAT policy. The Select NAT policy form opens.

28 Select a policy in the list and click on the OK button. The Select NAT policy form closes, and the policy name is displayed on the NAT Configuration (Create) form.

29 Click on the Apply button. A dialog box appears.

30 Click on the Yes button.

31 Perform the following steps to configure static port forwarding, if required.

Note — You can configure NAT static port forwarding only for large-scale NAT.

i Click on the Static Port Forwarding tab button.

ii Click on the Add button. The NAT Static Port Forwarding Display (Create) form opens.

iii Configure the IP Address parameter.

iv Click on the Port Configuration tab button.

v Click on the Add button. The NAT Static Port Forwarding Port Display (Create) form opens.

vi Configure the parameters:

- Port
- Protocol
- Outside Port

Note — You cannot specify the same set of Port and Protocol values in more than one static port mapping to an IP Address.

You can specify the same Outside Port value in multiple mappings to an IP Address.

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The NAT Static Port Forwarding Port Display (Create) form closes, and the new entry is listed on the NAT Static Port Forwarding Display (Create) form.

ix Repeat steps v to viii to assign an additional static address, if required.

x Click on the General tab button.

xi Configure the Administrative State parameter.

xii Click on the OK button. A dialog box appears.

xiii Click on the OK button. The NAT Static Port Forwarding Display (Create) form closes, and the new static port forwarding entry is displayed on the NAT Configuration (Create) form.

32 Perform the following steps to configure a NAT pool.

i Click on the NAT Pools tab button.

ii Click on the Add button. The NAT Pool (Create) form opens.

iii Configure the parameters:

- Displayed Name
- Description
- NAT Pool Type
- Administrative State
- Port Reservation Type
- Port Reservation Value
- High Watermark
- Low Watermark

iv Click on the Select button to choose an ISA-NAT group. The Select ISA-NAT group form opens.

v Select an ISA-NAT group in the list and click on the OK button. The Select ISA-NAT group form closes, and the ISA-NAT group name is displayed on the NAT Pool (Create) form.

vi Click on the NAT Pool Ranges tab button.

vii Click on the Add button. The NAT Pool Range (Create) form opens.

viii Configure the parameters:

- Description
- Range Start
- Range End

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The NAT Pool Range (Create) form closes, and the NAT Pool (Create) form lists the pool range.

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The NAT Pool (Create) form closes, and the NAT Configuration (Create) form lists the NAT pool.

xiii Repeat steps vii to xii to add another pool, if required.

33 Perform the following steps to add an IP address for L2-aware NAT forwarding, if required.

i Click on the L2 Aware IP Addresses tab button.

ii Click on the Add button. The L2 Aware IP (Create) form opens.

iii Configure the parameters:

- IP Address
- Prefix Length

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The L2 Aware IP (Create) form closes, and the NAT Configuration (Create) form lists the IP address.

vi Repeat steps ii to v to add another IP address, if required.

34 Perform the following steps to add a NAT destination address.

i Click on the NAT Destinations tab button.

ii Click on the Add button. The NAT Destination (Create) form opens.

iii Configure the parameters:

- IP Address
- Prefix Length

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The NAT Destination (Create) form closes, and the NAT Configuration (Create) form lists the destination.

vi Repeat steps ii to v to add another destination, if required.

35 Click on the OK button. A dialog box appears.

36 Click on the Yes button. The NAT Configuration (Create) form closes, and the NAT configuration is listed on the Routing Instance form.

37 Click on the RSVP Tunnel Interfaces tab button to create an RSVP tunnel interface entry, if required.

i Click on the Add button. The RSVP Tunnel Interface (Create) form opens.

ii Click on the Select button beside the Lsp Name parameter. The Select - RSVP Tunnel Interface form opens.

iii Select an RSVP tunnel interface and click on the OK button. The Select - RSVP Tunnel Interface form closes and the RSVP Tunnel Interface (Create) form reappears.

iv Configure the Sender Address parameter.

v Click on the OK button. The RSVP Tunnel Interface (Create) form closes.

38 Click on the LDP Tunnel Interfaces tab button to create an LDP tunnel interface entry, if required.

i Click on the Add button. The LDP Tunnel Interface (Create) form opens.

ii Configure the parameters:

- Description
- P2MP ID
- Root Node
- Sender Address

iii Click on the OK button. The LDP Tunnel Interface (Create) form closes.

39 Click on the Multi-Homing Interface tab button to create a multi-homing interface entry, if required. the Multi-Homing Interface (Create) form opens with the General tab displayed.

Note 1 — The Multi-Homing Interface is a loopback interface used in multi-homing resiliency for a pair of protected routers. When it is active, the Primary interface can be used to advertise reachability information of the alternate router to the rest of the network. The Secondary interface is used to resolve routes advertised by the alternate router in the event that router becomes unavailable. This mechanism applies to both IP and VPN traffic.

Note 2 — Only one Primary and one Secondary multi-homing interface may be created for a router.

Note 3 — You can configure a multi-homing interface on the 7750 SR, 7710 SR, and 7450 ESS (in mixed mode) network elements. Chassis mode "D" must be enabled.

i Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Type
- Hold Time (seconds)
- Administrative State

The Hold Time (seconds) parameter only appears if you specify Secondary as the Interface Type.

ii Click on the Addresses tab button. The Multi-Homing Interface Addresses list is displayed.

iii Click on the Add button. The IP Address (Create) form opens.

iv Configure the IP Address parameter.

Note — Only IPv4 addresses are supported when creating the multi-homing interface.

v Click on the OK button. The IP Address (Create) form closes and the new address appears selected in the list.

vi Click on the OK button. The Multi-Homing Interface (Create) form closes.

40 Click on the Route Aggregation tab button to configure route aggregates that can be generated into the virtual router.

i Click on the Add button. The Aggregation (Create) form opens.

ii Configure the parameters, if present:

- IP Address Prefix
- Mask
- Summary Only
- As Set
- Aggregator
- Aggregator AS
- Aggregator IP Address

The Aggregator AS and Aggregator IP Address parameters are configurable when the Aggregator parameter value is set to True.

The 7705 SAR-8 supports Summary Only route aggregation only.

41 Click on the BGP Confederations tab button, if present, to view and create BGP confederations. See chapter 28 for more information about BGP confederation configuration.

42 Click on the Service Address Ranges tab button, if present, to provide a mechanism to reserve one or more IP address ranges for use by services, such as IES.

i Click on the Add button. The Service Address Range form opens.

ii Configure the parameters:

- IP Address
- Prefix Length
- Exclusive

iii Click on the OK button. The Service Address Range form closes and the Routing Instance form reappears.

43 Configure an override source IP address or L3 interface for use by a selected IP application, if required.

i Click on the Source Address tab button.

ii Click on the Add button. The Source Address form opens.

44 Choose an IP application from the Source IP Application drop-down menu.

45 Perform one of the following:

Note — If you choose the interface index option, the router must already have a network interface or an IES L3 access interface created on the routing instance.

a Choose IP Address in Source Address Termination to specify a source IP address on the node for use by the IP application.

i Enter an IP address in the Source IP Address field.

ii Go to step 46.

b Choose Interface Index in Source Address Termination to use the primary address on the L3 network interface as the source address on the node for the IP application.

i Click on the Select button to choose an interface. The Select Source Address Network Interface form opens. Select an interface in the list and click on the OK button. The IP address and Interface ID of the L3 interface appears on the form.

ii Go to step 46.

Note — You must select an IPv6 Source IP Address to select an IPv6 Source IP Application.

46 Click on the OK button. The Source Address form closes and the Routing Instance form reappears. The IP application source address and parameters appear on the form.

47 Perform the following steps to configure a local DHCP server on the routing instance, if required or applicable.

i Click on the Local DHCP Servers tab button.

ii Click on the Add button. The Local DHCP Server (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Server Name
- Description
- Administrative State
- Use GI Address

iv Click on the Select button. The Select Local User Database form opens.

v Select a local user database in the list and click on the OK button. The Select Local User Database form closes and the local user database information is displayed on the Local DHCP Servers (Create) form.

vi Configure the following parameters:

- Allow Send Force Renews
- Use Pool From Client

vii Click on the IP Address Pools tab button to assign one or more IP addresses to the local DHCP server.

viii Click on the Add button. The IP Address Pool (Create) form opens with the General tab displayed.

ix Configure the following parameters:

- Pool Name
- Description

x Configure the parameters in the Minimum Lease Time panel:

- Days
- Hours
- Minutes
- Seconds

xi Configure the parameters in the Maximum Lease Time panel:

- Days
- Hours
- Minutes
- Seconds

xii Configure the parameters in the Offer Time panel:

- Minutes
- Seconds

xiii Click on the Subnets tab button to add subnets to the DHCP server pool.

xiv Click on the Add button. The Subnet (Create) form opens with the General tab displayed.

xv Configure the parameters:

- IP Address
- Prefix Length
- Free Addresses Minimum Threshold
- Maximum Declined Addresses Stored

xvi Click on the Address Ranges tab button.

xvii Click on the Add button. The Subnet Address Range (Create) form opens.

xviii Configure the parameters:

- Action
- Start Address
- End Address

Note — You must exclude static IP addresses from the subnet address range because static IP addresses are dedicated.

xix Click on the OK button. The Subnet Address Range (Create) form closes and a dialog box appears.

xx Click on the OK button. The Subnet (Create) form reappears.

xxi Click on the Options tab button.

xxii Click on the Add button. The Subnet Option (Create) form opens.

xxiii Configure the parameters:

- Option
- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Number parameter is configurable when the Option parameter is set to Custom Option.

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xxiv Click on the OK button. The Subnet Option (Create) form closes and a dialog box appears.

xxv Click on the OK button. The Subnet (Create) form reappears.

xxvi Click on the OK button. The Subnet (Create) form closes and a dialog box appears.

xxvii Click on the OK button. The IP Address Pool (Create) form reappears.

xxviii Click on the Options tab button.

xxix Click on the Add button. The IP Address Pool Option (Create) form opens.

xxx Configure the Option parameter.

xxxi If you set the Option parameter to Custom Option, configure the following parameters:

- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xxxii If you set the Option parameter to DNS Name Servers or Netbios Name Server, configure the following parameters:

- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

xxxiii If you set the Option parameter to Domain Name, configure the Value parameter.

xxxiv If you set the Option parameter to Lease Time, Lease Renew Time, or Lease Rebind Time, configure the following parameters:

- Days
- Hours
- Minutes
- Seconds

xxxv If you set the Option parameter to Netbios Node Type, configure the Netbios Node Type parameter.

xxxvi Click on the OK button. The IP Address Pool Option (Create) form closes and a dialog box appears.

xxxvii Click on the OK button. The IP Address Pool (Create) form reappears.

xxxviii Click on the OK button. The IP Address Pool (Create) form closes and a dialog box appears.

xxxix Click on the OK button. The Local DHCP Server (Create) form reappears.

xl Click on the OK button. The Local DHCP Server (Create) form closes and a dialog box appears.

xli Click on the OK button. The VPRN Site (Create) form reappears.

48 Click on the Self Generated Traffic tab button. The DSCP Marking tab is displayed with a list of all the applications for which the DSCP can be set.

49 Choose an application to view or edit the DSCP setting.

50 Click on the Properties button. An Application DCSP Marking form opens.

51 Configure the DSCP parameter.

52 Click on the OK button. A dialog box appears.

53 Click on the Yes button.

54 Click on the DSCP Mapping tab button.

55 Select a DSCP mapping in the list and click on the Properties button. The Application DCSP Mapping form opens.

56 Configure the Forwarding Class parameter.

57 Click on the OK button. A dialog box appears.

58 Click on the Yes button.

59 Click on the Dot1p Marking tab button.

60 Select a Dot1p marking entry in the list and click on the Properties button. The Application Dot1p Marking form opens.

61 Configure the Dot1p parameter.

62 Click on the OK button. A dialog box appears.

63 Click on the Yes button. The Routing Instance (Edit) form reappears.

64 Close the Routing Instance (Edit) form.

Procedure 27-2 To configure an OmniSwitch 6xxx or 9xxx routing instance

To configure an OS 9700E or OS 9800E routing instance, see Procedure 27-1.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an OmniSwitch routing instance by choosing Network→OmniSwitch 6xxx or OmniSwitch 9xxx→ Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Routing tab button.

5 Configure the Router ID parameter, if required.

6 Click on the Interfaces tab button. See Procedure 27-5 for information about creating additional OmniSwitch L3 interfaces.

7 Click on the Address tab button.

8 Configure IP address parameters for L3 interfaces.

i Choose an address in the list.

ii Click on the Properties button. The IP Address (Edit) form opens.

iii Configure the parameters, if required:

- IP Address
- Prefix Length

iv Click on the OK button to save the changes. A dialog box appears.

v Select the check box to indicate that you understand the implications of making the change or click on the No button and go to step ix.

vi Click on the Yes button. A dialog box appears.

vii Click on the Yes button. The Routing Instance (Edit) form reappears.

viii Go to step 9.

ix Close the IP Address (Edit) form.

9 Click on the Static Routes tab button to view a list of static routes and to add static routes. See Procedure 27-18 for more information.

10 Click on the OK button to save the configuration. A dialog box appears.

11 Click on the Yes button to verify the action.

12 Close the form.

Omniswitch DHCP relay and snooping

A DHCP relay agent is a BOOTP relay agent that relays DHCP messages between DHCP clients and DHCP servers on different IP networks. The Omniswitch supports global or per-VLAN BOOTP/DHCP relay service and per-VLAN UDP port relay services.

DHCP Option-82 and DHCP snooping provide security for a DHCP relay service. The DHCP Option-82 switch-level feature allows the relay agent to insert identifying information into client-originated DHCP packets before the packets are forwarded to the DHCP server. DHCP Snooping, at the switch or VLAN level, improves network security by filtering DHCP messages received from devices outside the network and building and maintaining a binding table to track access information for each device. DHCP relay Option-82 and snooping cannot be run on the switch at the same time.

DHCP relay and snooping is configured at the default routing instance level, see Procedure 27-3. In addition, per-VLAN DHCP snooping can be enabled on a VLAN site. See procedures 65-4, 65-6, and 65-7 for more information.

It is necessary to configure ports connected to DHCP servers within the network and/or firewall as trusted ports so that necessary DHCP traffic to/from the server is not blocked. Configuring the port mode as trusted also identifies the device connected to that port as a trusted device within the network. See Procedure 17-62 for more information.

Procedure 27-3 To configure UDP relay/DHCP snooping on an OmniSwitch in routing instances

This procedure describes how to configure UDP Relay and DHCP Option-82 and snooping on default routing instances for all OmniSwitch NEs.

Note — For VRF instances on the OS 9700E and OS 9800E NEs, only UDP Relay service is supported.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an OmniSwitch routing instance by choosing Network→OmniSwitch → Routing Instance.

Warning 1 — The routing instance must be the default routing instance.

Warning 2 — UDP Server Statistics/UDP Service Statistics will be lost as part of the parent change from Bridge Instance to Routing Instance.

3 Right-click on the routing instance icon and choose Properties from the contextual menu. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the UDP Relay tab button to configure UDP relay. The UDP Relay General Configuration tab is displayed.

5 Configure the following parameters in the UDP BOOTP/DHCP Relay General Configuration panel.

- Forwarding Delay (seconds)
- Maximum Hops
- Forwarding Option

6 If you need to use the DHCP Option-82 functionality, configure the following parameters in the Relay Information Configuration panel.

- Relay Agent Information Mode
- Relay Agent Information Policy

7 If you need support for PXE devices, configure the PXE Support parameter.

Note — For VRF instances on the OS 9700E and OS 9800E NEs, the following parameters are read only:

- Forwarding Delay (seconds)
- Maximum Hops
- Relay Agent Information Mode
- Relay Agent Information Policy
- PXE Support

The values of these parameters are updated automatically if the corresponding value is modified under the default VRF instance.

8 Click on the DHCP Snooping tab button to configure DHCP snooping.

9 Configure the following parameters:

- DHCP Snooping Mode
- Bypass Option-82 Check
- Option-82 Format Type
- MAC Address Verification
- Option-82 Data Insertion
- Binding Database Mode
- Synchronization Timeout (seconds)
- Action
- Binding Persistency

If you selected the User String option for the Option-82 Format Type parameter, configure the Option-82 User String parameter.

10 Configure UDP port relay services, if required. Click on the Relay Services tab button.

11 Click on the Add button.

12 Configure the UDP Relay Service parameter.

If you selected the Other option, configure the Relay Service Port and Relay Service Description parameters.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button.

15 Click on the Relay Destinations tab button.

16 Click on the Add button. The Create UDP Service Destinations form opens with the Select Relay Service step displayed.

17 Click on the Select button. The Select UDP Service-UDP Relay Service Destination form opens.

18 Choose a UDP relay service from the list. Click on the OK button.

19 If you selected BOOTP/DHCP (67/68) in step 18 and the parameter Forwarding Option is set to Standard, click on the Next button. Otherwise, go to step 22.

20 The Forwarding Address step is displayed.

21 Configure the Forwarding Address parameter, if required.

22 Click on the Next button. The Select VLANs step is displayed.

23 Configure the search filter and click on the Search button. The Select VLANs form displays the VLANs that match the search criteria.

24 Choose one or more VLANs to be used to forward the UDP traffic.

25 Click on the Finish button. The Create UDP Service Destinations form closes and the selected VLANs appear in the relay destinations list.

Procedure 27-4 To create an L3 interface

This procedure describes how to create L3 interfaces. The interfaces you can configure include the following:

- L3 network interface
- ICMP interface
- system interface
- management interface
- VRRP instance
- IGMP interface
- PIM interface
- MLD interface

1 Choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→Router→Routing Instance.

3 Create a new L3 interface by right-clicking on the routing instance icon and choose Create Interface. The Create Network Interface form opens.

Note — The steps that appear on the Create Network Interface form vary, depending on the device type, device version, and the options that are selected during configuration.

4 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- IPv6 Allowed
- MAC Address
- Allow Directed Broadcasts
- Class
- Loopback Enabled
- PIM RP Delayed Up Period
- Cflowd Type
- Trusted
- Admin Link Local Address
- Admin Link Local Address Preferred
- Strip Label
- LDP Synchronization Timer

5 Click on the Next button and perform one of the following:

a If you chose Numbered in the Class parameter in step 4, the Configure IP Address form opens. Specify the IP address information for the L3 interface:

i Click on the Add button. The IP Address (Create) form opens.

ii Configure the parameters:

- IP Address
- Prefix Length
- IGP Inhibit
- Broadcast Address Format
- EUI-64
- IP Address Preferred

The Broadcast Address Format parameter only appears if the IP Address parameter is set to an IPv4 address.

The EUI-64 and IP Address Preferred parameters only appear if the IP Address parameter is set to an IPv6 address.

iii Click on the OK button to save the changes. A dialog appears.

iv Click on the OK button. The IP Address (Create) form closes and the Configure IP Address form reappears.

b If you chose Unnumbered for the Class parameter in step 4, the Configure Unnumbered Interface form opens. Configure the parameters:

- Unnumbered Type
- Unnumbered Reference

6 Click on the Next button. The Select Port form opens.

Note — If the Loopback Enabled parameter is selected on the Define General Properties form, The Select Port step does not appear in the step menu for the 7450 ESS, 7750 SR, 7705 SAR, and 7710 SR.

7 Associate the L3 interface with a physical port.

i Click on the Select button. The Select Port form opens.

ii Choose a port from the list.

iii Click on the OK button. The port is associated with the L3 interface.

8 Click on the Next button. The Select Network Policy form opens.

9 Click on the Select button in the Network Policy panel to list and choose a network policy for the interface. Network policies are used to determine QoS settings based on the packet DSCP bits on the ingress and egress of the network.

Note — If you select a network policy with a forwarding class mapped to a queue group queue ID, you must ensure that the mapping queue group queue ID is in the selected Queue Group Template Policy.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

10 Click on the Select button beside the Queue Group Template Policy to list and choose a network egress queue group template policy for the interface. Queue group template policies allow SAP or IP interface forwarding classes to be redirected from the typical queue mapping to a shared queue.

Note — You must ensure that the port you selected in step 7 has a network egress queue group with the same name as the Queue Group Template policy created on it.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

11 Click on the Next button. The Select ACL Filters form opens.

12 Click on the Select buttons to list and choose Ingress and Egress IPv4 and IPv6 ACL filters for the interface. ACL filters are used to filter out IP traffic that matches user-defined criteria.

13 Click on the Next button. The Configure ICMP form opens.

Configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

14 Click on the Next button. If the IPv6 Allowed parameter in step 4 is enabled, the Configure ICMPv6 form opens. Otherwise, go to step 15.

Configure the parameters:

- Redirects
- Unreachables
- Packet Too Big
- Param Problem
- Time Exceeded
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of Packet Too Big
- Packet Too Big Time (seconds)
- Number of Param Problem
- Param Problem Time (seconds)
- Number of Time Exceeded
- Time Exceeded Time (seconds)

15 Click on the Next button. The Configure ARP form opens.

i Configure the Timeout (seconds) parameter.

ii Click on the Add button to statically associate an IP or MAC address to the interface. The Static ARP (Create) form opens.

Configure the parameters:

- IP Address
- Physical Address

iii Click on the OK button. The Static ARP (Create) form closes.

16 Click on the Next button. The Configure Proxy ARP form opens.

Proxy ARP allows a device, such as a router, to answer ARP requests that are intended for another device. This allows a device to reach a remote subnet without configuring routes to the subnet or a default gateway device.

17 Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP

18 Click on the Next button. The Configure Proxy ARP Policies form opens.

19 Configure the parameters:

- Proxy Arp Policy 1
- Proxy Arp Policy 2
- Proxy Arp Policy 3
- Proxy Arp Policy 4
- Proxy Arp Policy 5

20 Click on the Next button. If the IPv6 Allowed parameter in step 4 is enabled, the Configure Neighbor Discovery form opens. Otherwise, go to step 26.

21 Click on the Add button to configure a neighbor. The Neighbor Discovery (Create) form opens.

22 Configure the parameters:

- IP Address
- Physical Address

23 Click on the OK button. The Neighbor Discovery (Create) form closes and the Configure Neighbor Discovery form reappears.

24 Click on the Next button. The Configure Proxy Neighbor Discovery form opens.

25 Configure the parameters:

- Enable Local Proxy
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Note — You must not leave an empty policy parameter between two configured policy parameters. For example, do not configure the Policy 1 and Policy 3 parameters and leave the Policy 2 parameter unconfigured. The 5620 SAM reorders the policies and moves the policy entered for the Policy 3 parameter to the Policy 2 parameter.

26 Click on the Next button. The Configure NTP form opens.

27 Configure the Broadcast parameter.

Note — When the Broadcast parameter is enabled, a time protocol such as NTP or SNTP must be enabled and configured on the device, or the device ignores broadcast time packets received on the interface. See chapter 12 for information about configuring NTP or SNTP on a device.

28 Click on the Next button. The Configure DHCP - General form opens.

29 Configure IPv4 DHCP for the interface, if required.

i Configure the parameters:

- Enable DHCP Relay
- Description
- Action
- Circuit ID
- Remote ID
- Remote ID String
- Copy to Option 43

Note — The Remote ID String parameter is configurable when the Remote ID parameter is set to Remote IDString.

ii Click on the Next button. The Configure DHCP - Server form opens.

iii Configure the Server 1 through Server 8 parameters.

30 Click on the Next button. The Configure VRRP form opens.

VRRP instances are members of a virtual router that provides backup if a router fails in a statically configured LAN. VRRP instances are created from network interfaces on a router, either as a master owner through which IP packets are routed before a failover or as a backup non-owner that assumes the packet-forwarding (master) role after a failover. Before you create or add a VRRP instance to a virtual router, ensure that the master and backup interfaces have the same VRID and occupy the same subnet.

31 Perform one of the following:

a If a VRRP instance is not required, click on the Next button until the Unicast RPF form opens in step 40.

b If an IPv4 VRRP instance is required, click on the Add button. The VRRP Instance (Create) form opens with the General tab displayed. See chapter 36 for information about VRRP instances and virtual routers.

c If an IPv6 VRRP instance is required, click on the Next button. The Configure IPv6 VRRP form is displayed. Click on the Add button and the VRRP IPv6 Instance (Create) form opens with the General tab displayed. See chapter 36 for information about VRRP instances and virtual routers.

32 Click on the Next button. The Configure Router Advertisement form opens.

33 Click on the Add button to add a router advertisement entry. The Router Advertisement (Create) form opens with the General tab displayed.

34 Configure the parameters:

- Send Advertisement
- Min Interval (seconds)
- Reachable Time (milliseconds)
- Managed Address Config
- MTU
- Use Virtual MAC Address
- Max Interval (Seconds)
- Retransmit Time (milliseconds)
- Other Stateful Config
- Current Hop Limit
- Lifetime (seconds)

If you are configuring the L3 interface for an IPv6 VRRP instance, then the Send Advertisement and Use Virtual MAC Address parameters must both be enabled.

35 Click on the Prefix tab button.

36 Click on the Add button. The Router Advertisement Prefix (Create) form opens.

37 Configure the parameters:

- IPv6 Prefix
- Prefix Length
- On-Link Determination
- Autonomous Address Configuration
- Lifetime (seconds)
- No Expiry
- Lifetime (seconds)
- No Expiry

Note — Each Lifetime (seconds) parameter is configurable when the associated No Expiry parameter is disabled.

38 Click on the OK button. A dialog box appears.

39 Click on the OK button. The Router Advertisement Prefix (Create) form closes.

40 Click on the Next button. The Unicast RPF form opens.

41 Configure the parameters:

- URPF Check State
- URPF Check Mode

42 Click on the Next button. The Configure Network Domain form opens.

43 Configure the parameters. You can Add Network Domain or Remove Network Domain and click on the Finish button. The Summary form opens.

44 Enable the View the newly created Network Interface parameter to view the interface configuration after closing the form, if required.

45 Click on the Close button. The Create Network Interface form closes.

46 If the View the newly created tunnel parameter in step 44 is enabled, the Network Interface (Edit) form opens with the newly created interface configuration displayed. To configure BFD on the network interface, go to step 47.

47 Configure Bi-directional Forwarding Detection for the interface, if required.

i Click on the BFD tab button. A configuration form opens.

ii Set the Admin Status parameter to Up. The configuration form is refreshed with additional parameters.

iii Configure the parameters:

- Admin Status
- Transmit Interval
- Receive interval
- Echo Interval
- Multiplier

iv To view local and remote session peers, click on the BFD Session tab button. 5620 SAM retrieves information from local and remote nodes and displays a list of BFD current sessions on router interfaces or L3 interfaces.

v Click on a session. A properties window opens for the session. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

The BFD Status field indicates one of the following:

- "no service", when BFD is disabled
- "in service", when BFD is running
- "out of service", when BFD has failed

vi Click on the OK button.

Note — You cannot enable BFD on an interface, if BFD is not configured on the interface. You cannot set the administration status of an interface to disabled, when protocols using the interface have BFD enabled. See chapter 28 for information about enabling and disabling BFD for routing protocols.

Procedure 27-5 To create an OmniSwitch L3 interface

An L3 interface enables IP routing on a VLAN. Without an L3 interface, traffic is bridged within the VLAN or across connections to the same VLAN on other switches.

1 Choose Routing from the navigation tree view selector.

2 Navigate to an OmniSwitch routing instance by choosing Network→OmniSwitch →Routing Instance.

3 Right-click on the routing instance icon and choose Create Interface from the contextual menu. The Create Network Interface form opens with the Define General Properties form displayed.

4 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Configured Primary Status
- Enable Forwarding

5 Click on the Next button. The Configure IP Address form opens.

6 Click on the Add button. The IP Address (Create) form opens.

7 Configure the parameters:

- IP Address
- Prefix Length

8 Click on the OK button. The IP Address (Create) form closes and a dialog box appears.

9 Click on the OK button.

10 Click on the Next button. The Configure Proxy ARP form opens.

11 Configure the Enable Local Proxy ARP parameter.

12 Click on the Next button. The Select VLAN form opens.

13 Click on the Select button. The Select VLAN - Network Interface form opens.

14 Choose a VLAN to which you want to add the interface.

15 Click on the OK button. The Select VLAN - Network Interface form closes.

16 Click on the Finish button. The Summary form opens.

17 Select the View the newly created Network Interface parameter to view the interface configuration after you close the Summary form, if required.

18 Click on the Close button. The Create Network Interface form closes.

Procedure 27-6 To configure an L3 interface

This procedure describes how to configure L3 interface parameters. The interfaces you can modify include the following:

- L3 network interface
- ICMP interface
- system interface
- management interface
- VRRP instance
- IGMP interface
- PIM interface
- MLD interface

1 Choose Routing from the navigation tree view selector.

2 Navigate to a network interface. The path is Routing→Router→Routing Instance→Interface.

3 Select an interface and choose Properties from the right-click contextual menu. The Network Interface (Edit) form opens.

4 Click on the appropriate tab button and configure the parameters, if required. Table 27-4 describes the tabs to choose, as shown when you modify an existing routing interface.

Table 27-4 Description of Network Interface configuration form tabs

Tab	Description
General	Configure the parameters: • Description • Administrative State • IPv6 Allowed • MAC Address • Allow Directed Broadcasts • Class • PIM RP Delayed Up Period • Cflowd Type • LDP Synchronization Timer • Loopback Enabled • Trusted
Port	To create an association between the L3 interface and a physical port or channel. The system interface is not associated with a port.
Policies	To associate network policies and ingress or egress IP ACL filter policies with the network interface.
Protocols	To view a list of protocols that are enabled on the interface, and to apply protocols. The protocols are: • MPLS • OSPFv2 • OSPFv3 • LDP • IS-IS • RIP
Multicast	To view a list of multicast protocols that are enabled on the interface, and to apply protocols. The protocols are: • PIM • IGMP • MLD
Local DHCP Servers	To assign local DHCP servers. Local DHCP servers are configured on the routing instance and VPRN service. They must be assigned to a network or an L3 interface.
Security	To assign a DoS protection policy to a network interface.
RCA Result	To view the results of RCA activities on the network interface
Address	To assign an IP address, subnet and broadcast address format to a network interface. Only one primary IP address can be associated with a network interface.
BFD	To configure BFD parameters

(1 of 2)

Tab	Description
ARP	To configure or view ARP and proxy ARP parameters. Click on the General tab button to configure the minimum time, in seconds, that an ARP entry is stored in the ARP table. Click on the Add button to configure static ARP IP and MAC address parameters. Click on the Proxy ARP tab button to view parameter information.
ICMP	To configure ICMP parameters
ICMPv6	If IPv6 is enabled on the interface, to configure ICMPv6 parameters
Neighbor Discovery	To configure neighbor discovery and proxy neighbor discovery for static routes. Click on the General tab button and Add button to configure neighbor discovery IP and MAC address parameters. Click on the Proxy ND tab button to configure proxy neighbor discovery parameters. (1)
VRRP	To add a VRRP instances to an existing virtual router that assumes routing responsibilities from a failed router in a statically configured LAN
Advertisement	To configure router advertisement
DHCP	To configure DHCP Relay parameters
NTP	To enable SNTP broadcasts on the network interface
Statistics	To view L3 network interface statistics
Faults	To view alarms that are raised against the network interface, or related alarms that affect the network interface

(2 of 2)

Note
(1) The Proxy ND tab is available only on the 7750 SR.

5 Click on the Apply button to save the changes.

6 Close the form.

7 Cable the network ports or channels of the device, with L3 interfaces enabled, to other devices configured the same way.

8 Configure routing protocols, as described in chapter 28.

Procedure 27-7 To configure an OmniSwitch L3 interface

1 Choose Routing from the navigation tree view selector.

2 Navigate to a network interface by choosing Network→ OmniSwitch →Routing Instance→Interface.

3 Choose an interface and choose Properties from the contextual menu. The Network Interface (Edit) form opens.

4 Click on the appropriate tab button and modify the parameters, if required. Table 27-5 describes the tabs.

Table 27-5 Description of OmniSwitch network interface configuration form tabs

Tab	Description
General	Configure the parameters: • Description • Administrative State • Configured Primary Status • Enable Forwarding • Encap Type
VLAN	View properties of the VLAN to which the interface is assigned or assign a VLAN to the interface.
Address	Assign an IP address to a network interface or view properties of an assigned address. Only one primary IP address can be associated with a network interface.
ARP	Configure the Enable Local Proxy ARP parameter.
Faults	View alarms that are raised against the network interface, or related alarms that affect the network interface.

5 Click on the Apply button to save the changes.

6 Close the form.

Procedure 27-8 To configure a routing policy statement

See "Routing policies" in section 27.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→Statement from the 5620 SAM main menu. A Routing Policy Statement Manager window opens.

2 Click on the Create button.

3 Configure the parameters:

- Policy Statement Name
- Description
- Default Action
- Check Dependencies

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Perform one of the following:

a Click on the Components tab button. Select and right-click on Policy Statement Entry and choose Create Policy Statement Entry. The Policy Statement Entry (Create) form opens with the General tab displayed. Go to step 6.

b Click on the Policy Statement Entries tab button.

5 Click on the Add button. The Policy Statement Entry (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Entry ID
- Description
- Action

7 Perform one of the following:

a If you choose Accept, Next Entry, or Next Policy for the Action parameter, go to step 8.

b If you choose None or Reject for the Action parameter, go to step 14.

8 Click on the Action tab button.

9 Configure the parameters:

- Route Origin
- Route Preference
- BGP Local Preference
- Local Preference Set
- Use Next Hop
- Metric Action
- Metric Value
- OSPF, RIP, or ISIS Tag (Hex)
- Next Hop Type
- OSPF Route Type
- Advertise Next Hop Self
- Damping Profile Name

10 Click on the Path tab button.

11 Configure the parameters:

- BGP AS Path Name
- BGP AS Path Action
- BGP AS Prepend Number
- Prepend Count

12 Click on the BGP Community tab button.

13 Configure the parameters:

- Community Name 1
- Community Action 1
- Community Name 2
- Community Action 2

14 Click on the From Criteria tab button. The Policy Statement Entry (Create) form appears with the General tab displayed.

15 Click on the Select button beside the AS Path Name parameter. A Select Policy Statement Entry - Site form opens.

16 Choose an AS path from the list.

17 Click on the Ok button. The AS Path Name is refreshed with the selected AS Path.

18 Click on the Select button beside the Community List Name parameter. A Select Policy Statement Entry - Site from opens.

19 Choose a community from the list.

20 Click on the Ok button. The Community List Name is refreshed with the selected community.

21 Configure the parameters.

- Protocol
- Origin
- Interface Name
- Static Route Tag
- Family
- IS-IS Route Level
- IS-IS External Route
- OSPF Route Type
- OSPF Area
- OSPF Area Set
- Multicast Source IP Address
- Neighbor IP Address

22 Click on the Select button beside the Multicast Group Prefix List Name parameter. A Select Policy Statement Entry window opens.

23 Choose a policy from the list.

24 Click on the Ok button. The Multicast Group Prefix List Name parameter is refreshed with the selected policy.

25 Click on the Select button beside the IGMP Host Prefix List Name parameter. A Select Policy Statement Entry window opens.

26 Choose a policy from the list.

27 Click on the Ok button. The IGMP Host Prefix List Name parameter is refreshed with the selected policy.

28 Click on the Select button beside the Interface Name parameter. A Select Zone Index From Criteria Site window opens.

29 Choose a site from the list.

30 Click on the Ok button. The Interface Name parameter is refreshed with the selected site.

31 Click on the Select button beside the Neighbor Prefix List Name parameter. A Select Policy Statement Entry window opens.

32 Choose a policy statement from the list.

33 Click on the Ok button. The Neighbor Prefix List Name parameter is refreshed with the selected policy.

34 Click on the Prefix List tab button.

35 Configure the parameters.

- Prefix List 1
- Prefix List 2
- Prefix List 3
- Prefix List 4
- Prefix List 5

36 Click on the To Criteria tab button. The Policy Statement Entry (Create) form appears with the General tab displayed.

37 Configure the parameters.

- Protocol
- Instance ID
- All Instances
- IS-IS Route Level
- Neighbor IP Address

38 Click on the Select button beside the Neighbor Prefix List parameter. A Select Policy Statement Entry window opens.

39 Choose a policy from the list.

40 Click on the Ok button. The Neighbor Prefix List parameter is refreshed with the selected policy.

41 Click on the Select button beside the Interface Name parameter. A Select Zone Index To Criteria Site window opens.

42 Choose an interface from the list.

43 Click on the Ok button. The Interface Name parameter is refreshed with the selected site.

44 Click on the Prefix Lists tab button.

45 Configure the parameters.

- Prefix List 1
- Prefix List 2
- Prefix List 3
- Prefix List 4
- Prefix List 5

46 Click on the OK button. A dialog box appears.

47 Click on the OK button.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 43-1.

48 Configure the following routing-related policies, if required:

a To configure a prefix list policy, see Procedure 27-9.

b To configure a community policy, see Procedure 27-10.

c To configure a damping policy, see Procedure 27-11.

d To configure an AS path policy, see Procedure 27-12.

e To view a routing policy from a CLI session, see Procedure 27-13.

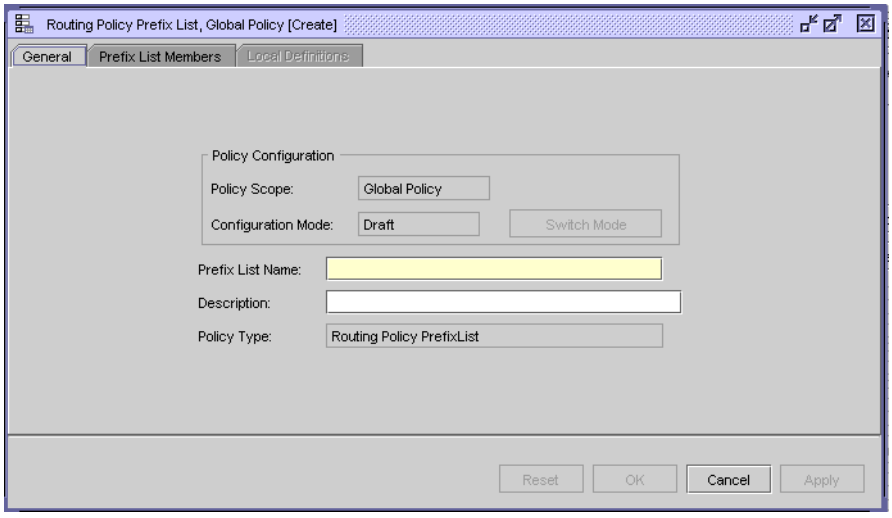
Procedure 27-9 To configure a prefix list policy

See "Routing policies" in section 27.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→Prefix List from the 5620 SAM main menu. A Routing Policy Prefix List Manager window opens.

2 Click on the Create button. The Routing Policy Prefix List (Create) form opens with the General tab displayed as shown in Figure 27-4.

Figure 27-4 Routing Policy Prefix List form- General



3 Configure the parameters:

- Prefix List Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Prefix List Members tab button.

5 Click on the Add button. The Prefix List Member (Create) form opens.

6 Configure the parameters:

- Prefix
- Mask
- Type
- Begin Length
- Through Length

The Begin Length and Through Length parameters are configurable when the Type parameter value is set to Range or Through.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Routing Policy Prefix List, Global Policy (Create) window appears with the newly created prefix member.

9 Close the Routing Policy Prefix List, (Create) window.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 43-1.

10 Configure the following routing-related policies, if required:

a To configure a policy statement, see Procedure 27-8.

b To configure a community policy, see Procedure 27-10.

c To configure a damping policy, see Procedure 27-11.

d To configure an AS path policy, see Procedure 27-12.

e To view a routing policy from a CLI session, see Procedure 27-13.

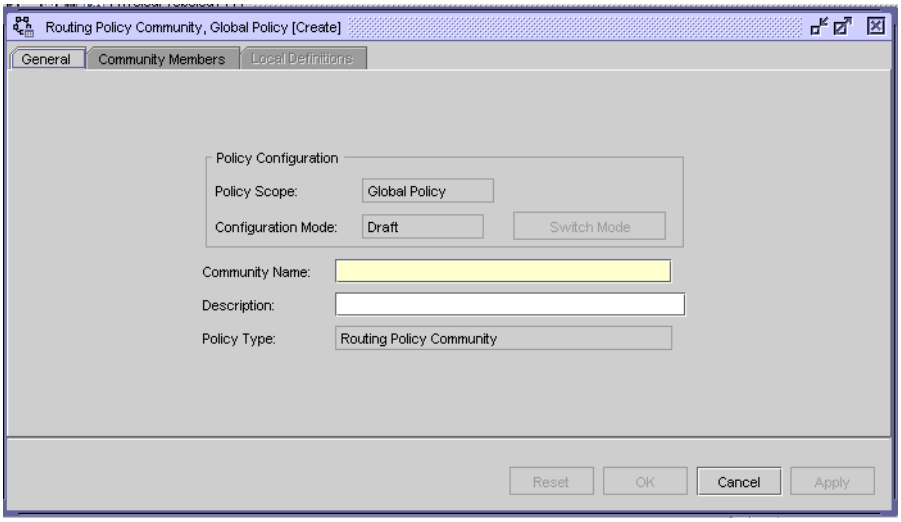
Procedure 27-10 To configure a community policy

See "Routing policies" in section 27.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→Community from the 5620 SAM main menu. A Manage Routing Policy - Community window opens.

2 Click on the Create button. A Routing Policy - Community, Global Policy (Create) form opens with the General tab displayed as shown in Figure 27-5.

Figure 27-5 Routing Policy Community form - General



3 Configure the parameters:

- Community Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Community Members tab button.

5 Click on the Add button. A Community Member Site (Create) window opens.

6 Configure the Community Member parameter.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Routing Policy Community (Create) window is updated with the newly created site.

9 Close the Routing Policy - Community, Global Policy (Create) window.

10 Close the Manage Routing Policy - Community window.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 43-1.

11 Configure the following routing-related policies, if required:

- **a** To configure a policy statement, see Procedure 27-8.
- **b** To configure a prefix list policy, see Procedure 27-9.
- **c** To configure a damping policy, see Procedure 27-11.
- **d** To configure an AS path policy, see Procedure 27-12.
- **e** To view a routing policy from a CLI session, see Procedure 27-13.

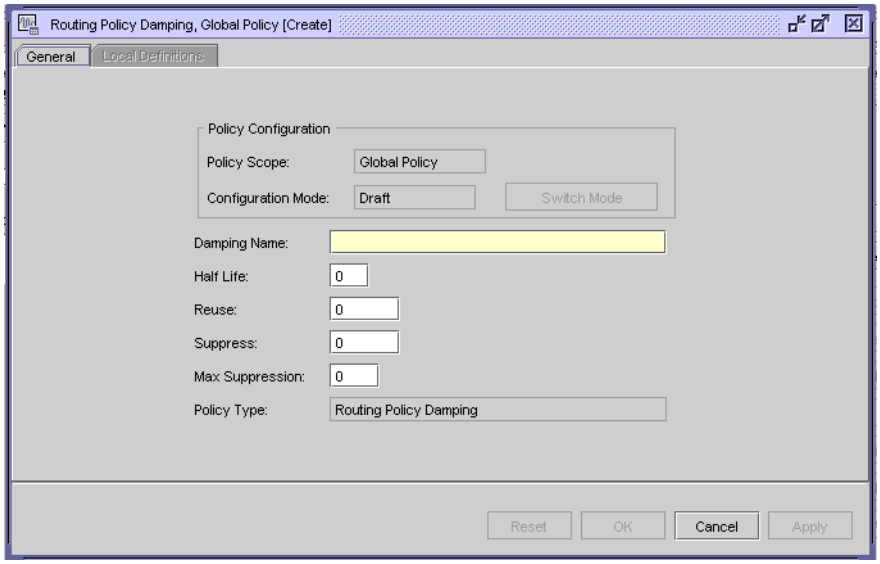
Procedure 27-11 To configure a damping policy

See "Routing policies" in section 27.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→Damping from the 5620 SAM main menu. A Manage Routing Policy - Damping window opens.

2 Click on the Create button. A Routing Policy - Damping, Global Policy (Create) form opens with the General tab displayed as shown in Figure 27-6.

Figure 27-6 Routing Policy Damping form - General



3 Configure the parameters:

- Damping Name
- Half Life
- Reuse
- Suppress
- Max Suppression

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button.

5 Close the Routing Policy - Damping, Global Policy (Create) window.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 43-1.

6 Configure the following routing-related policies, if required:

a To configure a policy statement, see Procedure 27-8.

b To configure a prefix list policy, see Procedure 27-9.

c To configure a community policy, see Procedure 27-10.

d To configure an AS path policy, see Procedure 27-12.

e To view a routing policy from a CLI session, see Procedure 27-13.

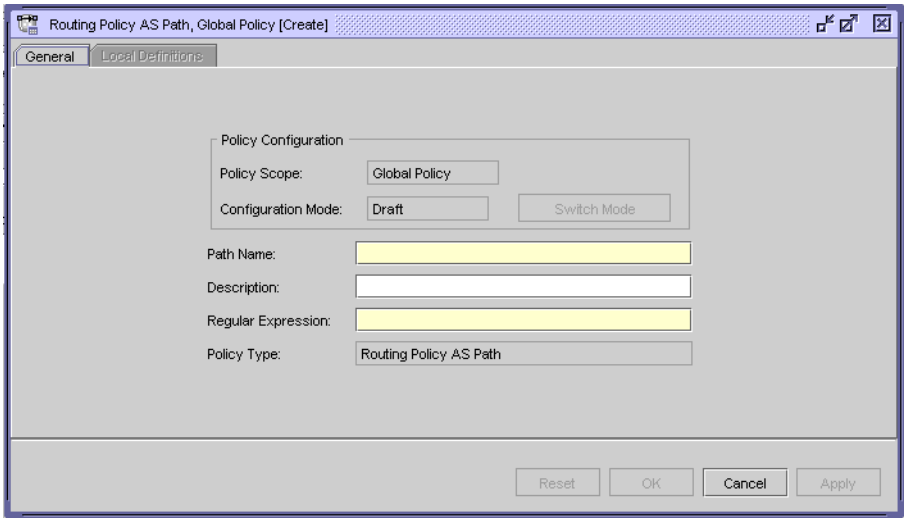
Procedure 27-12 To configure an AS path policy

See "Routing policies" in section 27.1 for more information about the use and purpose of routing policies.

1 Choose Policies→Routing→AS Path from the 5620 SAM main menu. A Manage Routing Policy - AS Path window opens.

2 Click on the Create button. An Routing Policy - AS Path, Global Policy (Create) window opens with the General tab displayed as shown in Figure 27-7.

Figure 27-7 AS Path Policy form - General



3 Configure the parameters:

- Path Name
- Description
- Regular Expression

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button.

Note — A routing policy is discovered as local edit only. To synchronize a routing policy with all NEs, you must change the distribution mode of the routing policy to sync with global. To configure the distribution mode, see Procedure 43-1.

5 Configure the following routing-related policies, if required:

a To configure a policy statement, see Procedure 27-8.

b To configure a prefix list policy, see Procedure 27-9.

c To configure a community policy, see Procedure 27-10.

d To configure a damping policy, see Procedure 27-11.

e To view a routing policy from a CLI session, see Procedure 27-13.

Procedure 27-13 To view a routing policy from a CLI session

To view a routing policy from a CLI session, navigate to the previously distributed local routing policy or view navigate to a routing instance by choosing Network→Router→Routing Instance. See Procedure 27-1 for more information.

1 Perform one of the following depending on which routing policy you want to view from a CLI session.

   a Choose Policies→Routing→Policy from the 5620 SAM main menu. A Routing Policy Statement Manager window opens.

   b Choose Policies→Routing→Prefix List from the 5620 SAM main menu. A Routing Policy Statement Manager window opens.

   c Choose Policies→Routing→Community from the 5620 SAM main menu. A Routing Policy Community Manager window opens.

   d Choose Policies→Routing→Damping from the 5620 SAM main menu. A Routing Policy Damping Manager window opens.

2 Click on the Search button. A list of policies appears.

3 Choose a policy from the list.

4 Click on the Properties button. A *Policy_type* (Edit) form opens.

5 Click on the Local Definitions tab button. A window appears displaying a list NEs to where the policy was distributed.

6 Choose a site from the list.

7 Click on the Properties button. A *Policy_type* Local Policy (Edit) form opens.

8 Click on the Show Policy button. A Routing Policy Show Policy window opens with the General tab displayed.

9 Click on the Ok button. A CLI display is initiated.

10 View the policy.

11 Click on the close button.

12 Close the A *Policy_type* Local Policy (Edit) form.

Procedure 27-14 To configure an MPLS administrative group policy

MPLS administrative group policies define administrative groups that can be assigned to MPLS interfaces, LSPs, and LSP paths. After you configure MPLS administrative groups, the administrative groups can be assigned to MPLS interfaces, LSPs, and LSP paths on their respective properties forms. Multiple administrative groups can be assigned to each of these objects.

When establishing LSP and LSP paths, devices are only consider MPLS interfaces which are associated with the same administrative group as the LSP or LSP path. MPLS interfaces advertise administrative group associations using CSPF. This is done using the 32 bit mask which you configure using the Value parameter on the MPLS administrative group policy form.

An administrative group can also be assigned to be explicitly excluded from LSPs and LSP paths. The device cannot use MPLS interfaces in the administrative group to establish LSPs or LSP paths. Administrative group exclusion takes priority over administrative group inclusion.

CSPF must be enabled on LSPs for administrative groups to be relevant. You can enable and configure CSPF on the LSP properties form. When CSPF is enabled on an LSP, it is automatically enabled on associated LSP paths. LSP paths can be configured on the LSP path properties form to inherit additional CSPF, administrative group, and other parameters from LSPs.

This procedure describes how to create MPLS administrative groups. Table 27-6 describes where to find information about assigning MPLS administrative groups to MPLS interfaces, LSPs, and LSP paths.

Table 27-6 MPLS administrative group assignments

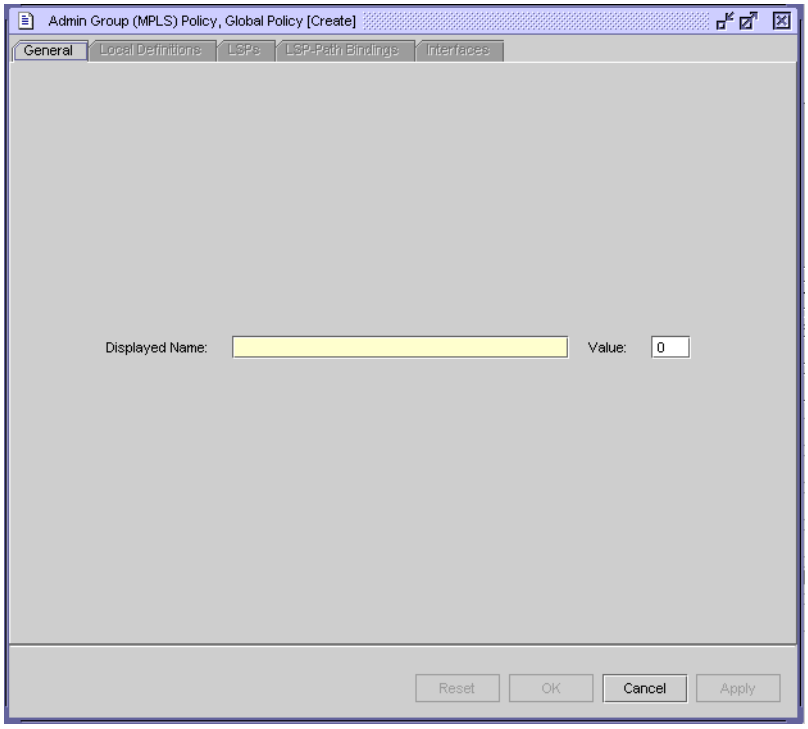
To assign groups to	See Procedure
MPLS interfaces	"To create an MPLS interface" in chapter 29
LSPs	"To create a static LSP" in chapter 29
LSP paths	"To configure an LSP path" in chapter 29
	"To configure a 7250 SAS-ES or 7250 SAS-ESA LSP" in chapter 29

1 Choose Policies→MPLS→Administrative Group from the 5620 SAM main menu. The Manage MPLS Administration Groups form opens.

2 Click on the Create button.

The Admin Group (MPLS) Policy (Create) form opens with the General tab displayed, as shown in Figure 27-8.

Figure 27-8 MPLS administrative group form - General



3 Configure the parameters:

- Displayed Name
- Value

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button to save the policy.

The Admin Group (MPLS) Policy (Edit) form is refreshed and the tabs are selectable. Table 27-7 describes the tabs that you can choose to configure the parameters.

Table 27-7 Description of MPLS administrative group form tabs

Tab	Description
Local Definitions	Lists MPLS administrative group policies and allows you to manage administrative group policy distribution.
LSPs	Lists and allows you to manage LSPs to which the administrative group has been assigned.
LSP-Path Bindings	Lists and allows you to manage LSP paths to which the administrative group has been assigned.
Interfaces	Lists and allows you to manage MPLS interfaces to which the administrative group has been assigned.
Faults	List and manage alarms related to the administrative group.

5 Click on the Distribute button to manually distribute the administrative group policy locally to managed devices. Policies are also automatically distributed to managed devices when they are used by resources on the device.

Procedure 27-15 To configure a Shared Risk Link Group policy

Shared Risk Link Groups, or SRLGs, are constructs which allow you to perform two operations that enhance overall system reliability. You can use SRLGs to establish a FRR LSP path. You can also use SRLGs to establish a secondary LSP path which is disjointed from the primary LSP path. Links that are members of the same SRLG represent resources which share the same risk. For example, fiber links sharing the same conduit, or multiple wavelengths sharing the same fiber.

An SRLG is modeled as a policy object. It therefore follows the normal policy behavior for creation, listing, updating, deletion, distribution, and re synchronization.

Configured SRLGs are associated with MPLS interfaces. The SRLGs are used by the CSPF when computing a FRR detour/bypass path, or a secondary LSP path. SRLGs indicate to the CSPF which interfaces to avoid in the path's computation.

This procedure describes how to create SRLG policies. Table 27-8 describes where to find information about related MPLS and LSP procedures.

Table 27-8 Related MPLS and LSP procedures

To:	See Procedure:
Configure an MPLS instance	"To configure an MPLS instance" in chapter 29
Create an MPLS interface	"To create an MPLS interface" in chapter 29
Configure LSP paths	"To configure an LSP path" in chapter 29

1 Choose Policies→MPLS→Shared Risk Link Group from the 5620 SAM main menu. The Manage Shared Risk Link Group Policies form opens.

2 Click on the Create button.

The Shared Risk Link Group, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Value

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button to save the policy.

The Shared Risk Link Group Policy (Edit) form is refreshed and the tabs are selectable. Table 27-9 describes the tabs that you can choose to configure the parameters.

Table 27-9 Description of Shared Risk Link Group Policy form tabs

Tab	Description
General	Displays information on the policy and allows you to prepare the policy for release and distribution.
Local Definitions	Lists Shared Risk Link Group policies and allows you to manage policy distribution.
Interfaces	Lists and allows you to manage MPLS interfaces to which the SRLG policy has been assigned.
Faults	List and manage alarms related to the SRLG.

5 Click on the Distribute button to manually distribute the SRLG policy locally to managed devices. Policies are also automatically distributed to managed devices when they are used by resources on the device. See chapter 43 for more information about policies and policy distribution.

Procedure 27-16 To create a static configuration for a SRLG Policy

This procedure describes how to create a static configuration for a SRLG policy. This differs from the standard SRLG policy described in Procedure 27-15 in that it allows you to manually enter into the SRLG database the SRLG membership for links in the entire network. This is typically done at the 7x50 head-end node and is mutually exclusive with the reading of this information from the traffic engineering database.

There are deployments where the 7x50 head-end node interoperates with routers that do not implement the SRLG membership advertisement using IGP SRLG Type-Length Value (TLV) or sub-TLV. In these situations, you can manually enter the link members of SRLG groups for the entire network at any 7x50 node which needs to signal LSP paths, such as a head-end node.

1 Choose Policies→MPLS→Shared Risk Link Group Static Configuration from the 5620 SAM main menu. The Manage Shared Risk Link Group Static Configuration form opens.

2 Click on the Create button.

The Static Configuration for SRLGs Policy (Create) form opens with the General tab displayed.

3 Configure the Displayed Name parameter.

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button to save the policy.

The Static Configuration for SRLGs Policy (Edit) form is refreshed and the tabs become selectable. Table 27-10 describes the tabs that you can choose to configure parameters or view fault information.

Table 27-10 Description of Static Configuration for SRLG Policy form tabs

Tab	Description
General	Displays information on the policy and allows you to prepare the policy for release and distribution.
Local Definitions	Lists Static Configuration for SRLG policies and allows you to manage policy distribution.
Routers	Lists and allows you to manage existing static configuration entries or add new ones.
Faults	List and manage alarms related to the static configuration for SRLGs.

5 Click on the Routers tab button.

6 Click on the Add button. The Router for Static Config for SRLG policy (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Router Id
- Admin State

8 Click on the OK button, and then click OK in the confirmation box that appears. The router(s) you added appears in the list on the Routers tab.

9 If you want to add other routers, repeat steps 6 and 7, otherwise, go to step 10.

10 Select one of the routers from the list and click on the Properties button. The Router for Static Config for SRLG policy (Create) window opens with the General tab displayed.

11 Configure the Admin State parameter.

12 Click on the Interfaces tab.

13 Configure the Interface Ip Address parameter. You can enter this manually or use the Select button to choose from a list.

14 Configure the Displayed Name parameter.

Note — You can associate the same Interface Ip Address parameter with more than one SRLG.

15 Click on the Apply button and repeat steps 10 to 14 to add other entries, or click OK to close the Static Configuration for SRLGs policy (Create) window.

16 If you clicked on Apply in the previous step, you can click on the Distribute button to manually distribute the Static Configuration for SRLGs policy locally to managed devices. Policies are also automatically distributed to managed devices when they are used by resources on the device. See chapter 43 for more information about policies and policy distribution.

Procedure 27-17 To create a static route

1 Choose Routing from the navigation tree view selector.

2 Navigate to the static routes icon. The navigation path is Routing→Router→Routing Instance→Static Routes.

3 Right-click on the static routes icon and choose Create Static Route from the contextual menu. The Static Route (Create) form opens.

4 Configure the parameters:

- Auto-Assign ID
- Static Route ID
- BFD Enabled
- Destination
- Prefix Length
- Multicast Capable Peers
- Type
- IP Address
- Interface Name
- Unnumbered Interface
- Preference
- Metric
- Administrative State
- Tag
- LDP
- Disallow IGP
- Enable CPE Check
- Target IP Address
- Interval (seconds)
- Drop Count
- Log
- Prefix List Name
- Prefix List Flag

The IP Address parameter is configurable when the Type parameter is set to an option other than Black Hole.

The Target IP Address, Interval (seconds), Drop Count, and Log parameters are only displayed when Enable CPE Check is enabled.

You cannot specify a Prefix List if either BFD Enabled or Enable CPE Check parameters are enabled for the static route.

The Prefix List Flag parameter is only displayed once the Prefix List Name parameter is configured.

5 If IPv6 is enabled on the routing instance, click on the Select button beside the Interface Name parameter to choose an IPv6 zone index for the static route. The Select Zone Index - Static Route form opens. Otherwise, go to step 7.

6 Select a zone index in the list and click on the OK button. The Select Zone Index - Static Route form closes and the zone index is displayed in the Static Route (Create) window.

7 Click on the OK button. The Static Route (Create) form closes.

Procedure 27-18 To configure an OmniSwitch static route

1 Choose Routing from the navigation tree view selector.

2 Navigate to the static routes icon by choosing Network→OmniSwitch or→Routing Instance→Static Routes.

3 Right-click on the static routes icon and choose Create Static Route from the contextual menu. The Static Route (Create) form opens.

4 Configure the parameters:

- Auto-Assign ID
- Static Route ID
- Destination
- Prefix Length
- Type
- IP Address
- Metric

Note — If the address entered for the IP Address parameter is unreachable by the node, the static route is not created on the node. Use the 5620 SAM to verify that all configured static routes are created successfully on the node by checking the list of static routes for the OmniSwitch routing instance.

5 Click on the OK button to save the configuration. The Static Route (Create) form closes.

27.4 Network domain overview

The 5620 SAM allows you to create, delete, associate and edit network domains. You can use the network domains view in the 5620 SAM GUI navigation tree to manage these functions. Network domains help determine which network ports are eligible to transport traffic of individual SDPs. This information is used for the SAP-ingress queue allocation which is applied to VPLS SAPs. No SAP-ingress queues are allocated if a given port does not belong to the network domain used in a VPLS.

Note 1 — A maximum of four network domains are supported in any VPLS.

Note 2 — If an SDP is used for E-PIPE, I-PIPE or A-PIPE bindings, the network domain configuration is not considered.

Note 3 — Network domains are not applicable to loopback and system interfaces.

By default, all network interfaces in a routing instance belong to the default network domain. You can associate an interface to any user defined network domain. The loopback and system interfaces cannot be associated with user defined network domains.

An SDP can be assigned to only one network domain. If no user defined network domain is created, an SDP will be assigned to the default network domain. All SAPs in VPLS will have a queue reaching all fwd complexes serving interfaces belonging to the same network domains as the SDPs. You can assign or remove a network domain association of the interface or SDP without deleting the respective object.

Procedure 27-19 To create a network domain

1 Choose Routing from the navigation tree view selector.

2 Navigate to the network domains icon by choosing Network→NE→Routing Instance→Network Domains.

3 Right-click on the network domains icon and choose Create Network Domain from the contextual menu. The Network Domain (Create) form opens.

4 Enter:

- Domain Name
- Description

5 Click on the OK button. The Domain Network (Create) form closes and a network domain is created in the navigation tree.

Procedure 27-20 To delete a network domain

1 Choose Routing from the navigation tree view selector.

2 Navigate to the network domains icon by choosing Network→NE→Routing Instance→Network Domains.

3 Right-click on the network domains icon and choose Delete from the contextual menu. A Confirm dialog box opens.

Caution 1 — The default network domain cannot be deleted.

Caution 2 — The network domain related to the Interface and SDP cannot be deleted.

4 Perform one of the following:

a Click on the No button to avoid deleting the network domain. The Confirm dialog box closes.

b Click on the Yes button. The network domain is deleted from the navigation tree.

Procedure 27-21 To associate a network interface with a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Network Interfaces tab and click on Add Network Interface. The Add Network Interface window opens.

4 Click on Search to display all the Network Interfaces. Select a Network Interface and click on OK the selected Network Interface is displayed on the Network Domain window.

Procedure 27-22 To remove a network interface from a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Network Interfaces tab and select the Network Interface that has to be removed from the domain.

4 Click on Remove Network Interface.

5 A Confirm dialog box opens.

Perform one of the following:

a Click on the No button to avoid removing the network interface. The Confirm dialog box closes.

b Click on the Yes button. The network interface is removed from the network domain.

Procedure 27-23 To associate a service tunnel with a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Service Tunnels tab and click on Add Tunnel. The Add Tunnel window opens.

4 Click on Search to display all the service tunnels. Select a service tunnel and click on OK the selected service tunnel is displayed on the Network Domain window.

Procedure 27-24 To remove a service tunnel from a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance→Network Domains→domain-userdomain.

3 Click on the Service Tunnels tab and select the service tunnel that has to be removed from the domain.

4 Click on Remove Tunnel.

5 A Confirm dialog box opens.

Perform one of the following:

a Click on the No button to avoid removing the service tunnel. The Confirm dialog box closes.

b Click on the Yes button. The service tunnel is removed from the network domain.

Procedure 27-25 To edit a network domain

1 Choose Routing from the navigation tree view selector.

2 Choose Network→NE→Routing Instance

3 Choose the newly created interface and right-click on the Interface and select Properties. The Network Interface form opens. See Procedure 27-4, steps 42 and 43 to associate a network interface to a network domain.

4 Select the Network Domain tab. The Network Domain form opens. See Procedure 27-4, steps 42 and 43 to edit a network domain.

28 — Protocol configuration

28.1 Protocol configuration overview

The 5620 SAM allows you to configure routing protocols and navigate to the device parameters. One device can support multiple routing protocols.

You use the network, IS-IS, and OSPF views in the 5620 SAM GUI navigation tree to view and configure parameters that set and manage the device routing protocol support. The routing protocols are enabled on the devices when you configure the devices. You configure the Layer 3 interfaces when you configure the routing instance on the device. You can then configure the routing protocols for specific Layer 3 interfaces.

Supported routing protocols include:

- BGP
- RIP
- OSPF
- RSVP
- LDP
- IS-IS
- L2TP

Routing protocols can be configured to import or export routes from other routing protocols using routing policies. See "Routing policies" in section 27.1 for more information.

In addition to routing protocols, the 5620 SAM supports the following router configurations:

- multicast protocols
  - PIM; see "PIM configuration" in section 28.3 for more information
  - IGMP; see "IGMP configuration" in section 28.3 for more information
  - MSDP; see "MSDP configuration" in section 28.3 for more information
  - MLD; see "MLD configuration" in section 28.3 for more information
- bridging on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch devices; see "Bridging configuration" in section 28.3 for more information

IPv6 support

The 5620 SAM supports IPv6 for control-plane addressing on the 7750 SR in chassis mode C and D, on the 7710 SR, and on the 7450 ESS in mixed mode. See chapter 15 for information about chassis modes.

Although the implementation of IPv6 is driven by the diminishing IPv4 address space, it is increasingly necessary to use a protocol that is designed to handle more complex network applications, such as broadband voice and video transmission, IP transit, Internet exchange peering, and other large enterprise applications.

Transition from IPv4 to IPv6

The transition from IPv4 to IPv6 is occurring in stages as network providers, service providers, and end users migrate existing applications and equipment to the new version. Control-plane forwarding of IPv6 packets is an important part of this transition; it allows isolated IPv6 hosts and smaller IPv6 networks to peer across an IPv4 network, using a mechanism such as 6over4 tunneling.

With 6over4 tunneling, a host encapsulates IPv6 packets in IPv4 packets for transport across an IPv4 network. Routers that identify 6over4 encapsulation remove the IPv4 encapsulation before they forward the packets to other native IPv6 hosts. The 6over4 mechanism uses the IPv4 multicast infrastructure for neighbor discovery.

IPv6 benefits

The general benefits of IPv6 include:

- **simplified header format and fixed header length**
  An IPv6 header contains fewer fields than an IPv4 header. IPv6 excludes obsolete IPv4 header fields and processes option fields only when they contain values. IPv6 also standardizes the size of the packet header to 40 bytes to streamline packet processing. These features reduce packet-processing overhead and make routing more efficient.
- **addressing enhancements**
  IPv6 increases the IP address size from 32 bits to 128 bits to support a greater number of nodes and to provide a more versatile addressing hierarchy. IPv6 also supports address autoconfiguration.
  The scalability of multicast routing is improved by the presence of a Scope field. IPv6 introduces anycast addressing, which designates a group of disparate nodes as the recipient of a specific data stream.
- **improved scalability and extensibility**
  Built-in traffic optimization makes IPv6 highly scalable, and IPv6 supports future routing technology enhancements using protocol extensions.
- **flow-labeling capability**
  IPv6 features packet prioritization which allows the labeling of packets that require special handling, such as real-time service for VoIP conferences.
- **improved privacy and security**
  Authentication, encryption, and data integrity features are mandatory components for which IPv6 supports standardized extensions.

The 5620 SAM and IPv6

The 5620 SAM entities that support IPv6 configuration include the following:

- BGP for base routing instances and VPRN services
- IS-IS adjacencies
- multicast routing
- static routes
- ICMP
- routing policies

- access ingress and egress policies
- CPM filter policies
- PPP
- IES and VPRN SAPs
- IES and VPRN bi-directional forwarding detection
- VLL Ipipe
- PIM-SSM

A 5620 SAM operator enables IPv6 on an interface during interface creation.

The benefits of the 5620 SAM IPv6 implementation include:

- integration with existing IPv4 configurations on many property and configuration forms
- automatic validation of IP addresses on the client GUI, regardless of the IP version
- support of compressed IPv6 addresses when repeated address octets are present
- support for IPv6 statistics
- simultaneous IPv4 and IPv6 support by routing protocols
- separate IPv4 and IPv6 administrative and operational states on an interface

Accepted IPv6 address formats

The 5620 SAM accepts IPv6 addresses in the following formats:

- colon-hexadecimal, or *x:x:x:x:x:x:x:x*
  where *x* is a 16-bit hexadecimal number from 0 to FFFF
- a combination of colon-hexadecimal and dotted-decimal, or *x:x:x:x:x:x:d.d.d.d*
  where
  x is a 16-bit hexadecimal number from 0 to FFFF
  d is an 8-bit decimal number from 0 to 255

Using a combination of colon-hexadecimal and dotted-decimal formats may be convenient in an environment that supports the use of IPv4 and IPv6 addresses.

The 5620 SAM allows IPv6 address compression for an address that contains repeated zero values. You can use two adjacent colons to represent any group of repeated zero values in an IPv6 address. For example:

2001:DB8::

expands to

2001:0DB8:0000:0000:0000:0000:0000:0000

It is not necessary to supply the leading zeros for a number in an IPv6 address. For example, 2001:DB8::3C:5 is a valid IPv6 address.

BGP

BGP is an inter-AS routing protocol. An AS is a network or a group of devices logically organized and controlled by a common network administration. BGP enables devices to exchange network reachability information. AS paths are the routes to each destination. There are two types of BGP: IBGP and EBGP.

- IBGP is used to communicate with peer devices in the same AS. Routes received from a device in the same AS are not advertised to other devices in the same AS but can be advertised to an EBGP peer.
- EBGP is used to communicate with peers in different ASs. Routes received from a device in a different AS can be advertised to both EBGP and IBGP peers.

See "Inter-AS connections" in section 71.1 for more information about connecting ASs in a VPRN.

You can use the 5620 SAM to enable BGP on the device and perform the following functions:

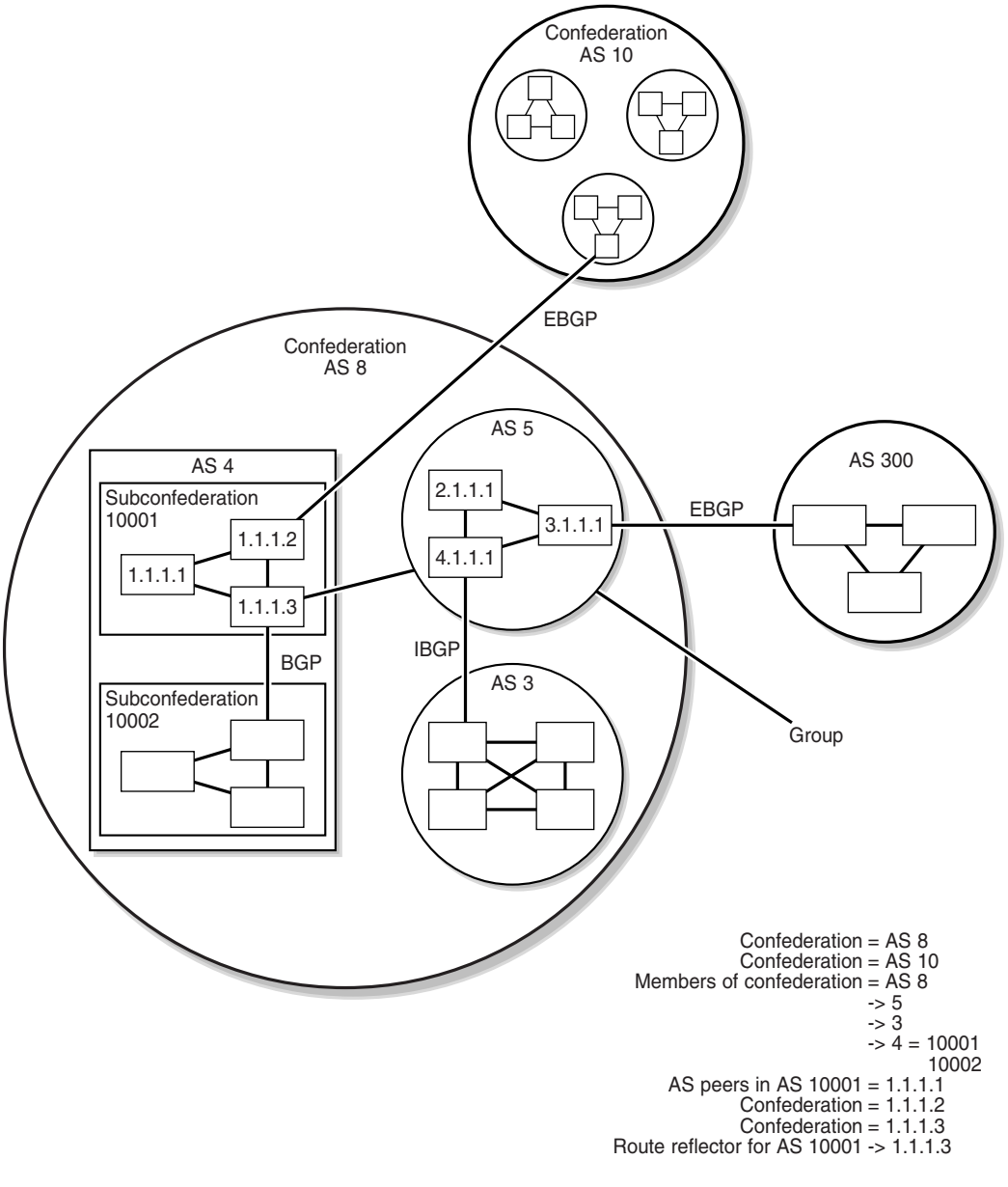
- set the AS values for the routing instance
- create confederations of group-managed devices
- create BGP peer groups
- create neighbors (peers) within the BGP peer groups

The 5620 SAM supports the configuration of IPv6 addresses for BGP peering on the base routing instance of the 7750 SR and the 7450 ESS in mixed mode.

A device can only belong to one AS. After the neighbor relationship is established between devices, they exchange BGP open messages, which contain information such as AS numbers, BGP versions, router IDs, hold-time values, and keepalive messages. This information determines the status of the BGP session. Peer relationships are defined by configuring the IP addresses of the devices that are peers of the local BGP system.

Figure 28-1 shows a simple BGP example using groups, subconfederations, and confederations.

Figure 28-1 BGP example



In a standard BGP configuration, all BGP-enabled devices within an AS have a full mesh of BGP peerings to ensure all externally learned routes are redistributed through the entire AS. This is needed because IBGP does not re-advertise routes learned from one IBGP peer to another IBGP peer. However, as more devices are added, scaling the IBGP mesh can become an issue. To solve this scaling issue, you can use:

- confederations
- subconfederations

Confederations are a way to subdivide a large AS into smaller ASs. Subconfederations further subdivide ASs. Within each smaller AS, or confederation, IBGP is still used, however EBGP is used between subconfederations. This means less meshing between peers is required.

Another method of subdividing an AS is route reflection. For route reflection, an AS is divided into groups called clusters. Each cluster contains at least one route reflector. The route reflector redistributes routing updates to all devices in its cluster. Because the route reflector provides all the routing updates, the other devices in the cluster do not maintain a BGP mesh.

MP-BGP

BGP distributes IP routing information between networks. The distribution of IP routing information between VPRNs requires MP-BGP. MP-BGP addressing uses an 8-byte RD with a 4-byte or 16-byte IP address, depending on whether IPv4 or IPv6 is used. The requirements for MP-BGP configuration are the following.

- MP-BGP must be enabled on the participating PE devices.
- All PE devices must be configured as BGP peers.

When PE devices learn routing information from the CE devices in a VPRN configuration, the routing information is shared using MP-BGP. The RD is used to associate the new routing information with a VPRN instance.

The PE devices distribute the route information to the other CE devices in the VPRN. Each learned route is assigned an MPLS label that is distributed to the devices.

When customer packets arrive at a PE device, the packets are encapsulated with the MPLS label that corresponds to the learned route for the packet destination.

The MP-BGP multicast extension can be applied to build separate routing tables for multicast paths. IGPs such as OSPF and IS-IS can import multicast and unicast routing information to the multicast and unicast routing tables. The multicast routing information can subsequently be used by PIM to perform RPF lookups.

RIP

RIP is an IGP that uses a distance-vector algorithm to determine the best route to a destination, using hop count as the deciding factor. In order for the protocol to provide complete information about routing, every device in the domain must participate in the protocol. RIP, a UDP-based protocol, updates its neighbors, and the neighbors update their neighbors.

Unlike OSPF and other link-state protocols, RIP directly advertises reachability information to its neighbors. RIP advertises reachability information by sending prefix, mask, and either hop count or cost metric data. Each device running the RIP protocol advertises all RIP devices periodically by sending RIP update PDUs. The route with the lowest metric is advertised as the best route.

The 5620 SAM supports the configuration of RIPv1 and RIPv2 on network and access interfaces.

LDP

LDP is used to distribute labels in non-traffic-engineered MPLS applications. Routers can establish LSPs across a network by mapping network-layer routing information directly to the data link layer switched paths. After the LDP distributes the labels to the LSR, the LSR assigns the label to a FEC, and then informs all other LSRs in the path about the label and how the label switches data accordingly.

A FEC is a collection of common actions associated with a class of packets. LDP helps establish the LSP by providing a set of procedures that LSRs can use to distribute labels.

When a service tunnel is configured on managed routers using LDP signaling in an MPLS environment, LDP sessions are set up based on the configured hello and other PDU values. If another service tunnel is created to the same destination, the LDP session is reused.

The LDP sessions between LSRs:

- find and establish LDP peers in the managed network
- exchange label mappings for each LSR
- exchange label bindings

After all the LSRs are LDP-aware and the LSP is created, forwarding can occur as follows:

1 A FEC is associated with the LSP.

2 The FEC maps the packets to the LSP.

3 The next LSR that is part of the LSP splices incoming FEC labels to the outgoing FEC label of the next hop.

There are two types of LDP:

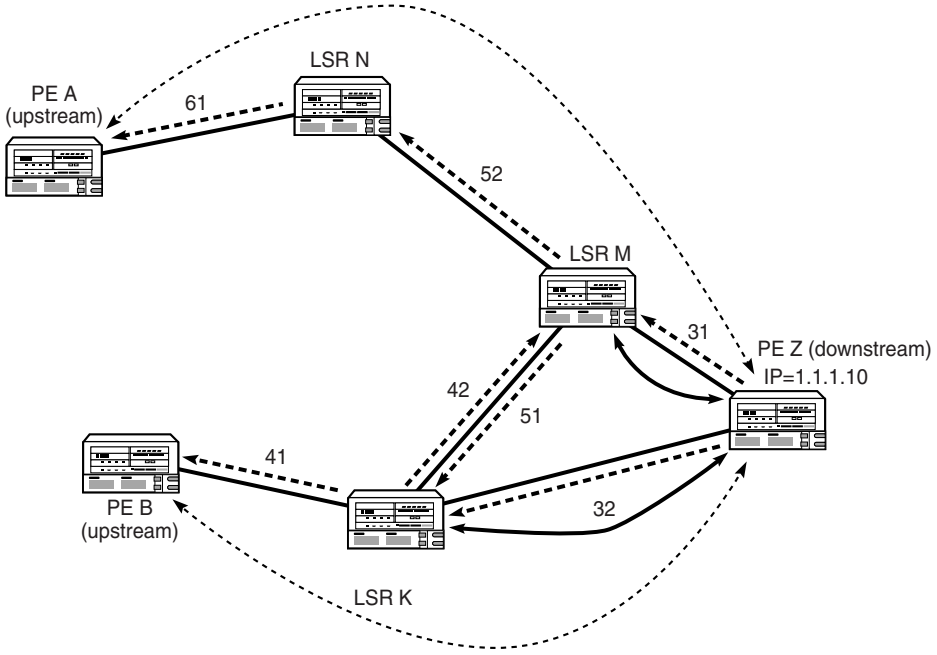
- T-LDP
- DU-LDP

T-LDP is used to distribute labels for VLL and VPLS. T-LDP allows the targeting of remote devices that are not directly connected as targeted peers.

DU-LDP can be used to create tunnels between PEs for IP-VPN services.

Figure 28-2 shows an example of LDPs that are used in a simple Layer 2 and Layer 3 service provider network.

Figure 28-2 LDP sample network



- The solid straight lines between the devices indicate IP connectivity. These are directly connected peers.
- The dotted bidirectional curved lines indicate T-LDP sessions. These are targeted peers that are not directly connected.
- The solid bidirectional curved lines indicate DU-LDP sessions. This example only shows two instances, between M and Z, and Z and K. If there is IP connectivity between all the devices, then all of the devices have DU-LDP sessions.

Provider edge router Z advertises the labels for its address 1.1.1.10 to adjacent link state devices M and K. Routers M and K distribute the labels for that address to the rest of the network.

If provider edge router A wants to send a VPN-labeled packet to router Z, it uses label 61 as the outer label. When the packet reaches router N, outer label 61 is swapped for outer label 52 and the packet continues downstream to router M. Router M then swaps out label 52 for either outer label 31 or 42, depending on router M's label selection algorithm. If outer label 31 is selected, the packet reaches router Z directly, which then continues to route the packet to the customer site based on the VPN label.

If a router receives more than one request for an IP address, and the router does not support ECMP, it selects the first label it receives. If the router supports ECMP, it selects the label with the lowest cost path, or selects both labels if the cost paths are identical.

When a router supports ECMP protocol, LSRs can have multiple equal cost paths to an IP address. ECMP LDP retains all labels it receives from multiple next hop peers. The forwarding plane contains multiple next hops for a FEC and as a result, provides load balancing for LDP-based LSPs.

When a router supports ECMP LDP and a device configured as the next hop is no longer valid, for example a session between peers is lost or the peer withdraws its label, a new valid LDP next hop peer is selected and the forwarding plane is updated.

Load balancing across LSPs for LDP over RSVP is also supported. When ECMP is enabled, all equal cost LSP endpoints are installed in the routing table by the IGP for consideration by LDP. LDP selects the LSP with the lowest LSP metric to determine the next hop. If multiple LSPs are available with equal cost, then ECMP is utilized until the ECMP count is exhausted. An LDP tree is created by sending LSP Trace messages along an ECMP path to downstream LSR nodes.

LDP for P2MP

LDP support for P2MP can be enabled on an LDP interface. You can configure an LDP interface for multicast traffic forwarding towards a downstream node. LDP configuration allows an exchange of P2MP FEC via an established session to a peer, and the use of next hops over an interface.

LDP configuration is supported on a tunnel interface under a base routing instance and under protocols such as PIM and IGMP. A P2MP ID is used as an index for LDP-based tunneling instead of an LSP ID.

Note — BFD and source redundancy are only supported on an RSVP tunnel interface.

IS-IS

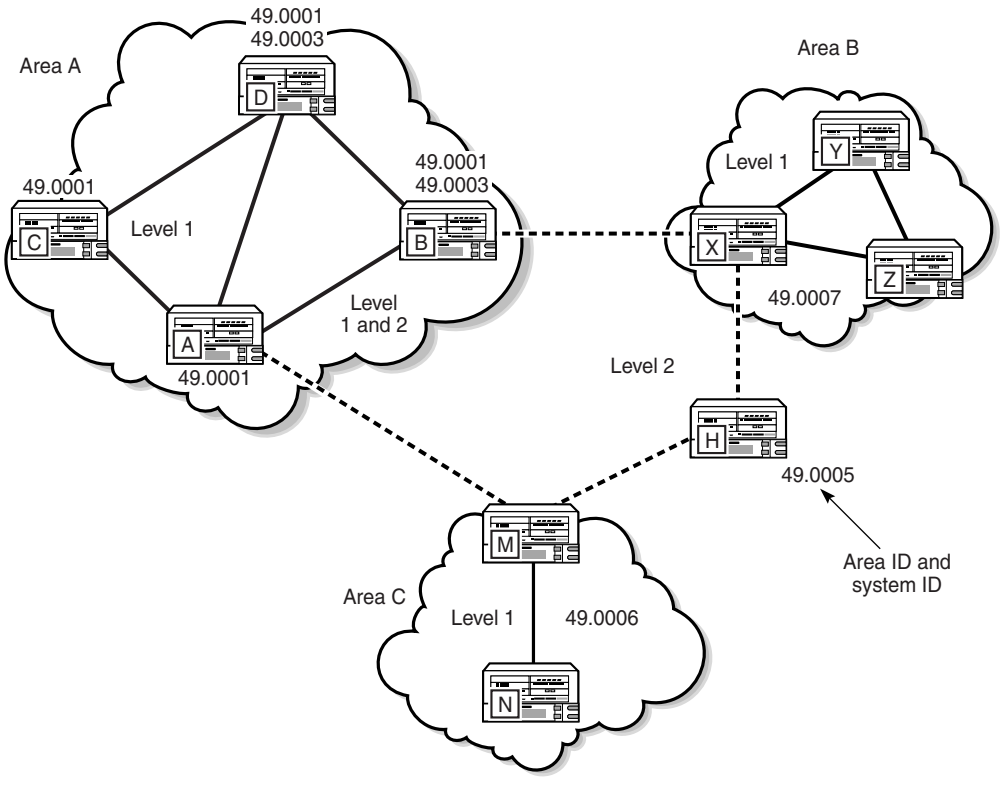
IS-IS is a link-state interior gateway protocol that uses the shortest path first algorithm to determine a route. Routing decisions are made using the link-state information. IS-IS entities include:

- networks, which are autonomous system routing domains
- intermediate systems, which are routers
- end systems, which are network devices that send and receive PDUs

End systems and intermediate system protocols allow devices and nodes to identify each other. The IS-IS protocol sends link state updates periodically through the network, so each device can maintain current network topology information.

Large networks, or autonomous systems, are supported by the IS-IS using a two-level hierarchy. This divides a large area into more manageable, smaller areas. The first level (level 1) of routing is performed within an area. The second level (level 2) of routing is performed between areas, as shown in Figure 28-3.

Figure 28-3 IS-IS routing domains example



Level 2 areas are also called backbones, similar to an OSPF backbone area. All traffic traversing different areas must traverse the backbone.A device can be configured as level 1, level 2, or both level 1 and 2. In this example, routers A, B, M, H, and X form the level 2 IS-IS backbone. The connection between routers A and B carries both level 1 and level 2 link-state PDUs. However, level 1 devices are only aware of their own area's topology, and must forward traffic to a layer 1/2 device to forward the data to another area.

Two devices are in the same level 1 area when they have level 1 adjacency. Level 1 adjacency occurs when the area IDs are common and there is a level 1 connection between the devices. Level 2 adjacency occurs when it has at least one level 1 or 2, or one level 2 interface configured.

The 5620 SAM supports the configuration of IPv6 addresses for IS-IS adjacencies.

Note — If two neighboring devices in the same level 1 area run both level 1 and 2, they establish both a level 1 and level 2 adjacency.

When LDP over RSVP is enabled for IS-IS, LSP can be used by the IGP to calculate its SPF tree. The IGP then provides LDP with all of the ECMP IDP next-hops and tunnel endpoints that the IGP identifies as the lowest cost path to the destination. If an IGP calculation and an LDP over RSVP have the same cost, LDP chooses an LDP over RSVP tunnel over an IGP route and ECMP between the two types is not considered. The type and number of tunnels that are to be considered by LDP depend on the IGP costs, where the lowest cost between the tunnel endpoint and the target is selected.

After the IS-IS is configured, routing occurs as follows:

1 Hello PDUs are sent to IS-IS-enabled interfaces to discover neighbors and establish adjacencies.

2 IS-IS neighbor relationships are formed.

3 Link-state PDUs are created based on local interfaces and prefixes that are learned from adjacent devices.

4 The devices flood LSPs to adjacent neighbors, and build a link-state database.

5 A shortest path tree is calculated by the IS-IS and the routing table is built.

OSPF

OSPF is a hierarchical link-state interior gateway protocol that operates within ASs and is used in IP networks. OSPF packets are routed based on the destination IP address of the IP packets. Each OSPF router collects link-state information to build a network topology based on OSPF areas. This topology is used to apply the Dijkstra algorithm to calculate the shortest path to each destination in the network. See the appropriate device documentation for more information about OSPF.

When LDP over RSVP is enabled for OSPF, LSP can be used by the IGP to calculate its SPF tree. The IGP then provides LDP with all of the ECMP IDP next-hops and tunnel endpoints that the IGP identifies as the lowest cost path to the destination. If an IGP calculation and an LDP over RSVP have the same cost, LDP chooses an LDP over RSVP tunnel over an IGP route and ECMP between the two types is not considered. The type and number of tunnels that are to be considered by LDP depend on the IGP costs, where the lowest cost between the tunnel endpoint and the target is selected.

OSPF areas

The hierarchical design of OSPF allows a collection of networks to be grouped into a logical OSPF area. The topology of the area is hidden from the rest of the AS, which significantly reduces OSPF protocol traffic. Routing in the AS takes place on two levels, depending on whether the source and destination of a packet reside in the same area (intra-area routing) or different areas (inter-area routing). In intra-area routing, the packet is routed solely on information obtained within the area; routing information obtained from outside the area is not used. Routers that belong to more than one area called an ABR. An ABR maintains a separate topological database for each area it is connected to. Every router that belongs to the same area has an identical topological database for that area.

OSPF super-backbone

The OSPF super-backbone provides an additional layer of hierarchy in OSPF. The OSPF super-backbone functions include:

- loop prevention
- handling LSAs received from the CE
- managing VPN IPv4 routes received by BGP

The PE routers that connect OSPF areas to the super-backbone function as ABRs in the OSPF areas to which they are attached. To achieve full compatibility, the PE routers can also serve as ASBRs in non-stub areas.

PE routers insert inter-area routes from other areas into the area in which the CE router is present. The CE routers are not involved at any level and are not aware of the super-backbone or other OSPF areas that exist outside of the super-backbone.

When you configure the super-backbone, all destinations that are learned by PEs with matching domain IDs become inter-area routes.

See the appropriate device documentation for more information about the OSPF super-backbone.

RSVP

RSVP is a network control protocol that hosts use to request specific qualities of service from the network for specific data streams. RSVP is also used to deliver QoS requests to all devices in a data path and to establish and maintain the state information required to provide the requested service quality.

RSVP is not a routing protocol. RSVP operates using unicast and multicast routing protocols. RSVP consults local routing tables to relay RSVP messages. By default, RSVP is enabled on all devices that support it.

RSVP requests typically result in the reservation of resources on each device in the data path. MPLS uses this RSVP mechanism to set up traffic-engineered LSPs. RSVP requests resources for unidirectional flows only. RSVP treats a sender as logically distinct from a receiver, although the same application process may act as both a sender and a receiver.

Diff-Serv Traffic Engineering support

For the 5620 SAM, Release 7.0 or later, Diff-Serv TE extensions are supported within the RSVP context. Diff-Serv TE extensions provide the ability to manage bandwidth in an MPLS network on a per TE-class basis. With Diff-Serv TE, a 7x50 LER can perform this on a per-class basis. Therefore, you can set different limits for admission control of LSPs in each TE class over each link in the network.

You do this by setting a bandwidth constraint, which configures the percentage of the RSVP interface bandwidth that each CT shares. The absolute value of the CT share of the interface bandwidth is derived as the percentage of the bandwidth advertised by IGP in the Maximum Reservable link bandwidth TE parameter, that is, the link bandwidth multiplied by the RSVP interface subscription parameter.

This configuration also exists at the RSVP interface level and the value specifically configured for the interface overrides the globally-configured value. The bandwidth constraint value can be changed on the fly. You are also allowed to specify the bandwidth constraint for a CT which is not used in any of the TE class definitions and which is not used by any LSP originating or transiting this node.

To enable this feature, in summary, you must:

- configure Diff-Serv Classes on the router RSVP Routing Instances
- configure protocol properties to allow Diff-Serv Classes on the required router RSVP Interfaces
- configure traffic engineering and specify the Class Type that the required dynamic LSPs belongs to
- configure the Diff-Serv Class Type that the required LSP Paths belongs to. This overrides the value set at the LSP level.
- configure Diff-Serv to LSP FC mappings on the required service tunnels (SDPs). User-entered mappings of FC to LSP name are validated automatically (to avoid configuration conflicts) by checking with the RSVP module.

L2TP

L2TP is a session-layer protocol that extends the PPP model by allowing L2 and PPP endpoints to reside on different devices that are interconnected by a PSN. L2TP extends the PPP sessions between the CPE and PPP/L2TP termination point on the L2TP network server (LNS), via an intermediate L2TP access concentrator (LAC). The LAC is the initiator of session-generated L2TP tunnels; the LNS is the server that waits for new tunnels. Manually configured and initiated L2TP tunnels can be initiated and stopped from either the LNS or LAC.

After an L2TP tunnel is established, the network traffic between the peers is bidirectional. If a tunnel carrying a session fails, another tunnel from the same tunnel group re-establishes the session. Within each L2TP tunnel, one or more L2TP sessions can exist. Each L2TP session transports PPP packets.

The 5620 SAM supports the configuration and management of the following:

- ISA-LNS groups
- L2TP sites
- L2TP tunnel group profiles
- L2TP tunnel profiles

ISA-LNS groups

The 5620 SAM supports the creation and configuration of ISA-LNS groups on the 7750 SR. ISA-LNS groups provide LNS PPP session termination. An ISA-LNS group is associated with specific L2TP inbound peers and groups. Session traffic is automatically balanced across the available active ISA broadband application MDAs in the group.

The following operations can be performed on an ISA-LNS group member:

- drain MDA—prevents new sessions from being accepted
- stop drain—allows new sessions to be established
- stop MDA sessions—terminates the active sessions

See Procedure 17-19 for information about creating and configuring an ISA-LNS group.

L2TP sites

By default, L2TP is enabled on a base routing instance, and an L2TP site is created. An L2TP icon appears in the routing view of the navigation tree. An L2TP site does not exist by default on the base routing instance of a 7450 ESS in non-mixed mode.

L2TP is not enabled by default on a VPRN site. To enable L2TP on a VPRN site, see Procedure 71-1.

L2TP tunnel group profiles

An L2TP tunnel group profile represents the configuration for a group of L2TP tunnels. L2TP tunnel group profiles must be configured on the LNS NE. If a local user database is used on the LAC for session authentication, an L2TP tunnel group profile must be configured on the LAC. When you create an L2TP tunnel group profile, the profile can be used by its child L2TP tunnel profile to inherit certain parameter values. The inherited parameter values are used as the default values during L2TP tunnel profile configuration.

The following operations can be performed on an L2TP tunnel group profile that has a configured L2TP tunnel profile:

- drain—prevents new sessions from being accepted
- stop drain—allows new sessions to be established
- stop—closes tunnel instances and terminates the active sessions

See Procedure 28-29 for information about managing L2TP tunnel group profiles.

L2TP tunnel profiles

You can create and manage L2TP tunnel profiles from the Tunnel Group Profile properties form.

The following operations can be performed on an L2TP tunnel profile:

- start instance—attempts to create new tunnels
- stop instance—attempts to close the tunnels
- drain—prevents new sessions from being accepted
- stop drain—accepts new sessions

See Procedure 28-29 for information about managing L2TP tunnel profiles.

L2TP tunnel instance endpoints

The endpoints of an operational L2TP tunnel are represented by tunnel instance endpoints. You can view tunnel instance endpoints from the Tunnel Instance Endpoints tab on the L2TP Site (Edit) form, and from the Tunnel Group Profile or Tunnel Profile properties form if the endpoint is created using the profile configuration.

An L2TP tunnel instance endpoint is automatically created when:

- a start operation is performed on an L2TP tunnel profile
- an incoming L2TP session is established using group and tunnel profiles
- RADIUS authentication returns a configuration for the tunnel when an incoming L2TP session is authenticated and PPP session authentication determines that L2TP is used, at which point an L2TP session is established.

The following operations can be performed on an L2TP tunnel instance endpoint:

- drain—prevents new sessions from being accepted
- stop drain—allows new sessions to be established
- stop—closes the tunnel instances and terminates the active sessions

L2TP peers

An L2TP site can have none or multiple L2TP peers. L2TP peer information is available on the Peers tab of the L2TP Site form. Information about L2TP tunnels for a specific L2TP peer is available on the Tunnels tab of the L2TP Peer properties form.

The following operations can be performed on an L2TP peer:

- drain—prevents new sessions from being accepted
- stop drain—accepts new sessions

L2TP tunnels and tunnel endpoints

You can view information about L2TP tunnels and tunnel endpoints from the L2TP Tunnel - Endpoint A - Endpoint B form. See Procedure 28-30 for information about viewing L2TP tunnels and tunnel endpoints.

28.2 Workflow to configure protocols

1 Prior to configuring OSPF or BGP, the router ID must be available. The router ID is a 32-bit number that uniquely identifies the device in the network.

2 Prior to configuring BGP, an AS number must be assigned to the device from the Routing tab of the Routing Instance configuration form.

3 Enable the routing protocols to be supported on the devices. The options are:

- LDP
- IS-IS
- MPLS
- RSVP (enabled by default)
- BGP
- RIP
- L2TP (enabled by default)
- OSPFv2
- OSPFv3
- PIM
- IGMP
- MSDP
- MLD

Note — L2TP is enabled by default on a base routing instance, but not on a VPRN routing instance.

4 Ensure the parameters to implement routing protocols on the Layer 3 interfaces are configured as needed. See chapter 27 for more information.

5 Configure routing policies for routing protocols that use policies.

6 The procedures to follow depend on the type of routing protocol that you want to configure.

a For BGP:

i Determine whether BGP confederations are necessary. If BGP confederations are necessary:

- Configure the Confederation Autonomous System number on the Routing tab of the Routing Instance configuration form.
- Configure BGP confederation members from the BGP Confederations tab of the Routing Instance configuration form.

ii For MP-BGP, do the following on the base routing instance of each NE that is to participate in a VPRN:

- Enable VPN IPv4 and VPN IPv6, as required.
- Enable multicast IPv4 to apply the multicast extension, if required.

iii Create at least one BGP peer group.

iv Create a BGP neighbor with which to peer.

v Create a BGP peer AS that is associated with the neighbor peer.

vi Create connections that exchange IPv4 and IPv6 VPN routes between ASs.

vii Create BGP keychains.

b For RIP:

i Configure global-level RIP parameters.

ii Configure group-level RIP parameters.

iii Configure neighbor-level (also known as interface) RIP parameters.

c For OSPFv2 and OSPFv3:

i Create at least one OSPFv2 or OSPFv3 area.

ii Assign routers to the OSPFv2 or OSPFv3 area.

iii Assign Layer 3 interfaces to the routers in the OSPFv2 or OSPFv3 area.

d For LDP:

i Configure global-level LDP parameters.

ii Create LDP interfaces for LDPs between adjacent devices (directly connected peers).

iii Create LDP targeted peers for LDPs between non-adjacent devices (non directly connected peers).

iv Configure ECMP on LDP routing interfaces.

v Create LDP keychains.

e For IS-IS:

i Configure global-level IS-IS parameters.

ii Configure at least one NET address.

iii Configure at least one IS-IS interface.

iv Configure an operational LSP between routers.

f For RSVP:

i Configure MPLS, LSP, MPLS path, and LSP path parameters, as required.

ii Configure the RSVP properties.

iii Configure the interface properties.

iv Enable LDP, as required.

g For L2TP:

i Create and configure an LNS group and group member for an LNS site. If the site is a LAC, this configuration is not required.

ii Create and configure an IES or VPRN LNS group interface on an LNS site.

iii Create and configure an L2TP tunnel group profile.

iv Create and configure an L2TP tunnel profile.

h For PIM:

i Enable PIM on the router.

ii Configure PIM on the router.

iii Configure an anycast RP for PIM on the router.

iv Configure a PIM interface.

i For IGMP:

i Enable IGMP on the router.

ii Configure IGMP on the router.

iii Configure an IGMP interface.

j For MSDP:

i Enable MSDP on the router.

ii Configure MSDP on the router.

iii Create at least one MSDP peer or group-peer.

k For MLD:

i Enable MLD on the router.

ii Configure MLD on the router.

iii Create an MLD interface.

7 Configure the protocol for the remote device, if applicable.

28.3 Protocol configuration procedures

Perform the appropriate procedures for the routing protocols that you need to configure.

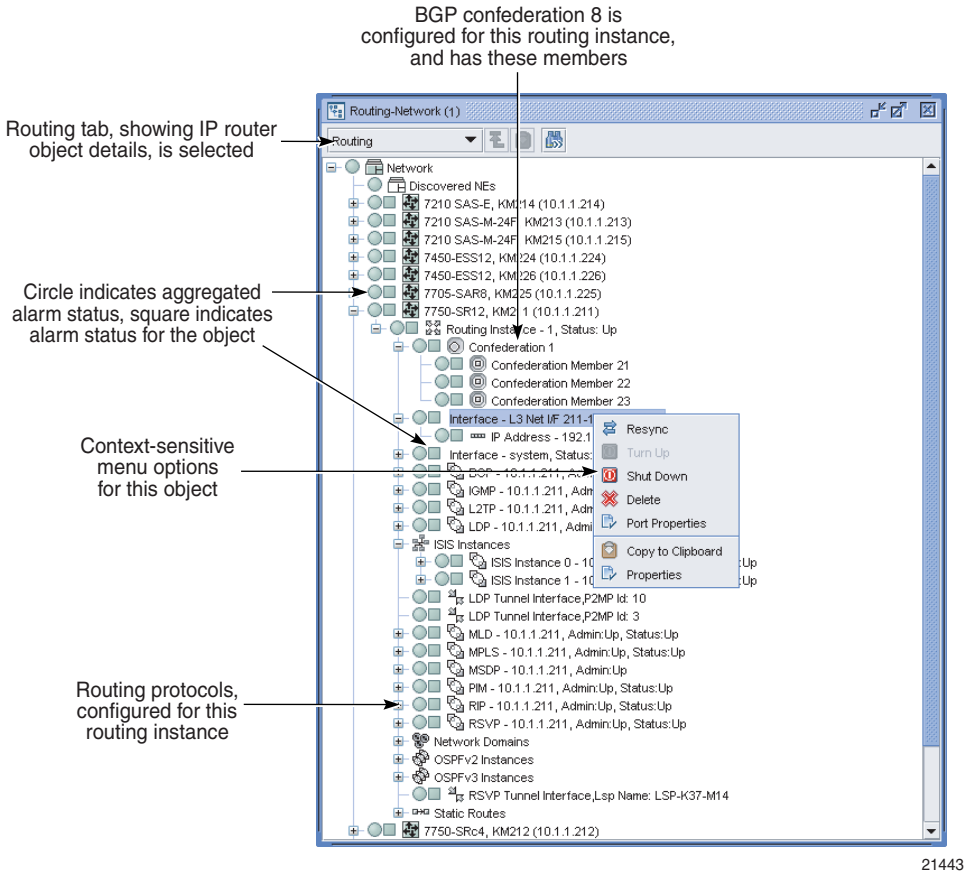
BGP configuration

The BGP command hierarchy consists of three levels:

- global
- peer group
- peer (also known as neighbor)

Figure 28-4 shows the network view open to show Confederations and BGP settings.

Figure 28-4 BGP in the navigation tree network view



BGP parameters are initially applied at the global level. These parameters are inherited by the group and peer levels. Parameters can be modified and overridden on a level-specific basis.

Many of the hierarchical BGP commands can be modified at different levels. BGP group-level parameters take precedence over BGP global-level parameters. BGP peer-level parameters take precedence over group- and global-level parameters.

Procedure 28-1 To enable BGP on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Network→equipment_group→device→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens with the General tab displayed.

4 Enable BGP.

i Click on the Protocols tab button.

ii Choose the BGP Enabled parameter.

Note 1 — You must configure an AS number before enabling BGP. Configure the Autonomous System parameter on the Routing tab of the Routing Instance (Edit) form.

Note 2 — If a confederation is required, configure the Confederation Autonomous System parameter on the Routing tab on the Routing Instance (Edit) form.

5 Click on the OK button. The Routing Instance (Edit) form closes, a BGP entry appears in the list of enabled protocols, and a BGP icon appears in the network view of the navigation tree.

Procedure 28-2 To configure global-level BGP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the BGP icon. The path is Routing→Router→Routing Instance→BGP.

3 Right-click on the BGP icon and choose Properties. The BGP (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Router ID
- Administrative State
- Cluster ID

5 Click on the Behavior tab button.

6 Configure the parameters:

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min. Route Advertisement
- Disable Standard Communities
- Disable Extended Communities
- Disable Fast External Failover
- Advertise Inactive Routes
- Enable Inter AS VPRN
- Enable Rapid Withdrawal
- Enable Peer Tracking
- BFD Enabled
- Connect Retry Time (seconds)
- Keep Alive (seconds)
- Purge Time (minutes)
- Hold Time (seconds)

The Enable Inter AS VPRN parameter is not configurable on a VPRN routing instance.

7 Click on the AS Properties tab button.

8 Configure the parameters:

- Local AS
- Local AS Private
- Remove Private AS
- Remove Private AS Limited
- Min AS Origination (seconds)
- Disable 4Byte ASN

The Local AS parameters are used to configure a virtual AS. A virtual AS is used when a router (RTA) is moved from one AS (AS1) to another AS (AS2). However, the customer router (CR1) is configured to belong to the AS1. To avoid reconfiguring CR1 to belong to AS2, CR1 can continue to belong to AS1, but RTA has its local AS value set to AS1. RTA can advertise AS1 for routes advertised to CR1.

9 Click on the MultiPath tab button.

10 Configure the parameters:

- Multi Path
  Set to 1 to disable. When set from 2 to 16, multipath is enabled and BGP load shares traffic across the number of links specified. If the equal cost routes available are greater than the configured value, then routes with the lowest next hop IP address are chosen.
- IBGP MultiPath
- EIBGP LoadBalance

11 Click on the MED tab button.

12 Configure the parameters:

- MED Compare
- MED Source
- MED Value

These parameters are used to find a way to leave the AS when there are multiple methods of leaving the AS.

13 Click on the VPN tab button.

14 Configure the parameters:

- Family
- Apply Import Route Policies
- Apply Export Route Policies
- AS Path Ignore
- AS Path Ignore Family

If you are configuring global-level BGP for BGP AD in VPLS or for BGP VPLS, then you must enable L2 VPN in the Family block.

The Apply Import Route Policies and Apply Export Route Policies parameters are not configurable on a VPRN routing instance.

The Apply Import Route Policies and Apply Export Route Policies parameters specify whether to apply the existing import and export route policies configured on the Import Policies and Export Policies tabs.

15 Configure the Address Family parameter in the Rapid Update block.

16 If you are configuring BGP for a VPRN routing instance, go to step 21.

17 Click on the IGP Shortcut tab button.

18 Configure the parameters:

- IGP Shortcut
- Disallow IGP

The Disallow IGP parameter is only displayed if you enable one of the IGP Shortcut options.

19 Click on the Graceful Restart tab button.

20 Configure the parameters:

- Graceful Restart
- Stale Routes Time (seconds)

The Stale Routes Time (seconds) parameter is configurable when the Graceful Restart parameter is enabled.

21 Assign a TCP key chain, if required.

Note — You can assign a TCP key chain to a BGP site, group, or peer on a 7750 SR, or on a 7450 ESS in mixed mode.

i Click on the KeyChain tab button.

ii Click on the Select button. The Select BGP Site Keychain - BGP form opens.

iii Select a key chain in the list and click on the OK button. The Select BGP Site Keychain - BGP form closes. The 5620 SAM assigns the key chain to the BGP instance.

22 Perform the following steps to add a peer group, if required.

i Click on the Group tab button.

ii Click on the Add button.The Peer Group (Create) form opens.

iii Perform steps 4 to 22 of Procedure 28-4.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Peer Group (Create) form closes.

23 Perform the following steps to add a peer, if required.

i Click on the Peer tab button.

ii Click on the Add button. The Peer (Create) form opens.

iii Perform steps 4 to 21 of Procedure 28-5.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Peer (Create) form closes.

24 Click on the Import Policies tab button.

25 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policies to determine which routes are accepted from peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

26 Click on the Export Policies tab button.

27 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policies to determine which routes are advertised to peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 27. A router performs no validation to ensure the policies match.

28 Click on the Authentication tab button.

29 Configure the parameters:

- Type
- Key

30 Click on the following tab buttons to view information:

- Statistics
- Faults

31 Click on the OK button. The BGP (Edit) form closes.

Procedure 28-3 To configure a BGP confederation

For BGP confederations, the following rules apply:

- A device can only belong to one confederation.
- Multiple devices can belong to one BGP confederation.

You must configure BGP on the device and configure global-level BGP parameters before you configure BGP confederations, as described in Procedures 28-1 and 28-2.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the Routing Instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Click on the Routing tab button.

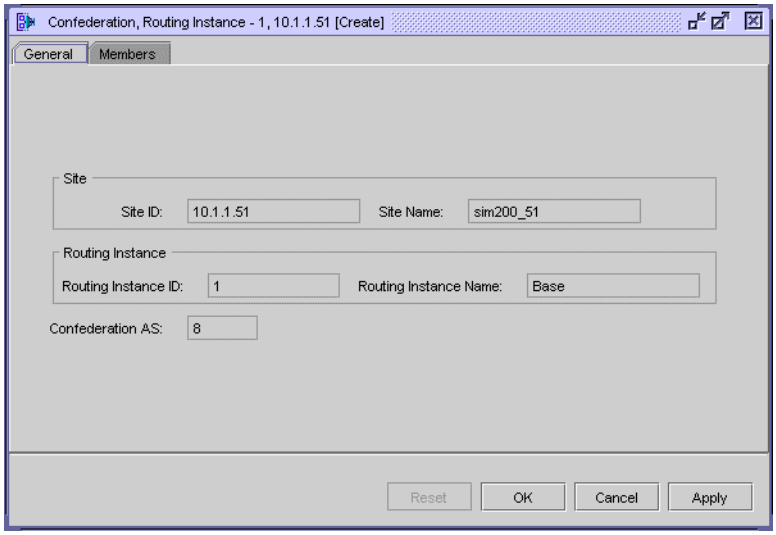
5 Enter the confederation number for the Confederation Autonomous System parameter and click on the Apply button.

6 Click on the BGP Confederations tab button.

7 Click on the Add button to add a BGP confederation, or select a BGP confederation from the list and click on the Properties button to configure an existing BGP confederation. The Confederation (Edit) form opens with the General tab displayed.

You can only have one BGP confederation per device. Figure 28-5 shows the configuration form for a routing instance confederation with the General tab displayed.

Figure 28-5 Routing instance confederation form - General tab

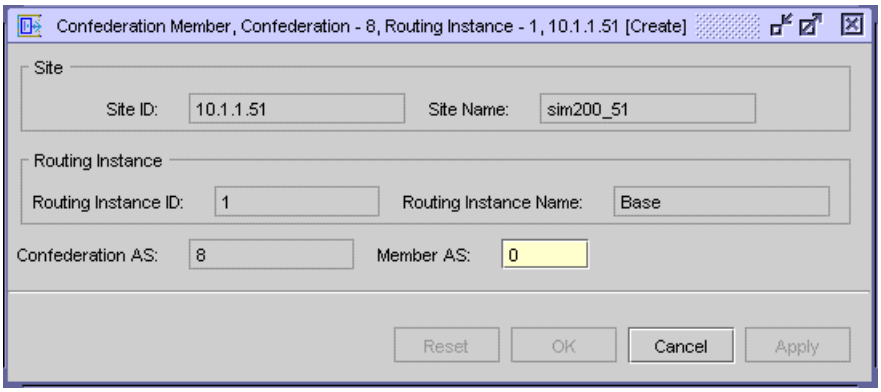


8 To add a new member to the confederation:

i Click on the Members tab button.

ii Click on the Add button. The Confederation Member (Create) form opens, as shown in Figure 28-6.

Figure 28-6 Confederation Member (Create) form



iii Configure the Member AS parameter as the number of ASs for the confederation. The member AS number represents the BGP instance of the device.

iv Click on the OK button. The Confederation Member (Create) form closes, and an entry for the new confederation member AS appears in the Confederation (Edit) form.

9 Click on the OK button. The Confederation (Edit) form closes and the Routing Instance (Edit) reappears. A Confederation icon appears in the Navigation Tree below the Routing Instance icon.

You can verify the confederation membership by opening the Confederation icon to view icons that represent the members of the confederation as specified in step 8.

10 Close the Routing Instance (Edit) form.

Procedure 28-4 To configure peer-group-level BGP

Note 1 — For most parameters in this procedure, you can specify that the parameter value is inherited from the parent BGP configuration using the Inherit Value parameter.

If you disable value inheritance for a parameter, the available options are restricted, based on the parent parameter value and the protocol functionality. For example, if a parameter in the global-level BGP configuration is set to True, the only available option for the same parameter in the peer-group-level BGP configuration is False, unless a value of False violates a protocol rule, in which case the only available option is True.

Note 2 — The parameters that you configure for a BGP peer group take precedence over the parameters that are configured for global-level BGP.

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to the BGP icon by choosing Routing→Router→Routing Instance→BGP.

3 Right-click on the BGP icon and choose Create Group. The Peer Group (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description
- Administrative State
- Cluster ID
- Local Address
- Inherit Value
- Dynamic Peer

5 Click on the Behavior tab button.

6 Configure the parameters:

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min. Route Advertisement
- Disable Standard Communities
- Disable Extended Communities
- Disable Fast External Failover
- Advertise Inactive Routes
- Enable Peer Tracking
- BFD Enabled
- Connect Retry Time (seconds)
- Keep Alive (seconds)
- Peer Type
- Passive
- Next Hop Self
- Minimum TTL Value
- Hold Time (seconds)
- Prefix Limit
- Prefix Limit Log Only
- Prefix Limit Threshold
- Inherit Value

7 Click on the AS Properties tab button.

8 Configure the parameters:

- Peer AS
  The parameter specifies the peer AS for this specific group, and the behavior, either internal or external. Multipath configurations are not supported at the BGP peer level.
- Local AS
- Local AS Private
- Remove Private AS
- Remove Private AS Limited
- Min AS Origination (seconds)
- Disable 4Byte ASN
- Inherit Value

9 Click on the MED tab button.

10 Configure the parameters:

- MED Source
- MED Value
- Inherit Value

These parameters are used to find a way to leave the AS when there are multiple methods of leaving the AS.

11 Click on the VPN tab button.

12 Configure the parameters:

- Family
- Advertise Label
- Apply Import Route Policies
- Apply Export Route Policies
- Inherit Value

Note 1 — The Advertise Label, Apply Import Route Policies, and Apply Export Route Policies parameters are not configurable for a VPRN routing instance.

Note 2 — The Apply Import Route Policies and Apply Export Route Policies parameters specify whether to apply the existing import and export route policies configured on the Import Policies and Export Policies tabs.

13 Click on the Graceful Restart tab button.

14 Configure the parameters:

- Graceful Restart
- Stale Routes Time (seconds)
- Inherit Value

15 Assign a TCP key chain, if required.

Note — You can assign a TCP key chain to a BGP site, group, or peer on a 7750 SR, or on a 7450 ESS in mixed mode.

i Click on the KeyChain tab button.

ii Click on the Select button. The Select BGP Group Keychain - Peer Group form opens.

iii Select a key chain in the list and click on the OK button. The Select BGP Group Keychain - Peer Group form closes and the 5620 SAM assigns the key chain to the BGP peer group.

16 Perform the following steps to add a peer, if required.

i Click on the Peer tab button.

ii Click on the Add button. The Peer (Create) form opens.

iii Perform steps 4 to 21 of Procedure 28-5.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Peer (Create) form closes.

17 Click on the Import Policies tab button.

18 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Inherit Value

Configure the import route policies to determine which routes are accepted from peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

19 Click on the Export Policies tab button.

20 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Inherit Value

Note — Configure the export route policies to determine which routes are advertised to peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 27. A router performs no validation to ensure the policies match.

21 Click on the Authentication tab button.

22 Configure the parameters:

- Type
- Key
- Inherit Value

23 Click on the following tab buttons to view information.

- Statistics
- Faults

24 Click on the OK button. The Peer Group (Create) form closes, and the 5620 SAM displays an icon for the new peer group under the BGP icon in the navigation tree.

Procedure 28-5 To configure peer-level BGP

Note 1 — For most parameters in this procedure, you can specify that the parameter value is inherited from the parent BGP configuration using the Inherit Value parameter.

If you disable value inheritance for a parameter, the available options are restricted, based on the parent parameter value and the protocol functionality. For example, if a parameter in the peer-group-level BGP configuration is set to True, the only available option for the same parameter in the peer-level BGP configuration is False, unless a value of False violates a protocol rule, in which case the only available option is True.

Note 2 — The parameters that you configure for a BGP peer take precedence over the parameters that are configured for group-level BGP.

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to a peer group by choosing Routing→Router→Routing Instance→BGP→Peer Group.

3 Right-click on the peer group icon and choose Create Peer. The Peer (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Peer Address
- Description
- Administrative State
- Cluster ID
- Local Address
- Inherit Value

5 Click on the Behavior tab button.

6 Configure the parameters:

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min. Route Advertisement
- Disable Standard Communities
- Disable Extended Communities
- Disable Fast External Failover
- Advertise Inactive Routes
- Enable Peer Tracking
- BFD Enabled
- Connect Retry Time (seconds)
- Keep Alive (seconds)
- Peer Type
- Passive
- Next Hop Self
- Minimum TTL Value
- Hold Time (seconds)
- Prefix Limit
- Prefix Limit Log Only
- Prefix Limit Threshold
- Inherit Value

7 Click on the AS Properties tab button.

8 Configure the parameters:

- Peer AS
  The parameter specifies the peer AS for the group to which the peer belongs, and the behavior, either internal or external. Multipath configurations are not supported at the BGP peer level.
- Local AS
- Local AS Private
- Remove Private AS
- Remove Private AS Limited
- Min AS Origination (seconds)
- Disable 4Byte ASN
- Inherit Value

9 Click on the MED tab button.

10 Configure the parameters:

- MED Source
- MED Value
- Inherit Value

These parameters are used to find a way to leave the AS when there are multiple methods of leaving the AS.

11 Click on the VPN tab button.

12 Configure the parameters:

- Family
- Advertise Label
- Advertise LDP Prefix
- Apply Import Route Policies
- Apply Export Route Policies
- Inherit Value

The Advertise LDP Prefix is only displayed when the Advertise Label parameter is enabled for IPv4 routes.

The Apply Import Route Policies and Apply Export Route Policies parameters specify whether to apply the existing import and export route policies configured on the Import Policies and Export Policies tabs.

13 Click on the Graceful Restart tab button.

14 Configure the parameters:

- Graceful Restart
- Stale Routes Time (seconds)
- Inherit Value

15 Assign a TCP key chain, if required.

Note — You can assign a TCP key chain to a BGP site, group, or peer on a 7750 SR, or on a 7450 ESS in mixed mode.

i Click on the KeyChain tab button.

ii Click on the Select button. The Select BGP Peer Keychain - Peer form opens.

iii Select a key chain in the list and click on the OK button. The Select BGP Peer Keychain - Peer form closes and the 5620 SAM assigns the key chain to the BGP peer.

16 Click on the Import Policies tab button.

17 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Inherit Value

Configure the import route policies to determine which routes are accepted from peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

18 Click on the Export Policies tab button.

19 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Inherit Value

Configure the export route policies to determine which routes are advertised to peers. These policies should match the policies you configure using the Routing Policy Manager, as described in chapter 27. A router performs no validation to ensure the policies match.

20 Click on the Authentication tab button.

21 Configure the parameters:

- Type
- Key
- Inherit Value

22 Click on the OK button. The Peer (Create) form closes and a Peer icon appears below the Peer Group icon in the Navigation Tree of the network view.

23 Configure the protocol for the far-end device, if applicable. Use CLI for devices that are managed outside the scope of the 5620 SAM.

Procedure 28-6 To enable or disable BGP peering

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to a peer group by choosing Routing→Router→Routing Instance→BGP→Peer Group.

3 Click on the Peer Group icon to display the peers in the peer group.

4 Right-click on a peer and choose one of the following menu items:

   a Turn Up to activate a peer

   b Shut Down to deactivate a peer

5 A dialog box appears. Click on the Yes button. The state information beside the Peer icon changes accordingly.

RIP configuration

The RIP command hierarchy consists of three levels:

- global
- group
- interface (also known as neighbor)

For RIP configuration, you must define at least one group and one interface. The parameters that are configured on the global level are inherited by the group and interface levels. Parameters can be modified and overridden on a level-specific basis.

Many of the hierarchical RIP commands can be modified on different levels. RIP group-level parameters take precedence over BGP global-level parameters. RIP interface-level parameters take precedence over peer-group and global-level parameters.

Procedure 28-7 To configure global-level RIP

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to the RIP icon by choosing Routing→Router→Routing Instance→RIP.

3 Right-click on the RIP icon and choose Properties. The RIP Site (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Administrative State

5 Click on the Behavior tab button.

6 Configure the parameters:

- Check Zero
- Message Size
- Metric In
- Metric Out
- Preference
- Receive
- Send

  The parameter specifies the type of messages received based on the RIP version, and the variation of RIPv2 messages sent, either broadcast or multicast.
- Split Horizon
- Propagate RIP Metric

  This parameter is configurable only when configuring RIP on a VPRN routing instance.
- Flush
- Timeout
- Update

7 Click on the Authentication tab button.

8 Configure the parameters:

- Type
- Key

9 Click on the Import Policies tab button.

10 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Specify routing policies that determine the routes that RIP interfaces import. You can specify up to five routing policies. The routing policies are enforced in order, from one to five.

11 Click on the Export Policies tab button.

12 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Specify routing policies that determine the routes that RIP interfaces export. You can specify up to five routing policies. The routing policies are enforced in order, from one to five.

13 To create a RIP group, click on the Group tab button.

i Click on the Add button. The RIP Group (Create) form opens.

ii Configure the parameters. See Procedure 28-8 for more information.

14 Click on the Interface tab button. To configure interface-level (also known as neighbor) RIP parameters:

i Click on the Add button. The RIP Interface (Create) form opens.

ii Configure the parameters. See Procedure 28-9 for more information.

15 Click on the following tab buttons to view statistic and alarm information.

- Statistics
- Faults

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The RIP Site (Edit) form closes.

Procedure 28-8 To configure group-level RIP

Note 1 — You can choose to inherit values from the global-level RIP configuration by selecting the Inherit Value parameter. If you choose not to inherit a parameter value from the global-level RIP configuration, only the parameter options that are not set in the parent configuration are available. For example, if the Check Zero parameter is set to false in the global-level RIP configuration, you can only set the parameter to true in the group-level RIP configuration.

Note 2 — The parameters that you configure for a RIP group take precedence over the parameters that are configured for the global-level RIP configuration.

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Navigate to the RIP icon. The path is Routing→Router→Routing Instance→RIP.

3 Right-click on the RIP icon and choose Create Group. The RIP Site Group (Create) form opens with the General tab displayed.

4 Configure the Name parameter.

5 Perform steps 4 to 12 of Procedure 28-7.

6 Click on the OK button. The RIP Group (Create) form closes, and the 5620 SAM displays an icon for the new RIP group in the navigation tree below the RIP icon.

Procedure 28-9 To configure interface-level RIP

Note 1 — You can choose to inherit values from the global-level RIP configuration by selecting the Inherit Value parameter. If you choose not to inherit a parameter value from the global-level RIP configuration, only the parameter options that are not set in the parent configuration are available. For example, if the Check Zero parameter is set to false in the global-level RIP configuration, you can only set the parameter to true in the interface-level RIP configuration.

Note 2 — The parameters that you configure for a RIP interface, also known as a RIP neighbor, take precedence over the parameters that are configured for the group- and global-level RIP configuration.

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Navigate to a RIP group. The path is Routing→Router→Routing Instance→RIP→RIP Group.

3 Right-click on the RIP group icon and choose Create Interface. The RIP Interface (Create) form opens with the General tab displayed.

4 Perform steps 4 to 12 of Procedure 28-7.

5 Click on the OK button. The RIP Interface (Create) form closes, and the 5620 SAM displays an icon for the new RIP interface below the RIP group icon in the navigation tree.

OSPF configuration

The 5620 SAM supports the configuration of OSPFv2 and OSPFv3.

Note 1 — OSPFv3 configuration is supported on the 7750 SR, 7710 SR, and the 7450 ESS in mixed mode.

Note 2 — OSPFv2 configuration is supported on Release 2.0 or later of the 7705 SAR.

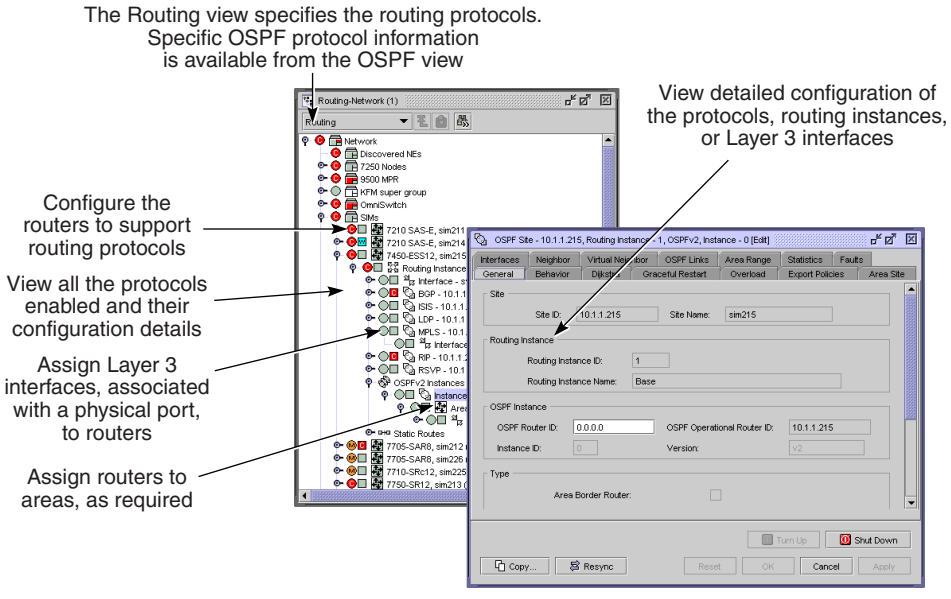
Note 3 — The 7750 SR, 7450 ESS, 7710 SR, OS 9700E, and OS 9800E support multiple instances of OSPFv2 on the base node. VPRN services do not support multiple OSPF instances, except for the 7750 SR (chassis mode C or D), the 7710 SR, Release 6.1 R1 or later, and the 7450 ESS (mixed mode chassis) which support OSPFv2 and OSPFv3 instances.

Configuration planning is essential to organize OSPF areas, interfaces, and virtual links. OSPF provides defaults for basic protocol operability. OSPF configuration requires, as a minimum, that:

- you create a single OSPF backbone area that contains the area border routers.
- for larger networks, you create several areas that contain the other routers.
- for smaller networks, you place all routers in the OSPF backbone area.

Use the 5620 SAM navigation tree to configure the OSPF parameters. Figure 28-7 shows the OSPF view in the navigation tree.

Figure 28-7 OSPF view



19502

The OSPF parameters that are required for OSPF deployment are:

- Router ID — Each device that runs OSPF must be configured with a unique router ID. The router ID is used by the OSPF and BGP routing protocols in the routing table manager. When you configure a new router ID, protocols are not automatically restarted with the new router ID. You must shut down and restart the protocol to initialize the new router ID.
- An area — At least one OSPF area must be created. An interface must be assigned to each OSPF area. The types of OSPF areas include a backbone area, stub area, and NSSA.
- Layer 3 interfaces — A Layer 3 interface is the logical IP connection between a router and one of its attached networks. A physical interface is associated with the Layer 3 interface to provide the cabled connected to another device. A Layer 3 interface has state information from the underlying lower-level protocols and the routing protocol. A network interface has an associated IP address and mask that combine to create an IP prefix, unless the interface is in an unnumbered, point-to-point network.

Procedure 28-10 To enable OSPF on a routing instance

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to the routing instance icon by choosing Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Click on the Protocols tab button.

5 Select the OSPFv2 Enabled parameter to enable OSPFv2, if required.

6 Select the OSPFv3 Enabled parameter to enable OSPFv3, if required.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Routing Instance (Edit) form closes, and an icon for each newly enabled protocol appears under the routing instance in the navigation tree.

Procedure 28-11 To configure OSPF on a routing instance

Note 1 — OSPFv3 configuration is supported on the 7750 SR, 7710 SR, 7450 ESS, in mixed mode.

Note 2 — OSPFv2 configuration is supported on Release 2.0 or later of the 7705 SAR.

Note 3 — The 7750 SR, 7450 ESS, 7710 SR, OS 9700E, and OS 9800E support multiple instances of OSPFv2 on the base node. VPRN services do not support multiple OSPF instances, except for the 7750 SR (chassis mode C or D), the 7710 SR, Release 6.1 R1 or later, and the 7450 ESS (mixed mode chassis) which support OSPFv2 and OSPFv3 instances.

Note 4 — The 7210 SAS-M supports only one OSPF instance.

1 Choose Routing from the navigation tree view selector from the 5620 SAM GUI.

2 Navigate to the OSPF area that you need to add a router by choosing one of the following:

- **a** 7750 SR, 7450 ESS, and 7710 SR, Network→Router→Routing Instance→OSPFv*N* Instances.
- **b** For all other devices, Routing→Router→Routing Instance→OSPFv*N*, where *N* is the OSPF version number; for example, 2 or 3

3 Perform one of the following, when OSPFv2 is required:

- **a** For the 7705 SAR, Release 2.0 or later, right-click on the appropriate OSPFv2 Instances icon and choose Properties. The OSPF Site, Routing instance, OSPFv2 instance (Edit) form appears. Go to step 5.
- **b** For the 7750 SR, 7450 ESS, or 7710 SR, right-click on the appropriate OSPFv2 Instances icon and choose Create OSPFv2 Instance. The OSPF (Create) form opens with the General tab displayed. Go to step 5.

4 For OSPFv3:

- **i** Right-click on the appropriate routing instance and choose Properties. The Routing Instance (Edit) form opens with the General tab displayed.
- **ii** Click on the Protocols tab button and ensure the OSPFv3 Enabled parameter is configured to create the OSPFv3 routing instance. Click on the appropriate OSPFv3 Instances icon.
- **iii** Select the appropriate Instance icon below the OSPFv3 Instances icon, and select Properties. The OSPF Routing Instance OSPFv3 (Edit) form opens.

5 Configure the parameters:

- OSPF Router ID
- Instance ID
- Autonomous System Border Router
- Domain ID
- Administrative State

6 Click on the Behavior tab button.

7 Configure the parameters:

- Traffic Engineering Support
- Interface Base Reference Cost (kbps)
- Overload Stubs
- Unicast Import
- Multicast Import
- Enable LDP Synchronization
- Ignore DN Bit
- Suppress DN Bit
- RFC1583 Compatible
- LDP Over RSVP Include
- Advertise Tunnel Links Enabled
- Exit Overflow Interval
- External LSA Limit
- Internal
- External

The Traffic Engineering Support, RFC1583 Compatible, LDP over RSVP, Multicast Import, and Unicast Import parameters are configurable for OSPFv2 only.

The Unicast Import and Multicast Import parameters are not configurable for OSPF in VPRN.

8 Click on the Dijkstra tab button.

9 Configure the following parameters:

For SPF:

- SPF Max Wait (milliseconds)
- Initial Wait (milliseconds)
- Second Wait (milliseconds)

For LSA:

- LSA Generate Max Wait (milliseconds)
- LSA Arrival Wait (milliseconds)
- Initial Wait (milliseconds)
- Second Wait (milliseconds)

10 Depending on the OSPF version, the Graceful Restart tab is configurable. Configure graceful restart, if required.

i Click on the Graceful Restart tab button.

ii Configure the parameters:

- Graceful Restart
- Helper Mode

The Helper Mode parameter is configurable when the Graceful Restart parameter is set to true.

11 Depending on the OSPF version, the Overload tab is configurable. Configure overload, if required.

i Click on the Overload tab button.

ii Configure the parameters:

- Overload Enabled
- Boot Overload Enabled
- Overload Interval (seconds)
- Boot Overload Interval (seconds)

The Overload Interval (seconds) parameter is configurable when the Overload Enabled parameter is selected.

The Boot Overload Interval (seconds) parameter is configurable when the Boot Overload Enabled parameter is enabled.

12 If the OSPF version is OSPFv2, the OSPF Super-Backbone tab is configurable. Configure the OSPF super-backbone, if required.

i Click on the OSPF Super-Backbone tab button.

ii Configure the parameters:

Note — These parameters apply only to VPRN instances of OSPF.

- VPN Domain Type
- VPN Domain ID (hex)
- VPN Tag
- Super-Backbone

13 Click on the Export Policies tab button to specify the export routing policies that determine the routes that are advertised to peers.

14 Configure the parameters:

- Policy 1
- Policy 2
- Policy 4
- Policy 3
- Policy 5

15 Click on the Area Site tab button to add a routing instance for the router to an OSPF area, if required. Otherwise, go to step 17.

i Click on the Add button. The AreaSite (Create) form opens.

ii Configure the parameters:

- Area ID
- Type
- Blackhole Range

iii Click on the OK button. The AreaSite (Create) form closes, and the OSPF (Edit) form reappears.

16 Perform steps 4 to 13 of Procedure 28-14.

17 Click on the following tab buttons to view OSPF configuration information:

- Interfaces
- Neighbor
- Virtual Neighbor
- Virtual Link (configurable only in a backbone area)
- Area Range
- Statistics
- Faults

The Statistics and Faults tabs are unavailable for OSPF in VPRN.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button to close the OSPF Site (Edit) form.

Procedure 28-12 To create an OSPF area

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Right-click on the Network icon and choose Create Area. The Area (Create) form opens.

3 Configure the parameters:

- Version
- ID
- Name
- Type
- Description

4 Click on the Apply button. Additional configurable tab buttons appear.

5 Click on the Area Site tab button.

6 Click on the Add button to add a routing instance to the area. The Area Site (Create) form opens.

7 Click on the Select button to choose a routing instance. The Select OSPF Instance - Area Site form opens.

8 Select an OSPF instance and click on the OK button. The Select OSPF Instance form closes, and the OSPF instance appears in the Routing Instance panel.

9 Configure the parameters:

- Type
- Blackhole Range

Configure the area as a blackhole range to avoid routing loops.

The Type parameter is not configurable for a backbone-area routing instance.

10 Click on the Apply button. Additional configurable tab buttons appear, and an icon for the new area appears in the navigation tree.

11 Depending on the Type parameter value, the Stub/NSSA tab is configurable. Configure stub or NSSA functionality, if required.

i Click on the Stub/NSSA tab button.

ii Configure the parameters:

- Default Cost
- Redistribute External Routes
- Originate Default Route

The Default Cost parameter is configurable only when the Type parameter value from step 9 is Stub (No Type 5 External) or Totally Stub (No Summaries).

The Redistribute External Routes and Originate Default Route parameters are configurable only when the Type parameter value from step 9 is NSSA (No Type 5 External) or NSSA (No Summaries).

12 If the area is a backbone area that requires links to remote areas that do not advertise OSPF topology, configure a virtual link.

i Click on the Virtual Link tab button.

ii Perform steps 4 to 8 of Procedure 28-16.

iii Click on the OK button. The new virtual link entry appears in the list.

13 Create an area range, if required.

i Click on the Area Range tab button.

ii Click on the Add button. The Area Range (Create) form opens.

iii Perform steps 4 and 5 of Procedure 28-15.

iv Click on the OK button. The new area range entry appears in the list.

14 Click on the OK button. The Area Site (Create) form closes, and a dialog box appears.

15 Click on the Yes button to confirm the action.

Procedure 28-13 To add a router to an OSPF area

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Navigate to the OSPF area to which you want to add a router. The path is Routing→Area.

3 Right-click on the area icon and choose Add OSPF Instance. The Area Site (Create) form opens.

4 Configure the parameters:

- Type
- Blackhole Range

Configure the area as a blackhole range to avoid routing loops.

5 Click on the Select button below the Routing Instance panel to choose a routing instance. The Select OSPF Instance - Area Site form opens.

6 Select a routing instance and click on the OK button. The routing instance appears in the Routing Instance panel.

7 Depending on the Type parameter value from step 4, the Stub/NSSA tab is configurable. Configure stub or NSSA functionality, if required.

i Click on the Stub/NSSA tab button.

ii Configure the parameters:

- Default Cost
- Redistribute External Routes
- Originate Default Route

The Default Cost parameter is configurable only when the Type parameter value from step 4 is Stub (No Type 5 External) or Totally Stub (No Summaries).

The Redistribute External Routes and Originate Default Route parameters are configurable only when the Type parameter value from step 4 is NSSA (No Type 5 External) or NSSA (No Summaries).

8 Click on the OK button. The Area Site (Create) form closes, and an icon for the router appears in the navigation tree under the Area icon.

Procedure 28-14 To add a Layer 3 interface to an OSPF router

Perform this procedure to allow an OSPF-enabled router to participate in area discovery and share routing information with other area members.

Note — This action assigns an existing Layer 3 interface to the router in the OSPF area rather than creating a new Layer 3 interface.

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Click on an Area icon to display the area routers.

3 Right-click on a router instance icon and choose Create Interface. The OSPF Interface (Create) configuration form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Administrative State
- Configured MTU (bytes)

5 Click on the Select button beside the Interface Name parameter to choose an interface. The Select Interface - OSPF Interface form opens.

6 Configure the filter criteria. A list of available Layer 3 interfaces appears.

7 Choose a Layer 3 interface and click on the OK button. The Select Interface - OSPF Interface form closes, and the interface entry appears in the Interface panel.

8 Click on the Protocol Properties tab button.

9 Configure the parameters:

- Type
- Priority
- Metric
- Advertise Subnet
- BFD Enabled
- Passive
- Hello Interval (seconds)
- Router Dead Interval (seconds)
- Retransmission Interval (seconds)
- Transit Delay (seconds)

The Advertise Subnet parameter is configurable for OSPFv2 only.

The TE Metric checkbox is a read-only field that indicates whether the TE Metric parameter is being configured in the interface for LSP path computation by CSPF.

10 Perform one of the following steps to configure authentication for the interface, if required. Otherwise, go to step 13.

a Click on the Authentication tab button, and go to step 11.

b For OSPFv3 interfaces, click on the IPsec Static SA tab button, and go to step 12.

11 Configure the Authentication Type parameter.

a Choose MD5-based Authentication.

i Click on the Add button to create an MD5 authentication key. The Md5Key (Create) form opens.

ii Configure the parameters:

- Key Index
- Key
- Re-enter Key

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Md5Key (Create) form closes, and the new authentication key appears in the list.

b Choose Simple Password.

i Click on the Change Password button to enter a password. The Password (Create) form opens.

ii Configure the parameters:

- Password
- Re-enter Password

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Password (Create) form closes.

12 Configure the parameters:

- IPsec Security Association Name
- IPsec In Static Security Association
- IPsec Out Static Security Association

13 Click on the OK button to close the OSPF Interface (Create) form. The 5620 SAM displays an icon for the new OSPF interface in the navigation tree below the area router.

Procedure 28-15 To create an OSPF area range

An area range summarizes a range of IP addresses in an LSA to minimize the number of flooded advertisements in the LSA.

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Click on an Area icon in the navigation tree to display the area routers.

3 Right-click on a router instance icon and choose Create Area Range. The Area Range (Create) form opens.

4 Configure the parameters:

- Network
- Prefix Length
- Link State DB Type
- Effect

5 Click on the OK button. The Area Range (Create) form closes, and an icon for the new area range appears in the navigation tree below the OSPF area.

Procedure 28-16 To create a virtual link

Perform this procedure to create a link between the backbone OSPF area and a remote OSPF area that does not advertise the OSPF topology.

1 In the 5620 SAM navigation tree, choose OSPF from the view selector.

2 Click on the backbone area icon in the navigation tree to display the area routers. The backbone area ID is 0.0.0.0.

3 Right-click on a backbone-area router instance icon and choose Create Virtual Link. The Virtual Link (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Virtual Neighbor Router (Site) ID
- Transit Area
- Administrative State

5 Click on the Protocol Properties tab button.

6 Configure the parameters:

- Hello Interval (seconds)
- Router Dead Interval (seconds)
- Retransmission Interval (seconds)
- Transit Delay (seconds)

7 Perform one of the following steps to configure authentication for the virtual link, if required. Otherwise, go to step 10.

a Click on the Authentication tab button, and go to step 8.

b For OSPFv3 interfaces, click on the IPsec Static SA tab button, and go to step 9.

8 Configure the Authentication Type parameter.

a Choose MD5-based Authentication.

i Click on the Add button to create an MD5 authentication key. The Md5Key (Create) form opens.

ii Configure the parameters:

- Key Index
- Key
- Re-enter Key

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Md5Key (Create) form closes, and the new authentication key appears in the list.

v Go to step 10.

b Choose Simple Password.

i Click on the Change Password button to enter a password. The Password (Create) form opens.

ii Configure the parameters:

- Password
- Re-enter Password

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Password (Create) form closes.

v Go to step 10.

9 Configure the parameters:

- IPsec Security Association Name
- IPsec In Static Security Association
- IPsec Out Static Security Association

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The VirtualLink (Create) form closes, and the 5620 SAM displays an icon for the new virtual link in the navigation tree.

LDP configuration

An LDP instance in the 5620 SAM network navigation tree has the following child objects:

- Interfaces–The interfaces object contains the configured LDP interfaces for directly connected peers. The 7210 SAS-M does not support configuration of LDP interfaces.
- Targeted Peers–The targeted peers object contains the indirectly connected peers.

T-LDP is supported on the 7750 SR, 7710 SR, 7450 ESS, 7210 SAS-M, 7210 SAS-X, 7250 SAS-ES, 7705 SAR, and 7250 SAS-ESA. DU-LDP is supported only on the 7750 SR.

Procedure 28-17 To enable LDP on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable LDP.

  i Click on the Protocols tab button.

  ii Select the LDP Enabled parameter.

5 Click on the OK button to save the changes. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes, and an LDP icon appears under the routing instance in the navigation tree.

Procedure 28-18 To configure global-level LDP

1 Enable LDP on the router, as described in Procedure 28-17.

2 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

3 Navigate to the LDP instance icon. The path is Routing→Router→Routing Instance→LDP.

4 Right-click on the LDP icon and choose Properties. The LDP - Routing Instance (Edit) form appears, with the General tab displayed.

5 Configure the Administrative State parameter.

6 Click on the Common tab button.

7 Configure the parameters:

- Targeted Sessions Allowed
- Prefer Tunnel-in-Tunnel
- Tunnel Down Damp Time (seconds)
- Enable Implicit Null Label
- Enforce Graceful Restart
- Multi Path Make Before Break Time (seconds)
- Neighbor Liveness Time (seconds)
- Maximum Recovery Time (seconds)
- Forward State Holding Time (seconds)
- Reconnect Time (seconds)
- Shortcut Local TTL Propagate
- Shortcut Transit TTL Propagate

Configure the Targeted Sessions Allowed parameter to true to configure the router for T-LDP. Targeted sessions are LDP sessions that distribute labels between indirectly connected peers.

The Neighbor Liveness Time and Maximum Recovery Time parameters are configurable when the Enforce Graceful Restart parameter is enabled.

8 Click on the Interface Properties tab button.

9 Configure the parameters:

- Address Type
  - Choose system to have the system IP address set up LDP sessions.
  - Choose interface to have the IP interface address set up LDP sessions only if there are not multiple interfaces between the two neighbors.
- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)

By default, these parameter values are inherited by all LDP interfaces.

10 Click on the Targeted Peer Properties tab button.

i Configure the parameters:

- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)

  By default, these parameter values are inherited by all LDP targeted peers.

ii Click on the Route Import Policy tab.

iii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

iv Click on the Route Export Policy tab.

v Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

11 Click on the Ecmp OAM tab button. The General tab displayed. See Procedure 28-22 for more information about configuring ECMP for LDP interfaces.

12 Click on the Interfaces tab button. A list of interfaces you can view or configure opens. See Procedure 28-19 for more information about configuring LDP interfaces.

13 Click on the Peers tab button. A list of peers you can view or configure opens. See Procedure 28-22 for more information about creating peers.

14 Click on the Targeted Peers tab button. A list of targeted peers you can view or configure opens. See Procedure 28-20 for more information about creating and configuring targeted peers.

15 Click on the Import Policies tab button.

16 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

17 Click on the Export Policies tab button.

18 Configure the parameters on the General tab page:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

19 Click on the Tunnel Table tab button.

20 Configure the parameters on the Tunnel Table tab page:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

The tunnel table policies are used to allow LDP-capable PE devices to offer services to PE routers in areas or domains where BGP-labeled routes are not supported. They are used to determine which routes are advertised to LDP. Only policy entries supporting the LDP protocol are considered; all other policies are ignored. See also Procedure 28-5 for information on enabling the advertisement of LDP prefixes to BGP peers.

21 Click on the Sessions tab button. A list of LDP sessions opens, showing information of the active LDP communication sessions between interfaces and targeted peers between the routers running LDP.

22 Click on the Static Prefix FECs tab button.

i Click on the Add button. The StaticFec (Create) form opens.

ii Configure the parameters:

- IP Prefix
- Prefix Length
- Advertised Label
- Next Hop Type
- Next Hop Address
- Swap Label

  Next Hop Address and Swap Label parameters appear when IP Address is selected for the Next Hop Address value.

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The static FEC form closes and the static FEC entry appears in the list.

23 Click on the Aggregate Prefix Match tab button.

24 Configure the parameters:

- Aggregate Prefix Match Enabled
- Administrative State

When the Aggregate Prefix Match Enabled parameter is enabled, the LDP installs a prefix binding in the LDP FIB by performing a longest match against an aggregate prefix in the routing table, as opposed to requiring an exact match of the prefix. The LDP prefix binding continues to be advertised on a per individual /32 prefix basis.

The Administrative State parameter can only be configured if the Aggregate Prefix Match Enabled parameter is enabled.

25 Configure the following parameters in the Prefix Exclude Policies block:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

The Prefix Exclude Policies can only be configured if the Aggregate Prefix Match Enabled parameter is enabled.

When routing policy statements are specified in the Prefix Exclude Policies block, any prefixes defined in the routing policies are excluded from the aggregate prefix matching procedure. In this case, when LDP receives a FEC-label binding for this prefix, it performs an exact match of a specific FEC element prefix, as opposed to a longest match of one or more LDP FEC element prefixes.

26 Click on the Accounting tab button.

27 Click on the Add button. The AccountingFecPrefix (Create) form opens.

28 Configure the Fec Prefix parameter.

29 Configure the parameters in the Egress Accounting Statistics panel:

- Click on the Select button. The Select Accounting Policy - AccountingFecPrefix form opens. Choose the required accounting policy and click on the OK button. Only accounting policies with the CombinedLdpLspEgressStats stats type are available for selection.
- Collect Accounting Stats
- Administrative State

See the 5620 SAM Statistics Management Guide for more information about the collection of statistics.

30 Click on the following tab buttons to view LDP statistic and alarm information.

- Statistics
- Faults

31 Click on the OK button. The LDP (Edit) form closes.

Procedure 28-19 To configure an LDP interface

Note — You can choose to inherit values from the global-level LDP configuration by selecting the Inherit Value parameter.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to an LDP instance. The path is Routing→Router→Routing Instance→LDP.

3 Right-click on the LDP instance and choose Create Interface. The LDP Interface configuration form opens with the General tab displayed.

4 Click on the Select button to choose a Layer 3 interface. The Select Interface - LDP Interface form opens.

5 Configure the filter criteria. A list of the available interfaces appears.

6 Select an interface in the list and click on the OK button.

7 Configure the parameters:

- Description
- Administrative State

8 Click on the Protocol Properties tab button.

9 Configure the parameters:

- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)
- Address Type
  - Choose system to have the system IP address set up LDP sessions.
  - Choose interface to have the IP interface address set up LDP sessions only if there are not multiple interfaces between the two neighbors.

  By default, these parameter values are inherited by all LDP interfaces.
- Local LSR ID
- Multicast Forwarding

10 Click on the OK button. The LPD Interface (Create) form closes, and an icon for the new LDP interface appears in the navigation tree list of interfaces below the LDP icon.

11 Click on the OK button. An icon for the new LDP interface appears in the navigation tree below the LDP icon.

12 Configure the protocol for the far-end device, if applicable. Use CLI for devices that are managed outside the scope of the 5620 SAM.

Procedure 28-20 To configure an LDP targeted peer

Note 1 — You can choose to inherit values from the global-level LDP configuration by selecting the Inherit Value parameter.

Note 2 — The parameters that you configure for a targeted peer take precedence over the parameters that are configured for the global-level LDP configuration.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to an LDP interface. The path is Routing→Router→Routing Instance→LDP.

3 Right-click on the LDP icon and choose Create Targeted Peer. The TargetedPeer (Create) configuration form opens with the General tab displayed.

4 Configure the parameters:

- Peer Address
- Description
- Administrative State

5 Click on the Protocol Properties tab button.

i Configure the parameters:

- Keep-Alive Factor
- Keep-Alive Timeout (seconds)
- Hello Factor
- Hello Timeout (seconds)

  By default, these parameter values are inherited from the global-level LDP instance.
- Tunneling Enabled
- BFD Enabled

ii Configure the Local LSR ID Name parameter by clicking on its associated Select button. The Select Local LSR ID window opens.

iii Select the desired Local LSR ID from the list and then click OK. The Select Local LSR ID window closes and the name of the Local LSR ID you chose appears in the Name field.

6 Click on the LSPs tab button. View, add, or configure associated LSPs, as required.

Refer to Chapter 29 for information on creating and configuring LSPs.

7 Click on the OK button. The TargetedPeer (Create) form closes, and an icon for the new LDP targeted peer appears in the navigation tree list of targeted peers below the LDP icon.

8 Configure the protocol for the far-end device, if applicable. Use CLI for devices that are managed outside the scope of the 5620 SAM.

Procedure 28-21 To configure an LDP peer

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to an LDP interface. The path is Routing→Router→Routing Instance→LDP.

3 Right-click on the LDP icon and choose Properties. The LDP (Edit) form opens.

4 Click on the Peers tab button.

5 Click on the Add button. The Peer (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Peer Address
- Minimum TTL Value
- DoD Label Distribution

7 Assign a TCP key chain to the LDP peer, if required.

i Click on the KeyChain tab button.

ii Click on the Select button. The Select LDP Peer Keychain - Peer form opens with a list of local key chains displayed.

iii Select a key chain in the list and click on the OK button. The Select LDP Peer Keychain - Peer form closes. The 5620 SAM assigns the key chain to the LDP peer.

8 Select the Authentication tab button.

9 Configure the parameters:

- Type
- Key

10 Click on the Import Policies tab button.

The FEC prefix Import Policy provides a mean of controlling which FEC prefixes received from other LDP and T-LDP peers should be re-distributed to this LDP peer. If no policy name is specified, the NE will import all FEC prefixes it learns from other LDP and T-LDP peers to this LDP peer.

11 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

12 Click on the Export Policies tab button.

The FEC prefix Export Policy provides a mean of controlling which FEC prefixes from this peer should be re-distributed to all other LDP and T-LDP peers. If no policy name is specified, the NE will export all FEC prefixes it learns from this LDP peer to all other LDP and T-LDP peers.

13 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The new peer appears in the list.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The LDP (Edit) form closes.

Procedure 28-22 To configure ECMP for LDP routing

Note — 5620 SAM supports LDP ECMP when LDP routing is configured on the 7450 ESS, 7450 ESS, and 7710 SR.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to an LDP interface. The path is Routing→Router→Routing Instance→LDP.

3 Right-click on the LDP icon and choose Properties. The LDP Routing Instance (Edit) form opens.

4 Click on the ECMP OAM tab button.

5 Perform one of the following steps:

a If the Tree Trace parameter is not configured, go to step 6.

b If the Tree Trace parameter is configured, go to step 7.

6 Select Configured from the Tree Trace drop-down menu. The LDP Routing Instance (Edit) form re-opens with all parameters displayed.

7 Configure the tree discovery configuration parameters:

- Tree Trace
- Administrative State
- Discovery Interval (Minutes)
- Discovery Timeout (Seconds)
- Retry Count
- Maximum Paths
- Forwarding Class
- Profile
- Maximum TTL
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5
- Probe Interval (Minutes)
- Probe Timeout (Minutes)
- Retry Count

8 Click on the Discovered FECs tab. A list of discovered FECs appears.

9 Select a FEC from the list and click on the Properties button. An Autodiscovered FEC (Edit) form opens with the General tab displayed.

10 Perform one of the following:

a Click on the Create LDP Tree Trace button to configure and execute an LSP trace test; see chapter 35 for information about configuring this test.

b Click on the Create LSP Ping button to configure and execute a LSP ping test; see chapter 35 for information about configuring this test.

c Click on the Create LSP Trace button to configure and execute a LDP tree trace; see chapter 35 for information about configuring this test.

11 Click on the Discovered ECMP tab. A list of ECMP paths associated with the FEC appears.

12 Select an ECMP path from the list.

13 Click on the Properties button. An Autodiscovered Path (Edit) form opens.

14 Click on the Create LSP Trace button. To configure and execute an LSP trace test; see chapter 35.

15 Click on the Create LSP Ping button. To configure and execute an LSP ping test; see chapter 35.

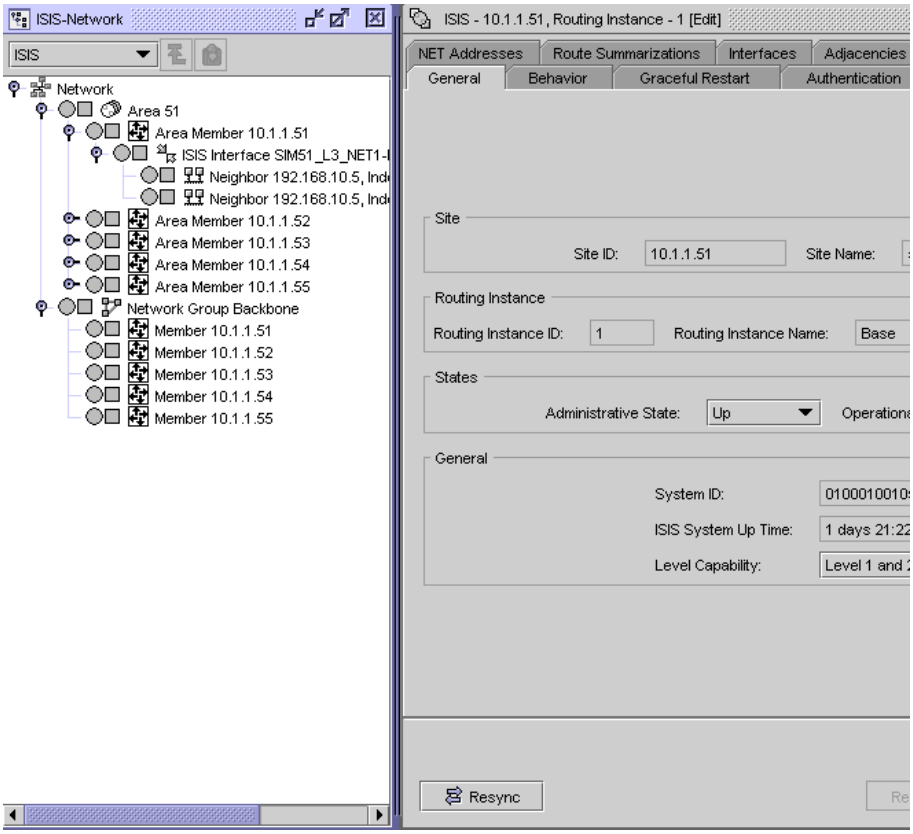
16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Autodiscovered FEC (Edit) form closes.

IS-IS configuration

Configuration planning is essential to organize devices in level 1, level 2 and level 1 and 2 areas. IS-IS provides defaults for basic protocol operability. Use the 5620 SAM to configure the IS-IS parameters. Figure 28-8 shows the IS-IS view in the navigation tree

Figure 28-8 IS-IS view



The IS-IS information that is displayed includes:

- backbone area and backbone-area devices
- a list of areas and the participating routers in each area
- a list of devices and associated interfaces that shows the IP address and the configured level (1, 2, or 1 and 2) of each interface
- the IS-IS adjacencies for each interface

Procedure 28-23 To enable IS-IS on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable the IS-IS protocol.

i Click on the Protocols tab.

ii Select the IS-IS Enabled parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. IS-IS is listed in the configuration form of configured protocols.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The Routing Instance (Edit) form closes, and an ISIS icon appears in the navigation tree below the routing instance.

Procedure 28-24 To configure IS-IS on a routing instance

Router-wide IS-IS parameter values can differ from the interface IS-IS parameter values that are configured in Procedure 28-26. Interface capabilities are compared to the outer-wide capabilities to determine the type of level 1, level 2, and level 1 and 2 adjacencies that are set up between routers to exchange IS-IS routing information.

1 Enable the IS-IS protocol on a router, as described in Procedure 28-23.

2 Navigate to an ISIS icon. The path is Routing→Router→Routing Instance→ISIS.

3 Right-click on the ISIS icon and choose Properties. The IS-IS Interface (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Administrative State
- Level Capability

A level 1 adjacency can be established when there is at least one area address shared by this router and a neighboring router. A level 2 adjacency is established when another router is configured as a level 2 or a level 1 and 2 router with interfaces configured as level 2 or level 1 and 2. A level 1 and 2 adjacency is created when the neighboring router is also configured as a level 1 and 2 router and the routers have at least one area address in common.

5 Click on the Behavior tab button.

6 Configure the parameters:

- Reference Bandwidth
- Traffic Engineering
- Unicast Import
- Multicast Import
- Hello Authentication
- CSNP Authentication
- PSNP Authentication
- Multi-Topology
- IPv6 Unicast Multi-Topology
- Enable LDP Synchronization
- LDP Over RSVP Include
- Isis Default Route Tag
- Advertise Only Passive Interfaces
- RSVP Shortcut Enabled
- Advertise Tunnel Links Enabled
- Overload On Boot
- Overload On Boot Timeout (seconds)
- Overload
- Overload Timeout (seconds)
- LSP Lifetime (seconds)
- LSP Max Wait (seconds)
- LSP Initial Wait (seconds)
- LSP Second Wait (seconds)
- SPF Max Wait (seconds)
- SPF Initial Wait (milliseconds)
- SPF Second Wait (milliseconds)

7 Click on the Graceful Restart tab button.

8 Configure the parameters:

- Graceful Restart
- Helper Mode

9 Depending on the device type and configuration, the IP Versions tab is configurable. Click on the IP Versions tab button to specify the allowed IP versions for the IS-IS instance.

10 Configure the parameters:

- Enable IPv6
- IPv6 Routing TLV type
- Enable IPv4
- Strict Adjacency Check

11 Click on the Authentication tab button.

12 Configure the parameters:

- Enable Authentication
- Type
- Key

13 Click on the Level 1 tab button. The General tab is displayed.

14 Configure the parameters:

- External
- Internal
- Wide Metrics Only
- Hello Authentication
- CSNP Authentication
- PSNP Authentication

15 Click on the Authentication tab button to configure level 1 authentication.

16 Configure the parameters:

- Type
- Key

Configure the authentication parameters to specify the MD5 key or password to verify PDUs from neighboring routers on the interface.

17 Click on the Level 2 tab button.

18 Repeat steps 14 to 16.

19 Click on the Export Policies tab button.

20 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

You can specify up to five routing policies, in order of preference, to determine the routes that are exported from the routing table to IS-IS. When multiple policies are specified, the policies are evaluated in order, from one to five.

21 Click on the NET addresses tab button. Perform step 4 of Procedure 28-25.

22 Click on the OK button. A dialog box appears.

23 Click on the OK button. The new NET address appears on the NET Addresses tab.

24 Click on the Route Summarizations tab button. IS-IS route summaries allow users to create aggregate IPv4 or IPv6 addresses that include multiple groups of IPv4 or IPv6 addresses for a specific IS-IS summary level. This can help reduce the size of the link state database and the routing table.

25 Click on the Add button. The Route Summarization (Create) form opens.

26 Configure the parameters:

- Network
- Mask
- Summary Level
- Summary Route Tag

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The new route summary appears on the form.

29 Click on the Interfaces tab button to add an IS-IS interface, if required.

i Click on the Add button.

ii Perform steps 4 to 17 of Procedure 28-26.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new interface appears on the form.

30 Click on the following tab buttons to view information.

- Adjacencies
  - An adjacency represents a connection between two IS-IS interfaces. The information listed for an adjacency includes the state of the adjacent interface, the interface ID, and the neighbor ID.
- SPF Logs
- Statistics
- Faults

31 Click on the OK button. A dialog box appears.

32 Click on the Yes button. The IS-IS (Edit) form closes.

Procedure 28-25 To configure an IS-IS NET address

1 Enable the IS-IS protocol on a device, as described in Procedure 28-23.

2 Navigate to an ISIS icon. The path is Routing→Router→Routing Instance→ISIS.

3 Right-click on the ISIS icon and choose Add NET Address. The Area ID (Create) form opens.

4 Configure the NET address for IS-IS using the Area ID parameter. The NET address is exchanged in hello and LSP PDUs. Level 1 interfaces must have at least one area ID in common. Level 2 interfaces can have different area IDs. If all of the interfaces have different area IDs, they are considered level 2 interfaces only.

NET addresses are built from some non-configurable elements, including the device system ID, the network SAP, and the network entity title.

5 Click on the OK button. The Area ID (Create) form closes, and an icon for the new area appears in the navigation tree below the ISIS icon.

Procedure 28-26 To configure an IS-IS interface

Interface IS-IS parameters can differ from the global policies set in Procedure 28-24. Interface-level parameters specify the interface routing levels. Interface level capabilities are compared to the router-wide capabilities to determine the type of level 1, level 2, and level 1 and 2 adjacencies that can be created between devices to exchange IS-IS routing information.

1 Enable the IS-IS protocol on a router, as described in Procedure 28-23.

2 Navigate to an ISIS icon. The path is Routing→Router→Routing Instance→ISIS.

3 Right-click on the ISIS icon and choose Create Interface. The IS-IS Interface (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Description
- Administrative State
- Level Capability
- Type
- BFD Enabled

5 Click on the Select button to choose a Layer 3 interface. The Select Interface - IS-IS Interface form opens.

6 Configure the filter criteria. A list of the available interfaces appears.

7 Select an interface in the list and click on the OK button.

8 Click on the Behavior tab button.

9 Configure the parameters:

- CSNP Interval (seconds)
- LSP Pacing Interval (seconds)
- Retransmit Interval (seconds)
- Mesh Group Status

  To create a mesh group, set the Mesh Group Status parameter to Enabled and specify the same mesh group number for all interfaces. The mesh group parameters specify the assigned mesh group for the interface. Mesh groups limit the amount of flooding when a new or changed LSP is advertised in an area.
- Mesh Group
- Passive
- Route Tag

  The TE Metric checkbox is a read-only field that indicates whether the TE Metric parameter is being configured in the interface for LSP path computation by CSPF.

10 Click on the Authentication tab button.

11 Configure the parameters:

- Type
- Key

You can enable authentication for any IS-IS PDUs sent by the interface. Configure the authentication parameters to specify the MD5 key or password to verify PDUs that are sent by neighboring routers on the interface.

12 Click on the Level 1 tab button.

13 Configure the parameters on the General tab:

- Hello Interval (seconds)
- Hello Multiplier
- Metric
- Passive
- Priority

14 Click on the Authentication tab button.

15 Configure the parameters:

- Type
- Key

16 Click on the Level 2 tab button.

17 Repeat steps 13 to 15.

18 Click on the following tab buttons to view information.

- Adjacencies
  - An adjacency represents a connection between two IS-IS interfaces. The information listed for an adjacency includes the state of the adjacent interface, the interface ID, and the neighbor ID.
- Statistics

19 Click on the OK button. The IS-IS Interface (Create) form closes, and the new interface appears in the navigation tree below the ISIS icon.

RSVP configuration

The RSVP hello protocol detects the loss of a neighbor node or the reset of a neighbor RSVP state information. In standard RSVP, neighbor monitoring occurs as part of the RSVP soft-state model. The reservation state is maintained as cached information that is first installed and then periodically refreshed by the ingress and egress LSRs.

If the state is not refreshed within a specified time interval, the LSR discards the state because it assumes that either the neighbor node has been lost or its RSVP state information has been reset.

Procedure 28-27 To configure RSVP on a routing instance

1 Navigate to an RSVP icon. The path is Routing→Router→Routing Instance→RSVP.

2 Right-click on the RSVP icon and choose Properties. The RSVP form opens with the General tab displayed.

3 Configure the parameters:

- Administrative State
- Keep Multiplier
- Refresh Time
- Message Pacing
- Enable Graceful Shutdown
- Enable Implicit Null Label
- Max Burst
- Period (milliseconds)
- Rapid Retransmit Time (hundred-milliseconds)
- Rapid Retry Limit

4 If you are going to configure Diff-Serv TE, then MPLS must be shutdown first. Otherwise, go to step 15.

5 Configure the parameters:

Note 1 — Enabling a Diff Serv Model only takes effect if you have already enabled traffic engineering at one or both of the following routing protocol levels:

- IS-IS, as described in Procedure 28-24
- OSPF, as described in Procedure 28-11

A dialog box appears if IS-IS and/or OSPF TE is not enabled, but you can save your configuration if IS-IS and/or OSPF TE is not enabled.

Note 2 — The Class Type BW Percent parameters are configured globally and the parameters are applied to all RSVP interfaces in the system. After the parameters are configured, the parameters can only be changed after you shut down the MPLS protocol. The total bandwidth specified for the eight classes should not exceed 100%.

- Diff Serv Model
- TE Threshold Update Enabled
- Class Type 0 BW Percent
- Class Type 1 BW Percent
- Class Type 2 BW Percent
- Class Type 3 BW Percent
- Class Type 4 BW Percent
- Class Type 5 BW Percent
- Class Type 6 BW Percent
- Class Type 7 BW Percent
- Update On CAC Failure Enabled
- Update Timer (seconds)

6 Click on the TE Classes tab.

7 Select one of the TE classes in the table and click on the Properties button. The TE Class (Create) form opens.

Note — The TE Class Definition is used to map all TE Classes (up to a maximum of 8) to Class Type and LSP setup priority. There is no default TE Class after Diff-Serv is enabled. You must explicitly define each TE Class. If Diff-Serv is disabled, the default CT (CT0) and eight pre-emption priorities are used internally.

8 Configure the parameters:

- Priority
- TE Class Type

9 Click on the ForwardingClassMaps tab.

10 Click on the Add button. The Forwarding Class Map (Create) form opens.

11 Configure the parameters:

- FC Name
- TE Class Type

12 Repeat steps 7 to 11 for the remaining TE classes, as required.

13 Click on the TE Thresholds tab.

14 Configure the parameters:

- Up Threshold 1 (%)
- Up Threshold 2 (%)
- Up Threshold 3(%)
- Up Threshold 4 (%)
- Up Threshold 5 (%)
- Up Threshold 6 (%)
- Up Threshold 7 (%)
- Up Threshold 8 (%)
- Up Threshold 9(%)
- Up Threshold 10 (%)
- Up Threshold 11 (%)
- Up Threshold 12 (%)
- Up Threshold 13 (%)
- Up Threshold 14 (%)
- Up Threshold 15 (%)
- Up Threshold 16 (%)
- Down Threshold 1 (%)
- Down Threshold 2 (%)
- Down Threshold 3 (%)
- Down Threshold 4 (%)
- Down Threshold 5 (%)
- Down Threshold 6 (%)
- Down Threshold 7 (%)
- Down Threshold 8 (%)
- Down Threshold 9 (%)
- Down Threshold 10 (%)
- Down Threshold 11 (%)
- Down Threshold 12 (%)
- Down Threshold 13 (%)
- Down Threshold 14 (%)
- Down Threshold 15 (%)
- Down Threshold 16 (%)

You can also click the Reset TE Up/Down Thresholds to Default buttons to set either the Up or Down Thresholds to their default values, respectively.

15 Click on the following tab buttons to view information.

- Interfaces
- Sessions
- Neighbors
- Statistics
- Faults

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The RSVP form closes.

Procedure 28-28 To configure an RSVP interface

1 Navigate to an RSVP interface icon. The path is Routing→Router→Routing Instance→RSVP→Interfaces→Interface.

2 Right-click on the RSVP interface and choose Properties. The RSVP Interface (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Description
- Administrative State

4 Click on the Protocol Properties tab button.

5 Configure the parameters:

- Enable Refresh Reduction
- Enable Reliable Delivery
- Enable Graceful Shutdown
- Enable Implicit Null Label
- Hello Interval (milliseconds)
- Subscription Ratio
- BFD Enabled
- Inherit SAM Class Type BW
- Class Type 0 BW Percent
- Class Type 1 BW Percent
- Class Type 2 BW Percent
- Class Type 3 BW Percent
- Class Type 4 BW Percent
- Class Type 5 BW Percent
- Class Type 6 BW Percent
- Class Type 7 BW Percent

The Class Type BW Percent parameters can only be configured if the Inherit SAM Class Type BW parameter is disabled. If you enter values at the RSVP interface level, they override the global values configured in Procedure 28-27 for the node RSVP routing instance.

6 Click on the Authentication tab button.

7 Configure the Key parameter.

8 Click on the TE Thresholds tab.

9 Configure the parameters:

- Inherit TE Up Thresholds
- Up Threshold 1 (%)
- Up Threshold 2 (%)
- Up Threshold 3(%)
- Up Threshold 4 (%)
- Up Threshold 5 (%)
- Up Threshold 6 (%)
- Up Threshold 7 (%)
- Up Threshold 8 (%)
- Up Threshold 9(%)
- Up Threshold 10 (%)
- Up Threshold 11 (%)
- Up Threshold 12 (%)
- Up Threshold 13 (%)
- Up Threshold 14 (%)
- Up Threshold 15 (%)
- Up Threshold 16 (%)
- Inherit TE DownThresholds
- Down Threshold 1 (%)
- Down Threshold 2 (%)
- Down Threshold 3 (%)
- Down Threshold 4 (%)
- Down Threshold 5 (%)
- Down Threshold 6 (%)
- Down Threshold 7 (%)
- Down Threshold 8 (%)
- Down Threshold 9 (%)
- Down Threshold 10 (%)
- Down Threshold 11 (%)
- Down Threshold 12 (%)
- Down Threshold 13 (%)
- Down Threshold 14 (%)
- Down Threshold 15 (%)
- Down Threshold 16 (%)

You can only configure the Up Threshold (%) and Down Threshold (%) parameters if the Inherit TE Up Thresholds and Inherit TE DownThresholds parameters are disabled, respectively.

10 Click on the following tab buttons to view information.

- Neighbors
- Statistics
- Faults

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The RSVP Interface (Edit) form closes.

L2TP configuration

The 5620 SAM supports the configuration and management of L2TP sites, tunnel group profiles, and tunnel profiles.

Note 1 — To enable L2TP, the NE must be in chassis mode B or higher.

Note 2 — The 7750 SR, Release 7.0 does not support L2TP in chassis mode B.

Note 3 — The 5620 SAM supports L2TP configuration and management on a routing instance of the 7750 SR, Release 7.0 for LAC functionality only, the 7750 SR, Release 8.0, and on the 7450 ESS in mixed mode, Release 8.0 for LAC functionality only.

Note 4 — L2TP can also be enabled on a VPRN site. See chapter 71 for more information.

Procedure 28-29 To configure L2TP on a routing instance

A typical L2TP configuration is applied to two NEs; one NE performs the LAC role and the other NE performs the LNS role. An NE can perform both LAC and LNS roles. At least one ISA-LNS group must be configured for the LNS NE. See section 15.9 for information about ISA-LNS groups. See Procedure 17-19 for information about creating and configuring an ISA-LNS group member.

Note 1 — Only the 7750 SR-7, and 7750 SR-12, Release 8.0 or later, can function as an LNS.

Note 2 — L2TP functionality is supported only by Ethernet MDAs. An IOM 2 or IOM 3 is required to configure an L2TP access interface, and an IOM 3 is required for an L2TP network interface. An IOM3-XP is required for configuration of a broadband ISA MDA.

Table 28-1 describes a sample workflow to configure L2TP.

Table 28-1 Sample 5620 SAM L2TP configuration

Task	Description
1. Enable L2TP if you are configuring L2TP on a VPRN routing instance.	Enable L2TP on a VPRN routing instance; see Procedure 71-1. If you are configuring L2TP on a VPRN routing instance, basic VPRN routing must be operational. For more information about VPRN, see chapter 71.
2. Create and configure an LNS group and LNS group members for an LNS site.	Create and configure an LNS group and group members for an LNS site; see Procedure 17-19
3. Configure the required ESM profiles for LNS L2TP termination.	Configure the required ESM profiles for LNS L2TP termination; for VPRN, see Procedure 71-11; for IES, see Procedure 70-8
4. Create and configure an L2TP tunnel group profile and L2TP tunnel profile.	Create and configure an L2TP tunnel group profile and L2TP tunnel profile; see Procedure 28-29
5. Configure L2TP on a local user database PPPoE host.	Configure L2TP on each local user database PPPoE host to be forwarded to the LNS (applicable for the LAC and the LNS, where RADIUS is not used); see Procedure 64-34.

1 Navigate to an L2TP icon. The path is Routing→Router→Routing Instance→L2TP.

2 Right-click on the L2TP icon and choose Properties. The L2TP Site (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Administrative State
- Session Limit
- Receive Window Size
- Peer Address Change Policy
- Excluded AVPs
- Calling Number Format

4 Click on the Tunnel Group Profiles tab button.

i Click on the Create button. The L2TP Tunnel Group Profile (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Group Name
- Description
- Administrative State
- Local IP Address
- Local Name
- LNS Group ID
- Password
- Challenge
- AVP Hiding
- Session Limit
- Session Assign Method
- Max Retries Established
- Max Retries Not Established
- Receive Window Size
- Hello Interval (seconds)
- Idle Timeout (seconds)
- Destruct Timeout (seconds)

Note 1 — You must configure the LNS Group ID parameter for the tunnel group profile or tunnel profile of the site acting as the LNS.

Note 2 — On the LAC NE, each L2TP tunnel must have the local IP address set to the system interface IP address. This restriction applies only to the 7750 SR, Release 7.0.

Note 3 — To generate operational L2TP tunnels, a start operation must be performed on the L2TP tunnel on the LAC NE. You can also perform a start operation from a tunnel profile on the LNS.

5 Click on the PPP tab button.

Note — You only configure PPP for LNS L2TP tunnel group profiles and L2TP tunnel profiles.

6 Configure the Authentication Protocol parameter.

7 Click on the Select button in the Authentication Policy panel. The Select Authentication Policy (PPPGroupProfile) form opens.

8 Select an authentication policy from the list and click on the OK button. The Select Authentication Policy form closes and the L2TP Tunnel Group Profile (Create) form displays the new PPP authentication policy.

9 If you did not select an authentication policy in step 8, click on the Select button in the User Database panel. The Select User Database (PPPGroupProfile) form opens.

10 Select a user database from the list and click on the OK button. The Select User Database form closes and the L2TP Tunnel Group Profile (Create) form displays the user database.

11 Click on the Select button in the Default Service ID panel. The Select Default Service ID (PPPGroupProfile) form opens.

12 Select a default service ID from the list and click on the OK button. The Select Default Service ID form closes and the L2TP Tunnel Group Profile (Create) form displays the default service ID.

13 Click on the Select button in the Default Group Interface panel. The Select Default Group Interface (PPPGroupProfile) form opens.

14 Select a default group interface from the list and click on the OK button. The Select Default Group Interface form closes and the L2TP Tunnel Group Profile (Create) form displays the default group interface.

15 Configure the parameters:

- Proxy LCP
- Proxy Authentication
- MTU (bytes)
- Keep-Alive Interval (seconds)
- Keep Alive Multiplier

16 Click on the Tunnel Profiles tab button.

i Click on the Create button. The L2TP Tunnel Profile (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Tunnel Name
- Description
- Administrative State
- Local IP Address
- Local Name
- Peer IP Address
- Remote Name
- LNS Group ID
- Password
- Auto Established
- Preference
- Challenge
- AVP Hiding
- Session Limit
- Max Retries Established
- Max Retries Not Established
- Receive Window Size
- Hello Interval (seconds)
- Idle Timeout (seconds)
- Destruct Timeout (seconds)

Note — When you configure parameters with the same name in a tunnel group profile and a tunnel profile, a non-default value in the tunnel group profile overrides the value specified for the L2TP site. Also, a non-default value in a tunnel profile overrides the value defined in the associated tunnel group profile and L2TP site.

17 Click on the PPP tab button.

Note — You only configure PPP for LNS L2TP tunnel group profiles and L2TP tunnel profiles.

18 Repeat steps 6 to 15 to configure PPP for an LNS L2TP tunnel profile.

19 Click on the OK button. A dialog box appears.

20 Click on the Yes button. The L2TP Tunnel Profile (Create) form closes.

21 Click on the following tab buttons to view information.

- Tunnel Instance Endpoints
- Peers
- Statistics
- Faults

Procedure 28-30 To view L2TP tunnels and tunnel endpoints

1 Choose Manage→ISA Functions→ISA-L2TP from the 5620 SAM main menu. The Manage ISA-L2TP form opens.

2 Choose L2TP tunnel (L2TP) from the object drop-down list.

3 Click on the Search button. A list of L2TP tunnels is displayed.

4 Select an entry in the list and click on the Properties button. The L2TP Tunnel - Endpoint A - Endpoint B form opens with the General tab displayed.

5 View the information for Tunnel Endpoint A and Tunnel Endpoint B.

6 Click on the L2TP Tunnel Endpoints tab button. The two L2TP tunnel endpoints are displayed.

7 Select an entry in the list and click on the Properties button. The L2TP Tunnel Endpoint (View) form opens.

8 View the information. You can also click on the Properties button to view additional information for the following:

- Site ID
- Tunnel Instance Endpoint
- Tunnel Profile
- Tunnel Group Profile
- Peer

9 Close the L2TP Tunnel Endpoint (View) form.

10 Close the L2TP Tunnel - Endpoint A - Endpoint B form.

PIM configuration

PIM is a component of multicast routing that defines the one-to-many or many-to-many transmission of information. You can use the following variations for PIM configurations:

- sparse mode
- dense mode

- source-specific multicast
- bidirectional

Sparse mode is the most common PIM configuration. Sparse mode is used for data transmission to nodes in multiple Internet domains that contain a small ratio of nodes that subscribe to the multicast traffic. Dense mode is used when a large ratio of the potential nodes subscribe to the multicast traffic. In source-specific multicast, paths originate at a single, defined source. Bidirectional PIM is not source-specific.

Anycast RP

Anycast RP for PIM-SM enables fast convergence when a PIM RP router fails. The receivers and sources rendezvous at the closest RP after the router failure. Anycast RP allows an arbitrary number of RPs for each group in a single, shared-tree PIM-SM domain. Triple play configurations that distribute multicast traffic using PIM-SM realize the benefits of fast RP convergence, which helps to avoid the loss of multicast data streams or IPTV delivery to the end user.

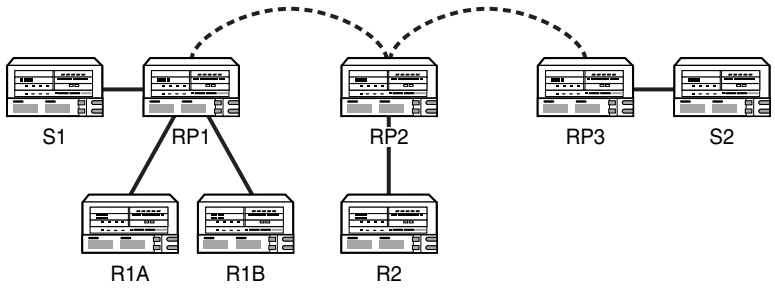
Anycast RP for PIM-SM environments is supported in the base routing PIM-SM instance of the service router. The 7750 SR, 7710 SR, and the 7450 ESS in mixed mode support Anycast RP in VPRN instances that are configured with PIM.

Anycast RP for PIM requires the completion of the following configuration information:

- An IP address specified as the RP address. This address is statically configured, or distributed using a dynamic protocol, to all PIM routers in the domain.
- A set of routers in the domain designated as RPs for the RP address. These routers form an anycast RP.
- Each of these routers is configured with a loopback interface that uses the RP address. The RP address, or a prefix that includes the RP address, is injected into the unicast routing system inside the domain.
- Each router in the anycast RP also needs a separate IP address, to be used for communication between the RPs.
- Each router in the anycast RP is configured with the addresses of all other routers in the anycast RP. The addresses must be consistently configured in all RPs in the set.

Figure 28-9 shows a sample implementation of anycast RP for PIM-SM.

Figure 28-9 Sample implementation of anycast RP for PIM-SM



R1A, R1B, and R2 are receivers for an AnyCast RP group
S1 and S2 send traffic to the AnyCast RP group
RP1, RP2, and RP3 use the same Anycast RP IP address

18605

Table 28-2 summarizes the sequence of events for the Anycast RP implementation shown in Figure 28-9.

Table 28-2 Sequence of events for Anycast RP fast convergence

Sequence	Event description
1	S1 sends a multicast packet.
2	The router connected to S1 forms a PIM registration message to send to the Anycast RP address. The unicast routing system delivers the PIM registration message to the nearest RP, in this case RP1.
3	RP1 receives the PIM registration message, decapsulates the message, and sends the packet down the shared tree to the R1A and R1B receivers.
4	RP1 is configured with the IP address for RP2 and RP3. Since the registration message did not come from one of the RPs in the anycast RP set, RP1 assumes that the packet came from a designated router.
5	RP1 sends a copy of the registration message from the S1 designated router to RP2 and RP3. RP1 uses its own IP address as the source address for the PIM registration message.
6	RP1 can join the source tree by sending a join message to S1. However, RP1 must create a source-specific state.
7	RP2 receives the registration message from RP1, decapsulates the message, and send the packet down the share tree to the R2 receiver.
8	RP2 sends a registration-stop message back to RP1. RP2 can wait to send the registration-stop message if it decides to join the source tree. RP2 should wait until it receives data from the source tree before it sends the registration-stop message. If RP2 does wait for the data, the registration-stop message is sent to RP1 when it receives the next registration message. If RP2 does not wait for the data, the registration-stop message is immediately sent to RP1.
9	RP2 can join the source tree by sending a join message to S1. However, RP2 must create a source-specific state.
10	RP3 receives the registration message from RP1 and decapsulates the message. No receivers joined for the group, so RP3 discards the packet.
11	RP3 sends a registration-stop message back to RP1.

(1 of 2)

Sequence	Event description
12	RP3 creates a source-specific state, so when a receiver joins after S1 starts sending traffic, RP3 can quickly join the source tree for S1.
13	RP1 processes the registration-stop message from RP2 and RP3. RP1 can cache the receipt of registration-stop messages from the RPs in the anycast RP set. (The cache of messages is completed on a per-RP or per-source-specific basis.) The cache of messages increases the reliability of the delivery of registration messages to each RP. Subsequent registration messages received by RP1 are sent only to the RPs in the anycast RP set that have not previously sent registration-stop messages from the source-specific entry.
14	RP1 sends a registration-stop message to the DR under the following conditions: • after receiving a registration message from the DR • if all RPs in the anycast RP set have returned registration-stop messages for a specific source-specific route

(2 of 2)

SPT switchover thresholds

SPT switchover thresholds allow you to configure the switchover threshold, in Kbps, for the group prefixes. The threshold value determines when the router switches from the shared tree to the source-specific tree. The switchover is attempted only if the traffic rate on the shared tree for the group exceeds the configured threshold.

MSDP

MSDP is a protocol that enables multiple PIM-SM domains to communicate with each other using their own RPs. MSDP also enables multiple RPs in a single PIM-SM domain to establish MSDP mesh-groups and to synchronize information between anycast RPs about the active sources being served by each anycast RP peer. The 7750 SR, 7710 SR, and the 7450 ESS in mixed mode support MSDP.

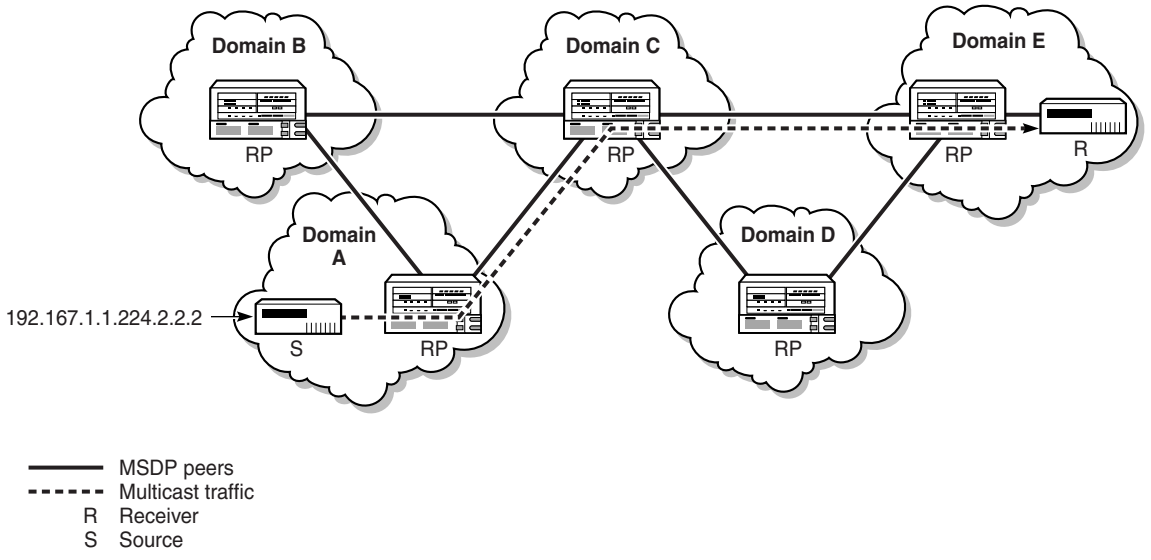
Each PIM-SM domain has its own RPs and MSDP enables these RPs to inform each other about active sources. When an active source is detected, the RPs send PIM-SM explicit join messages to the active source. When RPs in remote domains know about active sources, they can pass on this information to their local receivers and multicast data can be forwarded between the domains.

The RP learns about a new multicast source within its own domain through the PIM register mechanism and encapsulates the first data packet in a source active message. After an RPF check, the MSDP source active message is flooded by each peer to its MSDP peers until it reaches every MSDP router in the interconnected networks. If the receiving MSDP peer is an RP, and the RP has a (*,G) entry for the group in the source active message, the message is accepted. The RP creates an (S,G) state for the source and join to the shortest path tree for the state of the source.

The encapsulated data is forwarded down the RP's shared tree. When the packet is received by a receiver's last hop router, the last-hop may also join the shortest path tree to the source.

Figure 28-10 shows a sample of how data flows from a source in Domain A to a receiver in Domain E in an MSDP implementation for PIM-SM.

Figure 28-10 Sample implementation of MSDP for PIM-SM



L3 Multicast Load Balancing for ECMP

Before Release 6.0 of 5620 SAM, multicast loads were distributed on a per multicast group address basis, over all the available ECMP paths. In order to obtain a more balanced load distribution, this approach has been altered so that balancing is based on the total available multicast bandwidth over all the ECMP paths.

ECMP rebalancing is managed on the base PIM Routing Instance and VPRN PIM Routing Instance configuration forms.

The 5620 SAM implementation of ECMP rebalancing has the following key characteristics:

- Multicast load balancing over ECMP links is enabled, by default.
- The rebalancing timer is set to 30 minutes, by default.
- Distribution of the multicast groups over the available links is processed based on the bandwidth configured for the specified group address. If the bandwidth is not configured for the multicast stream, then the configured default value is used.
- If a link failure occurs, the load on the failed channel is distributed to the remaining channels. The bandwidth required to accommodate the load from the failed link is evenly distributed over the remaining links.
- If an additional link becomes available for a specific multicast channel, it is then treated in an equivalent manner to the other links of the interface.
- A manual (operator-initiated) rebalance command is typically used to re-evaluate the current balance, with regard to bandwidth utilization. If necessary, multicast streams can subsequently be moved to different links to achieve a balance.
- In an automatic timed rebalance, the system rebalances multicast streams over the available links, based on the configured bandwidth and interval. If no links have been added or removed, or it is determined that no multicast streams will benefit from a rebalance, then it is not be implemented.

- When multicast load rebalancing is not enabled, any ECMP changes are not optimized. However, whenever a link is added, an attempt is made to balance the number of multicast streams on all the available ECMP links. This may however, not result in balanced bandwidth utilization of all the ECMP links.
- Only a single rebalance command can be executed at any specific time. If a rebalance is in progress and a manual rebalance command is entered, it is rejected and a message is displayed informing the user that a rebalance is already in progress.

Procedure 28-31 To enable PIM on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable PIM:

i Click on the Multicast tab button.

ii Select the PIM Enabled parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes, and a PIM icon appears in the navigation tree below the routing instance.

Procedure 28-32 To configure PIM on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to a PIM icon. The path is Routing→Router→Routing Instance→PIM.

3 Right-click on the PIM icon and choose Properties. The PIM (Edit) form opens with the General tab displayed.

4 Configure the Administrative State parameter in the States panel.

5 In the PIM General Configurations panel, configure the following parameters:

- Apply To
- Non DR Attract Traffic

6 In the ECMP Balancing panel, configure the following parameters:

- ECMP Balancing Enabled
- Hold Time (minutes)

7 In the Lag Usage panel, configure the Lag Usage Optimization parameter.

8 Click on the RP Behavior tab button.

9 If you are configuring for IPv4 then click on the IPv4 sub-tab and go to step 10. Otherwise click on the IPv6 sub-tab and go to step 15.

10 Configure the Ipv4 Administrative State parameter in the States panel.

11 Configure the Ipv4 RPF Lookup Sequence parameter in the PIM General Configurations panel.

12 Configure the following parameters in the Candidate Bootstrap Router panel:

- CBSR Address
- CBSR Priority
- CBSR Hash Mask Length
- CBSR Admin State

13 Configure the following parameters in the Candidate Rendezvous Point panel:

- Administrative State
- C-RP Address
- C-RP Priority
- C-RP HoldTime (seconds)

14 Go to step 20.

15 Configure the Ipv6 Administrative State parameter in the States panel.

16 Configure the Ipv6 RPF Lookup Sequence parameter in the PIM General Configurations panel.

17 Configure the following parameters in the Candidate Bootstrap Router panel:

- CBSR Address
- CBSR Priority
- CBSR Hash Mask Length
- CBSR Admin State

18 Configure the following parameters in the Candidate Rendezvous Point panel:

- Administrative State
- C-RP Address
- C-RP Priority
- C-RP Hold Time (seconds)

19 Configure the following parameters in the Embedded-RP panel:

- Enable Embedded RP
- Embedded-RP Administrative State

20 Click on the Candidate-RP Groups tab.

21 Click on the Add button to add a new entry, if required. The C-RP Group Prefix (Create) form opens.

22 Configure the parameters:

- Group IP Address
- Mask

23 Click on the OK button. A dialog box appears.

24 Click on the OK button. The C-RP Group Prefix (Create) form closes and the new Candidate-RP entry appears in the table.

25 Click on the Embedded-RP Groups tab button.

Note — The Embedded-RP Groups tab is only selectable if you enabled the Enable Embedded RP parameter in step 19.

26 Click on the Add button to add a new entry, if required. The E-RP Group Range (Create) form opens.

27 Configure the parameters:

- Group IP Address
- Prefix

28 Click on the OK button. The E-RP Group Range (Create) form closes and the new Embedded-RP entry appears in the table.

29 Click on the Group To RP tab button.

30 In the Static RP tab, click on the Add button to add a new entry, if required. The Static RP (Create) form opens.

31 Configure the parameters:

- Static RP IP Address
- RP Override

32 Click on the Static Group-To-RP tab button.

33 Click on the Add button to add a new entry, if required. The Static Group To RP (Create) form opens.

34 Configure the parameters:

- Static Group IP Address
- Static Group Mask

35 Click on the OK button. A dialog box appears.

36 Click on the OK button. The new Static Group-To-RP entry appears on the form.

37 Click on the OK button. A dialog box appears.

38 Click on the OK button. The new Static RP entry appears on the form.

39 If you are performing this procedure to create a PIM site on a VPRN routing instance (referenced from Procedure 71-3), the MVPN tab button appears. Click on the MVPN tab button. Otherwise, go to step 45.

40 Configure the parameters:

- Auto-Discovery
- MCast Signaling
- Inclusive Tunnel Type

Note — You must set the Inclusive Tunnel Type parameter to PIM if you are creating a PIM inclusive tunnel in step 41. You must set the Inclusive Tunnel Type parameter to RSVP if you are creating an RSVP inclusive tunnel in step 41.

41 Click on the MVPN Inclusive Tunnel tab button. Perform one of the following:

a Click on the PIM tab button to create a PIM inclusive tunnel, if required.

i Configure the parameters:

- Provider Tunnel Inclusive PIM Mode
- Group Address

The Group Address parameter is only configurable if the Provider Tunnel Inclusive PIM Mode parameter is set to ASM or SSM.

ii Go to step 42.

b Click on the RSVP tab button to create an RSVP inclusive tunnel, if required.

i Configure the P2MP Administrative State parameter. Until you have selected an MVPN LSP template, you cannot set the P2MP Administrative State parameter to Up. To create an MVPN LSP template, see Procedure 29-23.

ii Click on the Select button. The Select MVPN Lsp Template form opens.

iii Choose an MVPN LSP template from the list and click on the OK button. The MVPN LSP template is displayed.

42 Click on the MVPN Selective Tunnel tab button. The Data MVPN Threshold tab is displayed.

43 Configure the parameters:

- PIM SSM Prefix
- PIM SSM Prefix Length
- Delay Interval (seconds)
- Pack Data Join TLV
- Auto-Discovery

The Delay Interval (seconds) parameter can only be configured if the Include Data parameter is enabled.

44 Perform one of the following:

a Click on the Search button in the Data MVPN Threshold tab.

i Select a Data MVPN Threshold entry from the displayed list.

ii Click on the Apply button.

iii Go to step 45.

b Click on the Add button in the Data MVPN Threshold tab. The Data MVPN Threshold (Create) form is displayed.

i Configure the parameters:

- Group IP Address
- Group Prefix Length
- Threshold (kbps)

ii Click on the OK button. The Data MVPN Threshold (Create) form closes and the new entry is displayed in the list.

iii Select the new Data MVPN Threshold entry.

iv Click on the Apply button.

45 Perform one of the following, if required:

Note — A Data Multicast Tunnel (MT) can be thought of as a connector between a set of PE routers forming a multicast domain. From the perspective of a VPN-specific PIM instance, a multicast tunnel is a single multi-access interface. The Data MT Interface can only be created or selected when the PIM address is configured as other than null (0.0.0.0).

a Click on the Search button in the Data MT Interface tab.

i Choose a Data MT Interface entry from the list.

ii Click on the Apply button.

iii Go to step 46.

b Click on the Add button in the Data MT Interface tab. The Data MT Interface (Create) form is displayed.

i Configure the parameters:

- Administrative State
- Hello Interval (seconds)
- Hello Multiplier
- Improved assert
- Three Way Hello
- Tracking Support

ii Click on the OK button. The Data MT Interface (Create) form closes and the new entry is displayed in the list.

iii Select the new Data MT Interface entry.

iv Click on the Apply button.

46 Click on the Import Policies tab button.

47 Click on the BootStrap Import Policies tab button.

48 Configure the parameters to filter bootstrap messages and to control the flow of bootstrap messages to the routing instance.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

49 Click on the Join/Prune Import Policies tab button.

50 Configure the parameters to filter join/prune messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

51 Click on the Register Import Policies tab button.

52 Configure the parameters to filter PIM register messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

53 Click on the Export Policies tab button.

54 Click on the BootStrap Export Policies tab button.

55 Configure the parameters to filter PIM-related export messages.

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

56 Depending on the device version, the Anycast RP tab is configurable. Click on the Anycast RP tab button to configure Anycast RP, if required.

Note — You can use the PIM configuration form to add peers to an anycast RP. The complete configuration of anycast RP for PIM requires additional supporting components, such as the configuration of loopback interfaces and static RPs. Due to the complex configuration dependencies, Alcatel-Lucent recommends that you use the Virtual Anycast manager. The Virtual Anycast manager automatically configures many of the supporting requirements for the protocol, which reduces operator configuration errors and assists in troubleshooting activities. See Procedure 28-33 for more information about using the Virtual Anycast manager.

57 Click on the General tab button.

58 Configure the RP IP Address parameter.

59 Click on the Anycast Peer tab button.

60 Click on the Add button to create a new entry, if required. The Anycast Peer (Create) form opens.

61 Configure the Peer IP Address parameter.

62 Click on the OK button. A dialog box appears.

63 Click on the OK button. The new anycast peer entry appears on the form.

64 Click on the OK button. A dialog box appears.

65 Click on the OK button. The new anycast RP entry appears on the form.

66 Click on the SSM Groups tab button.

67 Click on the Add button to create a new entry, if required.

68 Configure the parameters:

- SSM Group IP Address
- SSM Group Mask

  These parameters are applicable to both IPv4 and IPv6.

69 Click on the OK button. A dialog box appears.

70 Click on the OK button. The new SSM group entry appears on the form.

71 Click on the Interfaces tab button to create an interface, if required.

i Click on the Add button to add a new entry.

ii Perform steps 4 to 10 of Procedure 28-34.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new interface entry appears on the form.

72 Click on the SPT Switch Threshold tab button to configure SPT switchover, if required.

73 Click on the Add button to create a new entry, if required. The Spt Switch Over Threshold (Create) form opens.

74 Configure the parameters:

- Group IP Address
- Group Prefix Length
- Infinity for Threshold
- Threshold (kbps)

75 Click on the OK button. A dialog box appears.

76 Click on the OK button. The new SPT switch threshold entry appears on the form.

77 Click on the following tab buttons to view and edit information.

- Groups
- Neighbor
- Statistics
- Faults

The Statistics and Faults tabs are unavailable for PIM in VPRN.

78 Click on the OK button. A dialog box appears.

79 Click on the Yes button. The PIM (Edit) form closes.

Procedure 28-33 To configure Anycast PIM on a router

This procedure describes how to use the Virtual Anycast Manager to configure anycast PIM on a router. The Virtual Anycast Manager automatically configures many of the supporting requirements for the protocol, which reduces operator configuration errors and assists in troubleshooting activities.

Note — The 5620 SAM does not automatically delete the supporting requirements for the protocol when you delete an anycast RP member.

You can also manually add peers to an anycast RP by navigating to the Anycast RP tab of the PIM configuration form. Ensure that PIM is enabled on the router. See Procedure 28-32 for more information.

The 5620 SAM raises an alarm when VRFs from different VPRNs are added to a single anycast RP set. You can only mismatch VRFs using methods that are not associated with the Virtual Anycast Manager; for example, by using the CLI or the PIM configuration form.

1 Choose Manage→Networking→Virtual Anycast RP from the 5620 SAM main menu. The Manage Virtual Anycast RP form opens.

2 Click on the Create button. The Virtual Anycast RP form opens with the General tab displayed.

3 Configure the parameters:

- Anycast RP Type
- Anycast RP Address
- Name
- Description
- Auto Created Interface Name

4 If the Anycast RP Type parameter value is VPRN, choose a VPRN service for the anycast RP.

i Click on the Select button. The Select Service form opens.

ii Select a VPRN service in the list and click on the OK button. The Select Service form closes, and the service is displayed in the Service panel.

5 Click on the Apply button. The Status panel appears. The Status panel is used in step 9 of this procedure to identify configuration problems.

6 Click on the Components tab button.

7 Add virtual Anycast RP members to the PIM configuration.

i Right-click on the Virtual Anycast RP Members icon and choose Add Anycast RP Member. The Enter Interface Name form opens.

ii Enter the interface name for the loopback interface. The Auto Created Interface Name parameter value appears, if configured.

iii Click on the OK button. The Enter Interface Name form closes, and the Select Local Address form opens.

iv Configure the filter criteria.

v Select the local IP address that is used to communicate with the other RP members in the virtual anycast set and click on the OK button. The new local address entry appears on the Components tab under the Virtual Anycast RP Members icon. The new local address entry also appears under the Static RP icon.

Note — The local address is typically the system address.

The 5620 SAM automatically performs the following virtual anycast RP required configuration tasks.

- It creates a PIM-enabled loopback interface, if not present, with the RP address.
- It adds a local address to the anycast RP peer set.
- It updates the peer sets that participate in the anycast RP so that all peer sets contain the same members.
- It enables PIM on the interface that contains the local IP address.
- It creates a static RP that uses the anycast RP address. Groups must be manually created using the Components tab.

vi Repeat steps 7 i to v for each member in the virtual anycast RP.

8 Add a static group-to-RP mapping for the anycast configuration.

i Right-click on a member in the Static RP list and choose Create Static RP. The Static RP (Create) form opens.

ii Configure the parameters:

- Static Group IP Address
- Static Group Mask

iii Click on the OK button. The Static Group To RP (Create) form closes.

iv Repeat steps 8 i to iii for each static group-to-RP mapping that you want to add to the virtual anycast RP configuration. Each member needs a static RP and at least one static group-to-RP mapping. The mappings typically use the same configuration values for each member in the group.

9 Verify the status of the anycast RP for PIM configuration.

i Click on the General tab button. The Status panel displays the status of the anycast RP configuration. The 5620 SAM updates the status when you add a member to or delete a member from the virtual anycast RP. You can also use the Update Status button to manually update the Status panel.

Table 28-3 lists the status check boxes that identify potential configuration problems.

Table 28-3 Anycast RP status fields

Check box	Description
Missing Group Range(s) Configurations	At least one anycast RP member does not have a group range for the anycast RP address.
Inconsistent Peer Sets	Peer sets of all the anycast RP members are not equal.
PIM not enabled on loopback interface(s)	PIM is not enabled on all loopback interfaces that are configured in the virtual anycast RP.
Only one peer configured	Only one peer is configured for anycast RP. The configuration requires two or more peers for correct functionality.

(1 of 2)

Check box	Description
Loopback interface(s) not properly configured	At least one anycast RP member does not have a loopback interface configured with the anycast RP address.
Missing Static RP configuration(s)	A member of the virtual anycast RP does not have a static RP. Each member requires a static RP.

(2 of 2)

ii Click on the OK button. The Manage Virtual Anycast RP form reappears, and the new virtual anycast RP entry appears on the form.

iii Close the Manage Virtual Anycast RP form.

Procedure 28-34 To create a PIM interface

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to a PIM icon. The path is Routing→Router→Routing Instance→PIM.

3 Right-click on the PIM icon and choose Create Interface. The PIM Interface (Create) form opens with the General tab displayed.

4 Click on the Select button to choose a Layer 3 interface. The Select Interface - PIM Interface form opens.

5 Configure the filter criteria.

6 Select an interface in the list and click on the OK button. The Select Interface - PIM Interface form closes, and the interface name appears in the Interface panel.

7 Configure the parameters:

- Description
- Administrative State
- BFD Enabled

8 Click on the Behavior tab button.

9 Click on the General sub-tab.

10 Configure the parameters:

- Hello Interval (seconds)
- Hello Multiplier
- Tracking Support
- Multicast Senders
- BSM Check Router Alert
- Improved assert
- Assert Period
- Max Groups
- Three Way Hello
- Sticky DR
- DR Priority
- Sticky DR Priority

The Sticky DR Priority parameter is configurable when the Sticky DR parameter is enabled.

11 Click on the Neighbor tab button, if configurable, to view and edit information. The Neighbor tab is configurable only when a neighbor PIM interface exists.

12 Click on either the IPv4 or IPv6 sub-tab, as required.

13 Configure either the Ipv4 Administrative State or Ipv6 Administrative State parameter in the States panel, as required.

14 Click on the Multicast CAC tab button to add a multicast CAC policy, if required.

i Click on the Select button to choose a multicast CAC policy. The Select Multicast CAC Policy - PIM Interface form opens.

ii Select a multicast CAC policy from the list and click on the OK button. The Multicast CAC Policy - PIM Interface form closes, and the multicast CAC policy name appears in the Multicast CAC Policy panel.

iii Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)

iv Click on the Levels tab.

v Click on the Add button. The PIM Interface Multicast CAC level form opens.

vi Configure the parameters:

- Level ID
- Bandwidth (kbps)

vii Click on the LAG Port Down tab.

viii Click on the Add button. The PIM Interface Multicast CAC LAG Port Down form opens.

ix Configure the parameters:

- Number of Ports Down
- Level

15 Click on the OK button. The PIM Interface (Create) form closes, and an icon for the new PIM interface appears in the navigation tree below the PIM icon.

IGMP configuration

The 5620 SAM supports IGMP configuration for core router functionality and IP services.

Procedure 28-35 To enable IGMP on a router

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) configuration form opens.

4 Enable IGMP.

i Click on the Multicast tab button.

ii Select the IGMP Enabled parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes, and an IGMP icon appears in the navigation tree below the routing instance icon.

Procedure 28-36 To configure IGMP on a router

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the IGMP icon. The path is Routing→Router→Routing Instance→IGMP.

3 Right-click on the IGMP icon and choose Properties. The IGMP Site (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Last Member Query Interval (seconds)
- Query Response Interval (seconds)
- Robust Count

5 Click on the SSM Translation tab button to configure SSM, if required.

i Click on the Add button to create a new entry. The SSM Translation (Create) form opens.

ii Configure the parameters:

- Start Mcast Address
- End Mcast Address
- Configured Source

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new SSM entry appears on the form.

6 Click on the Interfaces tab button to add an interface, if required.

i Click on the Add button.

ii Perform steps 4 to 14 of Procedure 28-38.

iii Click on the OK button. The new interface entry appears on the form.

7 Click on the Group Interfaces tab button to view IES group interfaces added to IGMP, if required.

8 Click on the LDP Tunnel Interfaces tab button to create an LDP tunnel interface entry, if required.

i Click on the Add button. The LDP IGMP Tunnel Interface (Create) form opens with the General tab button displayed.

ii Click on the Select button next to the P2MP ID parameter. The Select - LDP IGMP Tunnel Interface form opens.

iii Select an LDP tunnel interface and click on the OK button. The LDP IGMP Tunnel Interface form reappears with the information displayed.

iv Click on the Static Group/Source tab button to create a static multicast entry, if required.

v Click on the Add button. The StaticGrpSrc (Create) form opens.

vi Configure the parameters:

- Static Multicast Group
- Static Source

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The new static multicast entry appears on the LDP IGMP Tunnel Interface (Create) form.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The LDP IGMP Tunnel Interface (Create) form closes.

9 Click on the RSVP Tunnel Interfaces tab button to create an RSVP tunnel interface entry, if required.

i Click on the Add button. The RSVP IGMP Tunnel Interface (Create) form opens with the General tab button displayed.

ii Click on the Select button next to the Lsp Name parameter. The Select - RSVP IGMP Tunnel Interface form opens.

iii Select an RSVP IGMP tunnel interface and click on the OK button. The Select - RSVP IGMP Tunnel Interface form closes and the RSVP IGMP Tunnel Interface (Create) form reappears with the information displayed.

iv Click on the Static Group/Source tab button to create a static multicast entry, if required.

v Click on the Add button. The StaticGrpSrc (Create) form opens.

vi Configure the parameters:

- Static Multicast Group
- Static Source

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The new static multicast entry appears on the form.

ix Click on the OK button. A dialog box appears. The RSVP IGMP Tunnel Interface (Create) form closes and the new tunnel entry is displayed.

x Click on the OK button. The RSVP IGMP Tunnel Interface (Create) form closes.

10 Click on the following tab buttons to view and edit information.

- Multicast Group/Source
- Statistics
- Faults

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The Routing Instance (Edit) form closes.

Procedure 28-37 To configure IGMP on an OmniSwitch

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the IGMP icon. The path is Routing→ Routing Instance→IGMP.

3 Right-click on the IGMP icon and choose Properties. The IGMP (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- Administrative State
- Querying
- Spoofing
- Proxying
- Querier Forwarding
- Zapping
- Max Group Action
- Query Interval (seconds)
- Last Member Query Interval (tenths of seconds)
- Query Response Interval (tenths of seconds)
- Robust Count
- Max Group
- Protocol Version
- Router Timeout (seconds)
- Source Timeout (seconds)
- Unsolicited Report Interval (seconds)

Note — When the Administrative State parameter is Up, IP multicast switching is enabled on the OmniSwitch.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Routing Instance (Edit) form closes.

Note — IGMP parameters can also be configured for each VLAN site. The VLAN site IGMP configuration overrides the routing instance IGMP settings. You can only configure VLAN site IGMP parameters after the VLAN is created. See Procedure 65-11 for information about configuring IGMP on an OmniSwitch.

Procedure 28-38 To create an IGMP interface

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the IGMP icon. The path is Routing→Router→Routing Instance→IGMP.

3 Right-click on the IGMP icon and choose Create Interface. The IGMP Interface (Create) form opens with the General tab displayed.

4 Click on the Select button to choose a Layer 3 interface. The Select Interface - IGMP Interface form opens.

5 Configure the filter criteria.

6 Select an interface in the list and click on the OK button. The Select Interface - IGMP Interface form closes, and the interface name appears in the Interface panel.

7 Configure the parameters:

- Description
- Administrative State
- Administrative Version
- Maximum Number of Groups
- Subnet Check

8 Click on the Behavior tab button.

9 Configure the Import Policy parameter.

10 Click on the Multicast CAC tab button to add a multicast CAC policy, if required.

i Click on the Select button to choose a multicast CAC policy. The Select Multicast CAC Policy - IGMP Interface form opens.

ii Select a multicast CAC policy from the list and click on the OK button. The Multicast CAC Policy - IGMP Interface form closes, and the multicast CAC policy name appears in the Multicast CAC Policy panel.

iii Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- Constraint Admin State

11 Click on the SSM Translation tab button, if required.

i Click on the Add button.

ii Configure the parameters:

- Start Mcast Address
- End Mcast Address
- Configured Source
- Start Mcast Address Type
- End Mcast Address Type
- Configured Source Type

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new SSM translation entry appears on the form.

12 Click on the Static Group/Source tab button to create a static multicast entry, if required.

i Click on the Add button.

ii Configure the parameters:

- Static Multicast Group
- Static Source

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new static multicast entry appears on the form.

13 Click on the following tab buttons to view and edit information.

- Multicast Group
- Multicast Group/Source

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The IGMP Interface (Create) form closes, and an icon for the new interface appears in the navigation tree below the IGMP icon.

Procedure 28-39 To turn up or shut down an IGMP interface

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Navigate to the IGMP icon. The path is Routing→Router→Routing Instance→IGMP.

3 Right-click on the interface icon and choose Properties. The IGMP Site (Edit) form opens.

4 Click on the Interfaces tab button.

5 Turn up or shut down the IGMP interface.

a Click on the Turn Up button to activate the interface. A dialog box appears.

b Click on the Shut Down button to deactivate the interface. A dialog box appears.

6 Click on the Yes button to confirm the action and close the dialog box.

7 Close the IGMP Site (Edit) form.

MSDP configuration

The MSDP command hierarchy consists of three levels:

- global level
- peer level and group level
- group peer level

MSDP parameters are initially applied at the global level. These parameters are inherited by the group and peer levels. Parameters can be modified and overridden on a level-specific basis.

Procedure 28-40 To enable MSDP on a router

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance.

3 Right-click on the routing instance icon and choose Properties. The Routing Instance (Edit) form opens.

4 Enable MSDP by performing the following steps.

i Click on the Multicast tab button.

ii Select the MSDP Enabled parameter.

5 Click on the OK button. A dialog box appears.

6 Confirm the action. The Routing Instance (Edit) form closes, and an MSDP icon appears in the navigation tree below the routing instance icon.

Procedure 28-41 To configure global-level MSDP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MSDP icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Properties. The MSDP (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- SA Limit
- Data Encapsulation
- Local IP Address
- RPF Lookup Sequence
- SA Cache Lifetime (seconds)
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Click on the Group tab button to add a group, if required. See Procedure 28-42 for more information about how to configure a group-level MSDP.

6 Click on the Peer tab button to add a peer, if required. See Procedure 28-43 for more information about how to configure a peer-level MSDP.

7 Click on the Source tab button to add a source, if required. See Procedure 28-44 for more information about how to configure an MSDP source.

8 Click on the Import Policies tab button.

9 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

10 Click on the Export Policies tab button.

11 Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 27. A router performs no validation to ensure the policies match.

12 Click on the following tab buttons to view information.

- Data Source Active
- Statistics
- Faults

13 Click on the OK button. A dialog box appears.

14 Confirm the action. The MSDP (Edit) form closes.

Procedure 28-42 To configure group-level MSDP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the routing instance icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Create Group. The MSDP Peer Group (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Mode
- SA Limit
- Local IP Address
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Click on the Peer tab button to add a peer, if required.

6 Click on the Add button. The MSDP Peer Group (Create) form opens.

7 Configure the parameters:

- Peer Address
- SA Limit
- Local IP Address
- Default Peer
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

8 Configure the import and export policies for the MSDP peer by performing the following steps.

i Click on the Import Policies tab button.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab button.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

9 Click on the Authentication tab button.

10 Configure the parameters:

- Type
- Key

11 Click on the OK button. The MSDP Peer Group (Create) form closes and a dialog box appears.

12 Confirm the action. The peer is listed on the MSDP Peer Group (Create) form.

13 Configure the import and export policies for the MSDP group by performing the following steps.

i Click on the Import Policies tab button.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab button.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

14 Click on the OK button. The MSDP Peer Group (Create) form closes, and an MSDP Peer Group icon appears in the navigation tree below the MSDP Routing Instance icon.

Procedure 28-43 To configure peer-level MSDP

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MSDP icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Create Peer. The MSDP Peer (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Peer Address
- SA Limit
- Local IP Address
- Default Peer
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Configure the import and export policies by performing the following steps.

i Click on the Import Policies tab button.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab button.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

6 Click on the Authentication tab button.

7 Configure the parameters.

- Type
- Key

8 Click on the OK button. The MSDP Peer (Create) form closes, and an MSDP Peer icon appears in the navigation tree below the MSDP Routing instance icon.

Procedure 28-44 To configure an MSDP source

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MSDP icon. The path is Routing→Router→Routing Instance→MSDP.

3 Right-click on the MSDP icon and choose Properties. The MSDP (Edit) form opens with the General tab displayed.

4 Click on the Source tab button.

5 Click on the Add button. The MSDP Source (Create) form opens.

6 Configure the parameters:

- IP Prefix
- Mask
- SA Limit

7 Click on the OK button. The MSDP Source (Create) form closes and a dialog box appears.

8 Confirm the action. The source is listed on the MSDP (Edit) form.

9 Click on the OK button. A dialog box appears.

10 Confirm the action. The MSDP (Edit) form closes.

Procedure 28-45 To configure group-peer-level MSDP

Note — The parameters that you configure for a MSDP peer take precedence over the parameters that are configured for the MSDP peer group.

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Navigate to a peer group. The path is Routing→Router→Routing Instance→MSDP→MSDP Peer Group.

3 Right-click on the peer group icon and choose Create Peer. The MSDP Group Peer, MSDP Peer Group (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Peer Address
- SA Limit
- Local IP Address
- Default Peer
- Receive Message Rate
- Receive Message Interval (seconds)
- Receive Message Threshold
- Administrative State

5 Configure the import and export policies by performing the following steps.

i Click on the Import Policies tab button.

ii Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the import route policy to determine which routes are accepted from peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

iii Click on the Export Policies tab button.

iv Configure the parameters:

- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Configure the export route policy to determine which routes are advertised to peers. These policies should match the policies you set when configuring the Routing Policy Manager, as described in chapter 27. There is no validation performed by the router to ensure the policies match.

6 Click on the Authentication tab button.

7 Configure the parameters:

- Type
- Key

8 Click on the OK button. The MSDP Group Peer, MSDP Peer Group (Create) form closes, and an MSDP Group Peer icon appears in the Navigation Tree below the MSDP Peer Group icon.

Procedure 28-46 To enable or disable MSDP peering

1 From the 5620 SAM, choose Routing from the navigation tree view selector.

2 Perform one of the following:

a Enable or disable MSDP peering in a peer group.

i Navigate to an MSDP peer group. The path is Routing→Router→Routing Instance→MSDP→MSDP Peer Group.

ii Right-click on an MSDP Peer Group icon.

b Enable or disable MSDP peering in a group peer.

i Navigate to an MSDP peer group. The path is Routing→Router→Routing Instance→MSDP→MSDP Peer Group→MSDP Group Peer.

ii Right-click on an MSDP Group Peer icon.

3 Choose one of the following menu items:

a Turn Up to activate

b Shut Down to deactivate

A dialog box appears.

4 Click on the Yes button. The state information beside the appropriate MSDP icon changes accordingly.

MLD configuration

MLD is an asymmetric protocol used by IPv6 routers to discover the presence of multicast listeners, that is, nodes that wish to receive multicast packets. MLD specifies separate behaviors for multicast address listeners and multicast routers.

The purpose of MLD is to enable each multicast router to discover, for each of its directly attached links, which multicast addresses and which sources have interested listeners on that link. The information gathered by MLD is provided to whichever multicast routing protocol is used by the router, such as PIM, to ensure that multicast packets are delivered to all links where there are listeners interested in such packets.

MLD is only supported on a chassis mode (C or D) that supports IPv6.

Procedure 28-47 To enable MLD on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to a routing instance by choosing Network→Router→Routing Instance.

3 Right-click on the Routing Instance and choose Properties. The Routing Instance (Edit) form opens with the General tab displayed.

4 Click on the Multicast tab and enable the MLD Enabled check box.

5 Click on the OK button. The Routing Instance (Edit) form closes, and an MLD icon appears in the navigation tree below the routing instance.

Procedure 28-48 To configure MLD on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MLD icon by choosing Network→Router→Routing Instance→MLD.

3 Right-click on the MLD icon and choose Properties. The MLD, Routing Instance (Edit) form opens with the General tab displayed.

4 Configure the optional parameters:

- Query interval (seconds)
- Last Member Query Interval (seconds)
- Query Response Interval (seconds)
- Robust Count

5 Click on the Apply button to save the changes.

6 Click on the SSM Translation tab button, and click on the Add icon. The SSM Translation, Routing Instance window opens.

7 Configure the mandatory parameters:

- Start Multicast Address
- End Multicast Address
- Configured Source

8 Click on the Apply button to save the changes.

If you wish to create an MLD interface from this window:

a Click on the Interface tab button and click on the Add icon. Go to step 4 of Procedure 28-49.

b Click on the OK button. The MLD, Routing Instance (Edit) form closes.

Procedure 28-49 To create an MLD interface on a routing instance

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Navigate to the MLD icon by choosing Network→Router→Routing Instance→MLD.

3 Right-click on the MLD icon and choose Create Interface. The MLD Interface, Routing Instance (Create) form opens with the General tab displayed.

4 Configure the optional parameter Description.

5 Click on the Select icon button. The Select Interface - MLD Interface - Routing Instance window opens.

6 Select an existing network interlace that has IPv6 enabled and click the OK button to save the entry. The Select Interface - MLD Interface - Routing Instance window closes and the MLD interface name appears in the navigation tree below the MLD icon.

7 Click on the Behavior tab button and configure the optional parameters:

- Maximum Number of Groups
- Query Interval (seconds)
- Maximum Response Time between Group Messages (seconds)
- Maximum Response Time For MLDv2 (seconds)

8 Click on the Apply button to save the changes.

9 Click on the Import Policy tab button.

10 Click on the Select icon to select an optional routing policy, or configure the optional parameter Import Policy.

11 Click on the Apply button to save the change.

12 Click on the Static/Group Source tab button and click on the Add icon. The MLD Group Source Static, null (Create) window opens.

13 Configure the mandatory Group Address parameter and the optional Group Source Address parameter.

14 Click on the Apply button to save the changes.

15 Click on the SSM Translation tab button and click on the Add icon. The MLD Interface Source Specific Multicast, null (Create) window opens.

16 Configure the mandatory parameters:

- Group Address One
- Group Address Two

17 Configure the optional parameter Group Source Address.

18 Click on the Apply button to save the changes.

19 Click on the OK button. The MLD Interface, Routing Instance (Create) form closes.

Bridging configuration

Bridging is used between a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device and a 7450 ESS to create a fast ring that bridges the end-user devices, such as BTV set-top boxes, and Layer 2 services, such as VPLS, that distribute multicast traffic. If required, you can configure the devices with MSTP or another STP.

STP is active by default on an OmniSwitch. The default mode of operation is 1x1 mode using RSTP. A loop-free network topology is automatically calculated based on default STP switch, bridge, and port parameter values.

Additional OmniSwitch configuration such as enabling and configuring OmniSwitch learned port security parameters for VLAN ports, DHCP relay, and DHCP snooping can be done while configuring other bridge parameters.

You can configure Multiple VLAN Registration Protocol (MVRP) as part of the bridging configuration on some versions of the OmniSwitch. MVRP provides a mechanism to maintain the contents of dynamic VLAN registration entries for each VLAN, and to propagate that information to other bridges.

In the 5620 SAM, a bridge is represented in the network view below a device, similar to the routing instance of a device.

Procedure 28-50 To configure bridging on a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device

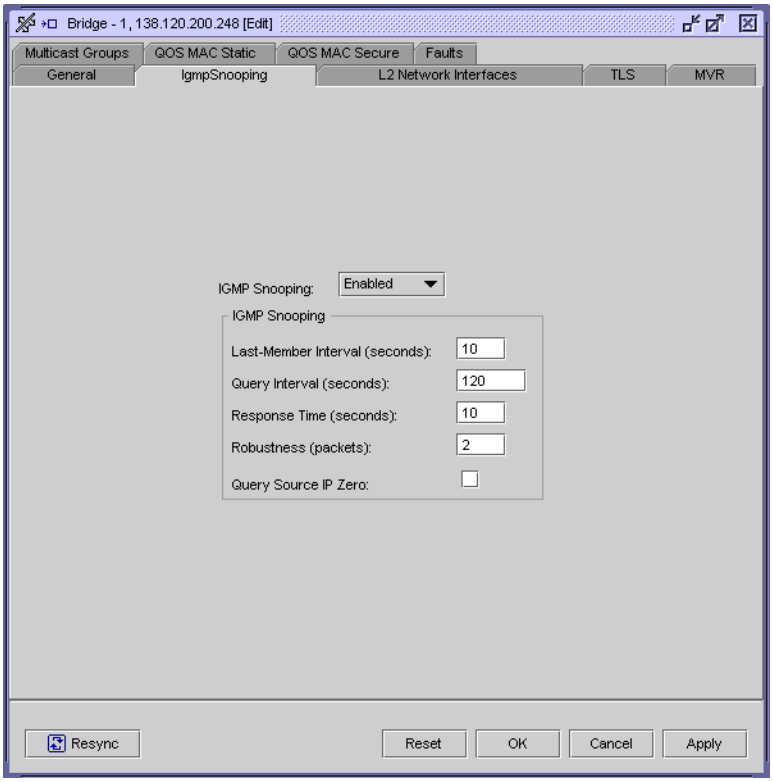
1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Click on an icon that represents a 7250 SAS or Telco device. The Bridge Instance icon appears.

3 Right-click on the Bridge Instance icon and choose Properties. The Bridge (Edit) form opens with the General tab displayed.

4 Click on the IGMP Snooping tab button. Figure 28-11 shows the Bridging configuration form with the IGMP Snooping tab displayed.

Figure 28-11 Bridging configuration form - IGMP Snooping tab



5 Configure the parameters:

- IGMP Snooping
- Query Source IP Zero

You must set the IGMP Snooping parameter to Enabled before you can configure the Query Source IP Zero parameter. IGMP snooping is required in a BTV VLAN and when MVR is used in a ring group to which the device belongs.

6 Click on the TLS tab button to configure parameters associated with 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices in TLS VLAN ring groups.

7 Configure the parameters:

- TLS Admin Status
- Ethertype
- Jumbo Frame

The Jumbo Frame parameter is configurable only for Telco devices.

8 Click on the MVR tab button to configure parameters associated with 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices in BTV ring groups.

9 Configure the parameters:

- MVR Admin Status
- Mode
- Query Time

The Mode parameter is configurable only for Telco devices.

10 Click on the Multicast Groups tab button to view the list of multicast group IP addresses for the specified VLAN.

11 Click on the QoS MAC Static tab button to configure static MAC QoS parameters for a port on the bridge.

Note — The QoS MAC Static tab button is not available for 7250 SAS and 7250 SAS-ES NEs, Release 2.0 or newer and the 7250 SAS-ESA.

i Click on the Add button. The QoS MAC Static Entry form opens.

ii Configure the parameters:

- Displayed Name
- Description
- MAC Address
- VLAN ID
- Priority

iii Click on the Select button to choose a physical port on the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device as an interface. The Select Interface form opens.

iv Select a port in the list and click on the OK button. The Select Interface form closes, and the port identifier appears in the Interface panel.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The new static MAC QoS entry appears on the form.

12 Click on the QoS MAC Secure tab button to configure secure MAC QoS parameters for the bridge.

Note — The QoS MAC Secure tab button is not available for 7250 SAS and 7250 SAS-ES NEs, Release 2.0 or newer or the 7250 SAS-ESA.

i Click on the Add button. The QoS MAC Secure Entry form opens.

ii Configure the parameters:

- Displayed Name
- Description
- MAC Address
- VLAN ID
- Priority

iii Click on the Select button to choose a physical port on the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device as an interface. The Select Interface form opens.

iv Select a port in the list and click on the OK button. The Select Interface form closes, and the port identifier appears in the Interface panel.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The new secure MAC QoS entry appears on the form.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The Bridge (Edit) form closes.

Procedure 28-51 To configure bridging on an OmniSwitch

Perform this procedure to configure OmniSwitch bridging, STP, and LPS parameters.

Caution — Changing bridge parameter values may affect the spanning tree calculations and trigger a topology change in the network.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Locate and expand an object that represents an OmniSwitch. A Bridge Instance object appears below the OmniSwitch object.

3 Right-click on the Bridge Instance object and choose Properties. The Bridge (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- STP Mode
- Path Cost

Configure the Auto VLAN Containment parameter if you the chose the flat STP mode.

5 Configure LPS, if required.

i Click on the Learned Port Security tab button. The Learned Port Security General tab is displayed.

ii Configure the parameters:

- Learning Time Window (minutes)
- Status

Note 1 — The Status parameter does not appear on the form and the Restart Timer button is dimmed until you enter a non-zero value for the Learning Time Window (minutes) parameter.

Note 2 — Click on the Restart Timer button to restart the MAC source learning timer if you need to restart dynamic MAC address learning on a port.

iii Click on the Ports tab button.

iv Click on the Add button to select ports on which you want to enable learned port security. The Select Port - Bridge form opens.

v Choose one or more ports and click on the OK button. The Select Port - Bridge form closes and the selected ports appear in the Ports form.

vi Click on the Apply button to enable learned port security on the selected ports. A dialog box appears.

vii Click on the Yes button.

viii If you need to apply the same LPS properties to multiple ports but do not need to configure static MAC addresses on the ports, go to step 5xxiv.

Note — Static MAC addresses can only be added to LPS-enabled ports individually.

ix Choose a port and click on the Properties button. The Learned Port Security (Edit) form opens.

x Click on the Properties button. The Physical Port (Edit) form opens on the General tab.

xi Click on the LPS Learned MAC Entries tab button.

xii Click on the Add button to add static MAC entries. The MAC Entries (Create) form opens.

Note — A port must be LPS-enabled and belong to a VLAN before you can add static MAC addresses.

xiii Click on the Select button. The Select VLAN Site - MAC Entries form opens.

xiv Configure the filter criteria. A list of VLANs appears at the bottom of the Select VLAN Site - MAC Entries form.

xv Choose a VLAN from the list.

xvi Click on the OK button. The Select VLAN Site - MAC Entries form closes.

xvii Configure the MAC Address parameter.

xviii Click on the Apply button to save the configuration.

xix Repeat steps 5xvii to 5xviii if you need to add another static MAC address to the port.

xx Click on the OK button. A dialog box appears.

xxi Click on the Yes button to close the dialog box.

xxii Click on the OK button to close the Physical Port (Edit) form. A dialog box appears.

xxiii Click on the Yes button. Go to step 5xxv.

xxiv Choose multiple ports and click on the Properties button. The Learned Port Security (Edit) form opens.

xxv Configure the parameters:

- Violation
- Administrative State
- Low MAC Range
- High MAC Range
- Max. MAC Addresses to Learn
- Max. Filtered MACs to Learn
- Trap Threshold

xxvi Click on the OK button to save the configuration and close the Learned Port Security (Edit) form.

xxvii If you need to stop the aging out of dynamic MAC addresses on the LPS port, convert the dynamic MAC addresses to static MAC addresses. Choose the port and click on the Convert to Static button.

Note — If traffic containing MAC addresses outside of the allowable MAC address range attempts to access an LPS port, the switch either restricts access to the port for that traffic or shuts the port down to all traffic. When this happens, the port is in an operationally violated state and an alarm is raised.

See Procedure 28-52 for information about how to release a violated LPS port.

6 Perform one of the following actions:

a Configure the STP Flat Mode.

b Configure the STP 1x1 Mode; go to step 25.

7 Click on the Spanning Tree tab button. The STP Flat Mode CIST General tab is displayed.

8 Configure the parameters:

Caution — Changing the Protocol parameter to MSTP resets the flat bridge priority and path.

- Protocol
- Forwarding Delay (seconds)
- Max Age (seconds)
- Instance BPDU Switching
- Priority
- Hello Time (seconds)
- TX Hold Count

9 Click on the Port tab button.

10 Choose one or more ports from the list.

11 Click on the Properties button. The CIST Instance Ports (Edit) form opens.

12 Configure the parameters:

- Priority
- Mode
- Admin Edge
- Restricted Role
- Path Cost
- Connection Type
- Auto Edge
- Restricted TCN

13 Click on the OK button. The CIST Instance Ports (Edit) form closes.

14 Click on the MSTI tab button if you need to configure MSTI, otherwise go to step 34.

Note — In order to configure MSTI, the Protocol parameter must be set to MSTP.

15 Click on the Add button. The MST Instance (Create) form opens.

16 Configure the parameters:

- Instance Index
- Priority
- Instance Name
- Auto VLAN Containment

17 Click on the VLAN tab button.

18 Click on the Add button to assign a VLAN to the MSTI. The Select VLAN Sites - MST Instance form opens.

19 Choose one or more VLANs from the list and click on the OK button. The VLANs appear on the MST Instance VLAN form.

20 Click on the OK button. A dialog box appears.

21 Click on the Yes button.

22 Click on the MST Region tab button.

23 Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

24 Go to step 34.

25 Click on the Spanning Tree tab button.

Caution — Changing the STP 1x1 Mode configuration may affect the STP calculations for this instance of the VLAN and trigger a topology change in the network.

26 Click on the STP 1x1 Mode tab button.

27 Choose a 1x1 instance from the list and click on the Properties button. The VLAN STP Instance (Edit) form opens with the General tab displayed.

28 Configure the parameters:

- Protocol
- Forwarding Delay (seconds)
- Max Age (seconds)
- Instance BPDU Switching
- Priority
- Hello Time (seconds)
- TX Hold Count

29 Click on the Port tab button.

30 Choose one or more ports from the list of ports that have been assigned to VLANs and click on the Properties button. The VLAN STP Instance Ports (Edit) form opens.

31 Configure the parameters:

- Priority
- Mode
- Admin Edge
- Restricted Role
- Path Cost
- Connection Type
- Auto Edge
- Restricted TCN

32 Click on the OK button. The VLAN STP Instance Ports (Edit) form closes.

33 Click on the OK button. The VLAN STP Instance form closes.

34 Click on the TLS tab button.

35 Configure the TLS Mode parameter.

36 Click on the QoS tab button.

37 Configure the parameters:

- QoS Status
- Trust Ports
- Default Servicing Mode
- Default Bridged Disposition
- Default Routed Disposition
- Default IGMP Disposition

38 Click on the Apply button. A dialog box appears.

39 Click on the Yes button. The applied values for the Default Bridged Disposition, Default Routed Disposition, and Default IGMP Disposition parameters should be the same as the configured values.

40 Click on the IGMP Port Group Limit tab button.

41 Configure the filter criteria. A list of ports appears.

Note — Only ports that are active (administratively Up) appear in the list.

42 Choose one or more ports from the list and click on the Properties button.

43 The IGMP Port Group Limit (Edit) or IGMP Port Group Limit - (Multiple Instances) (Edit) form opens.

44 Configure the parameters:

- Port Max Group
- Port Action

45 Click on the OK button.

Note — Click on the Multicast VLAN Port tab button in the multicast VLAN IGMP site properties to view the Port Max Group and Port Action parameter information for a multicast VLAN port. You can also view the number of IGMP groups dynamically learned by the port. See Procedure 65-12 for more information.

46 If you need to configure the IGMP port group limit parameters for an inactive (administratively Down) port, click on the Add button. Otherwise, go to step 57.

47 The Select Port form opens.

48 Configure the filter criteria. A list of ports appears.

49 Choose one or more ports from the list and click on the OK button. The Select Port form closes and the selected ports appear in the list of ports.

50 Choose an inactive port from the list and click on the Properties button.

51 Configure the parameters:

- Port Max Group
- Port Action

52 Repeat steps 50 and 51 for each inactive port that you need to configure.

53 Click on the Apply button. A dialog box appears.

54 Click on the Yes button to save your configuration.

Note 1 — The inactive ports do not appear in the list of ports. Only active ports are displayed in the list. You can view the configuration of the inactive ports using the OmniSwitch CLI.

Note 2 — Click on the Multicast VLAN Port tab button in the multicast VLAN IGMP site properties to view the Port Max Group and Port Action parameter information for a multicast VLAN port. You can also view the number of IGMP groups dynamically learned by the port. See Procedure 65-12 for more information.

55 Click on the MVRP tab button to configure MVRP (if required).

56 Configure the parameters:

- VLAN Registration Protocol Type
- Status
- Transparent Switching Status
- Max VLAN

57 Click on the OK button. A dialog box appears.

58 Click on the Yes button. The Bridge (Edit) form closes.

Procedure 28-52 To release a violated OmniSwitch LPS port

Perform the following procedure to release a violated LPS port.

1 From the 5620 SAM GUI, choose Routing from the navigation tree view selector.

2 Locate and expand an object that represents an OmniSwitch. A Bridge Instance object appears below the OmniSwitch object.

3 Right-click on the Bridge Instance object and choose Properties. The Bridge (Edit) form opens with the General tab displayed.

4 Click on the Learned Port Security tab button. The Learned Port Security General tab is displayed.

5 Click on the Port tab button.

6 Select one or more violated LPS ports. Violated LPS ports are highlighted in orange. When you select one or more violated ports the Release Violated Port button is enabled.

7 Click on the Release Violated Port button to release the selected ports. Releasing a violated port restores the port to the same operational state it was in before the violation. When a violated port is released, all MAC addresses known to the port are flushed from the switch MAC address table.

8 Close the Bridge (Edit) form.

29 — MPLS

29.1 MPLS overview

The 5620 SAM supports the configuration and provisioning of MPLS paths and LSPs.

MPLS is a data-carrying mechanism that emulates some properties of a circuit-switched network over a packet-switched network. MPLS prepends a packet with an MPLS header that is comprised of labels in a stack. As an NE forwards a packet through an MPLS network, it examines the top label for routing instructions and pops it off the stack; the contents below the label stack are not examined. The label stack is not removed until it reaches the egress NE.

MPLS uses one or more IGPs, such as IS-IS, OSPF, or RIP, to forward packets. Regardless of the IGP chosen, the MPLS configuration is the same. An advantage of MPLS is that if more than one IGP is enabled, it continues to work when another protocol fails. See chapter 28 for more information on IS-IS, OSPF, and RIP.

MPLS can be used as the underlying transport mechanism for service tunnels. For MPLS to be used as such, an MPLS mesh and an LSP mesh must be created before the tunnel is created. Since LSPs and service tunnels are unidirectional, they must be created in both directions. See chapter 30 for more information about service tunnels.

When MPLS is enabled on a 5620 SAM-managed NE routing instance, the 5620 SAM displays an MPLS instance below the routing instance in the network view of the navigation tree. Using this view, you can perform various functions on the MPLS instance, for example, assign an L3 interface to an MPLS instance.

If a link, NE, or path fails, MPLS can determine a redundant path by using fast reroute. Fast reroute uses an alternative NE to complete the failed LSP. Fast reroute provides the following types of route protection.

- Many-to-one—one backup route is maintained for multiple protected LSPs on an NE.
- One-to-one—a separate backup route is maintained for each protected LSP on an NE algorithm.

You can list and view MPLS objects such as MPLS and RSVP instances and interfaces, static and dynamic LSPs, cross connections, and MPLS paths using the 5620 SAM Manage MPLS Objects form.

LSPs

An LSP is a path through an MPLS network that is set up based on criteria in a forwarding equivalency class, or FEC. A FEC is a set of characteristics that define how NEs in an MPLS network forward packets that are bound to an MPLS label. A FEC includes specifications such as the destination IP address and QoS parameters. A FEC is associated with a specific LSP, but an LSP may be used for multiple FECs.

An LSP begins at a PE device called an LER, which is the ingress NE that prepends a label to a packet based on a FEC and sends the packets to the next transit NE in the path. The transit NE swaps the packet label for a new one, and sends the packet to the next NE. The LER that acts as the egress PE NE removes the label and forwards the packet according to the header of the next layer, for example, IP.

LSPs are unidirectional; they enable the label switching of a packet through an MPLS network from one endpoint to another. Bidirectional communication through an MPLS network requires the configuration of an LSP in the opposite direction.

The types of LSPs are the following.

- Static LSPs specify a static path through an MPLS network. All transit NEs require manual configuration with LSP labels and require no signaling protocol, such as LDP or RSVP.
- Bypass-only LSPs are LSPs with manually configured bypass tunnels on Point-of-Local-Repair (PLR) nodes. Such LSPs are used exclusively for the purpose of bypass protection.
- Dynamic, or signaled LSPs, use a protocol such as LDP or RSVP. The signaling protocol allows an ingress NE to dynamically assign labels to an egress NE. You must configure the ingress NE, but not the transit NEs in an LSP. LDP LSPs are not explicitly defined. The downstream unsolicited (DU) method configures them automatically through the network.
- Point-to-Multipoint LSPs allow the source of multicast traffic to forward packets to one or many multicast receivers over a network without requiring a multicast protocol, such as PIM, to be configured in the network.

You can apply a metric value to a dynamic LSP or a Point-to-Multipoint LSP that determines which LSP the 5620 SAM uses when multiple LSPs lead to the same destination. The metric value for a static route is set to 1 and cannot be configured.

You can list and view detailed information on LSPs, templates, cross connections, service tunnels, and detour and bypass information on the LSP (Edit) forms.

Dynamic LSPs

A dynamic LSP uses a signaling protocol such as LDP or RSVP-TE and an MPLS path between two NEs. You can then create an LSP between the two NEs and bind it to an MPLS path. An LSP-MPLS path binding is called an LSP path. You can configure the LSP path after the MPLS path and the LSP are bound.

Dynamic LSPs are categorized as follows:

- Explicit-path LSPs resemble static LSPs when all hops are strict; each hop in the LSP requires explicit configuration. MPLS uses RSVP-TE to set up an explicit-path LSP. Transit NE hops can be strict, and use a direct path between NEs, or loose, and include other NEs in the path between NEs.
- Constrained-path LSPs have dynamically assigned intermediate NE hops that rely on CSPF to find a path that satisfies the LSP constraints. CSPF is a routing algorithm that takes different LSP constraints, such as the available bandwidth and MPLS administrative groups, into account to balance the network load. When the CSPF path is found, RSVP uses the path to request the LSP setup. If Fast Reroute is enabled, the ingress NE signals the downstream NEs to set up a detour configuration for the LSP.

When an LSP is established, the reserved bandwidth is controlled by the bandwidth parameter at the primary path level, regardless of whether the LSP has auto-bandwidth enabled. When auto-bandwidth is enabled and a trigger occurs, the NE attempts to change the bandwidth of the LSP to a value between the minimum and maximum bandwidth, which are configurable at the LSP level. Automatic bandwidth allocation is supported on RSVP LSPs that have both CSPF and MBB enabled. If an RSVP LSP is configured for auto-bandwidth, the ingress LER determines, at every adjust interval, whether to attempt an auto-bandwidth adjustment. You can change the minimum bandwidth, maximum bandwidth, or threshold parameters on an operational LSP, however, the changes do not take effect until the next auto-bandwidth trigger, for example, an adjust interval expiry. If the bandwidth adjustment fails, for example, the CSPF cannot find a path, the existing LSP is maintained with its existing bandwidth reservation. See Procedure 29-8 for more information.

Static LSPs

A static LSP uses an IGP instead of a signaling protocol, such as LDP or RSVP-TE. The 5620 SAM attempts to derive the hop configurations based on the hop labels in the path. You must use an ingress label that is unique within an NE when you create a new static hop; otherwise, the 5620 SAM rejects the new hop.

You can assign static label mappings for LSP cross-connections on an MPLS interface during interface creation or modification. A static label map is used only for intervening unmanaged NEs. The 5620 SAM attempts to derive the interface and label values from the swap egress label of the previous hop. The Static Label Maps form lists the static label maps for an interface whether they are created using the 5620 SAM client GUI, an OSS client, or CLI.

The 5620 SAM does not raise an alarm against an unmanaged NE.

The 5620 SAM raises an alarm against a static LSP under the following conditions when the LSP destination is managed by the 5620 SAM:

- No hops are configured for the static LSP.
- The last hop does not match the LSP destination.
- The label action specified for the last hop is not a pop action.

Point-to-Multipoint LSPs

A Point-to-Multipoint (P2MP) MPLS LSP allows the source of multicast traffic to forward packets to one or many multicast receivers over a network without requiring a multicast protocol, such as PIM, to be configured in the network. A P2MP LSP tree is established in the control plane for which the path consists of a head-end node, one or many branch nodes, and multiple leaf nodes. Packets that are injected by the head-end node are replicated in the data plane at the branching nodes before they are delivered to the leaf nodes.

The P2MP LSP has a source IP address but does not a have a destination address. Instead, you must create S2L Leaf nodes for each destination in the P2MP LSP tree. The P2MP LSPs are not supported in SDP bindings.

Each P2MP LSP object has one P2MP LSP Instance object. This is the primary instance, and can hold multiple child S2L Paths objects. Just as the P2MP LSP can appear as a tree, each S2L Path object then represents a root-to-leaf (S2L) sub-LSP path for the primary instance. The S2L Paths can be empty paths, or can specify a list of explicit hops. The same path can be used by more that one S2L of the instance. However the destination IP address must have a unique argument per S2L, because it corresponds to the address of the egress LER node.

PIM tunnel interfaces are associated with a P2MP LSP. The tunnel interfaces are needed at both the ingress LER and the egress LER nodes. You must also associate static multicast groups to the tunnel interfaces that are associated with the P2MP LSPs.

On the ingress side, you can create one or more tunnel interfaces in PIM and associate each with a different RSVP P2MP LSP. The tunnel interface is associated with the P2MP LSP name. You can then assign static multicast group joins to each tunnel interface using an IGMP configuration. A specific <*,G> or <S,G> can only be associated with a single tunnel interface. A multicast packet which is received on an interface and matches the <*,G> or <S,G> specified in the IGMP join for the tunnel interface is replicated and forwarded to all branches of the P2MP LSP.

On the egress side, the PIM tunnel interface is associated with both the P2MP LSP name and the system address of the ingress LER. You must define a multicast info policy to associate specific multicast groups, or a specific <S,G>, to the primary tunnel interface on each egress LER leaf node. The multicast info policy must then be applied to the router. A multicast packet synced from a tunnel interface associated with a P2MP LSP on the egress leaf node can then be forwarded over a PIM or IGMP interface, which can be an access interface or a network interface, including a spoke SDP-based IES interface. You may create multiple tunnel interfaces per node, where each interface is associated with a different P2MP LSP. The P2MP LSP association to a multicast group can be applied at the bundle, channel, and/or source channel level in the policy.

You can create a P2MP LSP using the LSP template for MVPN from the Policies→MPLS→LSP Template MVPN menu option. You can configure the scope as either local or global. The global template can be modified and multiple local versions can exist on the NEs. You must assign a default MPLS path to the template on the local definition before the template is turned up. If you modify the template, you must shut down the local policy first. When you turn up the local policy, all previously created P2MP LSP parameters are synchronized with the new template. See Procedure 29-23 for more information.

Bypass LSPs and manual bypass tunnels

You can create manual bypass tunnels and dynamic (or automatic) bypass tunnels on the SR/ESS, 7705 SAR, and 7210 SAS. You can manually configure an LSP to be bypass-only on a PLR node. The LSP is then used exclusively for the purpose of bypass protection.

You can use manual bypass alone or with dynamic bypass. When used with the dynamic bypass, the manual bypass has precedence over the dynamic bypass for the path selection.

Dynamic bypass tunnels can be disabled on a per node basis. They are enabled by default. If dynamic bypass is disabled on a node while dynamic bypass tunnels are active, traffic loss occurs. Furthermore, if no suitable manual bypass LSPs are found, the protected LSP remains without protection.

A bypass-only LSP does not have all the configurable attributes of a regular dynamic LSP. The main differences include:

- Manual bypass LSPs only support primary path. No secondary or standby paths can be created.
- Manual bypass LSPs do not support bandwidth or fast-reroute.
- Path monitoring is not available for manual bypass LSPs.
- Manual bypass LSPs cannot be assigned to a service tunnel, or be added to an LDP targeted peer as the LDP tunnelling LSP.
- There is no rule-based topology support available for manual bypass LSPs.
- There is no network-wide LSP view (the physical map LSP view) support available for manual bypass LSPs,
- You cannot create a static LSP using a tunnel template.

The following additional characteristics also apply to a manual bypass:

- The default protection level for a bypass tunnel is “node-protect”.
- CSPF is supported for the manual bypass tunnel. When CSPF is enabled, loose path and hop-less path are allowed on a manual bypass tunnel. The CSPF calculation is performed when the manual bypass tunnel is first set up.

Tunnel Templates

Tunnel templates allow users to configure dynamic LSP, LSP path, and SDP templates to define common characteristics for a tunnel or templatable tunnel object. Configure tunnel templates to reduce configuration time. See the *5620 SAM Scripts and Templates Developer Guide* for information about creating tunnel XML API templates.

To simplify creating tunnel templates, the 5620 SAM provides examples of common tunnel templates that can be copied and customized. You can also create a tunnel template from an existing templatable object. See the *5620 SAM Scripts and Templates Developer Guide* for information about using tunnel template examples and creating a tunnel template from an existing object.

After a template is configured, dynamic LSPs, LSP paths and SDPs can be configured by choosing a create from template button during configuration. Users can configure multiple LSP paths for a dynamic LSP. For example you can configure one primary, one standby, and many secondary LSP paths.

When the 5620 SAM auto-tunnel creation is used to create LSP paths, the LSP paths must use a hopless path. If the paths belong to the same LSP, they must use different MPLS paths, even when the MPLS paths are hopless. For a RSVP LSP policy, one LSP template can be specified. When an LSP template with multiple LSP paths is specified, many LSP paths are created.

LSP Path Optimization Policy

The 5620 SAM allows you to resignal LSP Paths to take advantage of new paths that are less congested, fewer hops, have a lower metric and meet least-fill criteria. NEs periodically check the network to determine whether a more efficient path is available and notify the 5620 SAM when another path is eligible for re-signalling. 5620 SAM maintains a list of LSP Paths that are eligible for re-signaling. When a LSP Path is eligible for optimization, the LSP Path can be routed to a different path. When a LSP Path not eligible for optimization, the LSP Path cannot use newly available network resources.

A LSP Path optimization policy allows the operator to filter the LSP Path candidates and set the execution rules to determine the candidacy and priority of an LSP Path for re signalling. The 5620 SAM operator can define LSPs Paths that are eligible for re-signaling and if a path is selected, the LSP Path is added to a candidate list. Execution rules determine the sequence in which the LSP Paths can re-signal and the number of seconds between re-signalling. Execution rules apply to the entire candidate list. Each time that optimization starts, the candidate list is filtered according to the candidate definition values and then re sequenced according to the sequencing target and order values.

To ensure that NEs are not overloaded by LSP re-signaling, an LSP Path optimization schedule can be created to identify when re-signaling can be evaluated and executed. You can also manually execute LSP Path optimization schedules. To avoid network congestion and maintain QoS standards, one policy should be executed at a time. Repetitive re-signaling requests are ignored, including manual or scheduled re-signaling requests. However, a re-signaling request that is initiated from the LSP Path binding properties window executes regardless of whether another LSP optimization policy is in progress.

The NEs notify the 5620 SAM about the current state and outcome of LSP Path re-signaling. You can access the LSP Path property window to view information about the state of LSP Path optimization. The following parameters are displayed:

- The Resignal Eligible parameter indicates whether a LSP Path is eligible for optimization. When the parameter value is true, the LSP Path can be optimized. When the parameter value is false, the LSP Path is not eligible for optimization.
- The Last Performed Type parameter indicates how resignaling was performed. Typically the value is Manual Resignal. However, if a schedule was set, the value is Timer Based Resignal.
- The Last Performed parameter indicates the last time the LSP Path was chosen to be re-signaled.
- The Last Performed State parameter indicates the re-signal state of a specific LSP Path.

LDP-over-RSVP tunnels

In networks that contain dozens of NEs spanning multiple routing areas, many RSVP service tunnels may be required. To reduce the number of RSVP tunnels required for service deployment in large networks, you can use the 5620 SAM to create LSPs using LDP-over-RSVP, sometimes called tunnel-in-tunnel encapsulation. An SDP can ride on multiple LDP-over-RSVP tunnels.

The 5620 SAM supports automatic, rule-based service-tunnel creation using NEs that are grouped according to their role in the 5620 SAM-managed network. This functionality greatly reduces the time and effort required to provision a mesh of service tunnels. See chapter 30 for more information about rule-based automatic service-tunnel creation.

The 5620 SAM can use tunnel rules and groups to create new RSVP LSP bindings between a PE device that is added to the network and the existing ABRs. It can also create a new LDP-over-RSVP tunnel between a new NE and an existing PE NE. See chapter 30 for more information about tunnel creation using rules and groups.

Service traffic that is transported by an LDP-over-RSVP tunnel requires a VC label, an LDP label, and an RSVP label. Unlike T-LDP sessions that use IGP SPF algorithms, RSVP LSPs are not advertised to an IGP instance. When the same FEC applies to the destination of an LDP-over-RSVP LSP tunnel and an IGP-based LDP tunnel, the 5620 SAM uses the LDP tunnel by default to minimize network overhead.

Using tunnel-in-tunnel encapsulation, a pair of LSP tunnels and a T-LDP session between two NEs are equivalent to two adjacent LDP NEs with a non-tunneled LDP session between them. In other words, the LDP tunnel uses the RSVP LSP as one hop between LSRs in the network.

During the configuration of LDP-over-RSVP, you can specify an explicit list of dynamic and static LSPs, or use the 5620 SAM to find eligible LSPs. After an LSP is explicitly configured for LDP tunnelling, the 5620 SAM associates the LDP targeted peer with the LSP.

You can configure LDP-over-RSVP to enable an OSPF area router to be a stitching point. You can specify which NEs to use as the stitching points in each area. When there are many NEs in an area, this function helps to reduce the number of LSPs required, because a full mesh is not required.

For an LSP to be eligible for LDP-over-RSVP, the following conditions apply:

- The LSP must be an RSVP-owned LSP (strict or loose)
- The LSP must start and terminate either on:
  - The router ID (system IP address)
  - The router ID (loopback address when used in multi-instance OSPF
- The OSPF system/loopback address must be advertised
- A T-LDP session must exist between the originating and terminating routers using the addresses cited above
- LDP-over-RSVP availability must be enabled in the LSP configuration. This indicates that the LSP is eligible for LDP-over-RSVP, and RSVP signals to the IGP that the LSP should be included in the SPF run.

Shared Risk Link Groups

Shared Risk Link Groups, or SRLGs, are constructs which allow you to perform two operations that enhance overall system reliability. Firstly, you can establish a FRR LSP path. In addition, you can also use SRLGs to establish a secondary LSP path which is disjointed from the primary LSP path.

Configured SRLGs are associated with MPLS interfaces. The SRLGs are used by the CSPF when computing a FRR detour/bypass path, or a secondary LSP path. Links which are members of the same SRLG represent resources which are assumed to share the same risk. These links are therefore avoided when computing and setting up an alternate LSP path.

- FRR backup

  The SRLG constraint can be enabled system-wide on a PLR node, in the computation of a FRR detour or bypass to be associated with a primary LSP path. CSPF includes the SRLG constraint in the computation of a FRR detour or bypass. CSPF then prunes all links with interfaces which belong to the same SRLGs as the egress interface being protected (or the immediate downstream node, depending on the protection level). If a path is found, the bypass or detour is set up. If not, and you included the Enable SRLG for FRR - Strict option, then the bypass or detour is not set up. If the Enable SRLG for FRR - Strict option is not specified, and a path exists that meets other TE constraints (other than the SRLG constraint), then the bypass or detour is still set up.
- Secondary LSP backup

  The SRLG constraint can also be enabled per LSP path on a head-end LER in the computation of an LSP secondary path that includes the standby path. The SRLG constraint is additional to the admin group constraint on the same secondary LSP path. CSPF includes the SRLG constraint in the computation of the secondary LSP path, which requires that the primary LSP path is configured and active. CSPF prunes links with interfaces that belong to the same SRLGs as the interfaces included in the primary path. If a path is found, the secondary LSP path is set up. Otherwise, CSPF keeps trying to set up the secondary LSP path.

You can enable only the SRLG constraint for the FRR backup operation. However, you can enable both the SRLG constraint and the admin-group include/exclude constraint for the secondary LSP backup path operation. In either case, you can still apply the admin-group constraint for the primary path.

The following conditions also apply to SRLGs:

- An SRLG is modeled as a policy object. It therefore follows the normal policy behavior for creation, listing, updating, deletion, distribution and resynchronization
- SRLGs are defined node wide
- Configured SRLGs are associated with MPLS interfaces. A specific MPLS interface can belong to multiple SRLGs. Up to 64 SRLGs can be associated with a specific MLPLS interface

Bandwidth-based equal cost RSVP LSP path selection

When multiple equal-cost paths satisfy the constraints of a specific RSVP LSP path, CSPF in the 7x50 head-end node uses a random number generator to select a path and return it to MPLS. While this method actually balances the number of LSP paths over the links in the network, it does not necessarily balance the bandwidth utilization across those links.

In order to achieve load balancing of the bandwidth amongst the available LSP paths, CSPF must include the link utilization as a criterion in the path selection. One algorithm that considers this is referred to as the “least-fill” path selection. This algorithm identifies the single link in each of the equal-cost paths that has the least available bandwidth in proportion to its maximum reservable bandwidth. CSPF then selects the path containing the link with the largest such available bandwidth to maximum reservable bandwidth percentage. The net effect of using this algorithm is that over time, LSP paths become spread over the network links in such a way that the percentage of link utilization is balanced.

When comparing the percentages of least available link bandwidth across the sorted paths, if two percentages differ by less than a value you configure as a minimum threshold, CSPF considers them equal. It then applies a random number generator to select amongst these paths. You can also specify a reoptimization threshold, which allows you include a path cost consideration into the decision of when to alter the paths used by the LSP.

LSP on-demand resynchronization

LSP on-demand resynchronization is supported on the 7750 SR and 7710 SR. You can modify the nms-server.xml file to allow a user to manually resynchronize an LSP. On-demand resynchronization does not affect the existing manual full node resynchronization functionality. However, when LSP on-demand resynchronization is enabled, any scheduled resynchronization is blocked for the following LSP objects:

- RSVP session
- cross-connect
- in-segment
- out-segment
- actual hop
- CSPF hop

Therefore, these LSP objects are not resynchronized as a result of a relevant trap. The exception is that for 5650 CPAM path monitored LSPs, the actual hop trap (a generic trap) is still processed.

By default, the LSP on-demand resynchronization functionality is disabled. See chapter 5 for information about how to enable LSP on-demand resynchronization. After you enable LSP on-demand resynchronization, click on the Resync button on the LSP configure form to start the manual LSP on-demand resynchronization. The following objects are resynchronized, depending on the type of LSP:

- for a dynamic LSP: the LSP, LSP path, CSPF and actual paths, bypass or detour path, cross-connects, in-segments, out-segments, and RSVP sessions
- for a manual bypass LSP: the LSP, LSP path, CSPF and actual paths, cross-connects, in-segments, out-segments, and RSVP sessions
- for a static LSP: the head-end LSP, the static hops, static label maps, cross-connects, in-segments, and out-segments. You must manually resynchronize all of the planned hop sites in a static LSP before creating a static LSP.

29.2 Sample MPLS configuration

Figure 29-1 shows a sample MPLS service configuration. The actual configuration depends on the specific network requirements.

Figure 29-1 Sample MPLS configuration

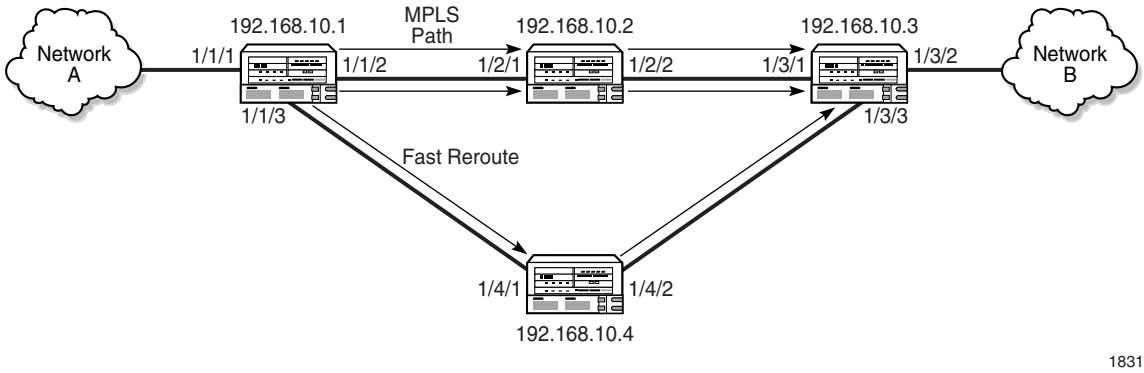


Table 29-1 describes the high-level tasks that are required to configure this sample MPLS service.

Table 29-1 Sample MPLS configuration

Task	Description
1. Verify the preconfigurations	• An IGP is enabled on all participating NEs and includes the system interface in the IS-IS or OSPF area. • Any additional Layer 3 interfaces that you wish to use are configured.
2. Create an MPLS path.	Specify 192.168.10.1 as the starting network element, and interface 1/3/2 on 192.168.10.3 as the destination site. Either of the other two NEs can be specified as hops.
3. Create a dynamic LSP.	• Specify interface 1/1/1 on 192.168.10.1 as the source IP address, and 192.168.10.3 as the destination IP address. • Bind this LSP to the MPLS path created in the previous step.
4. Create a static LSP, if required.	—
5. Configure the dynamic LSP binding to an MPLS path.	Configure options such as fast reroute and CSPF, if required.
6. Configure service tunnels as required.	See chapter 30 for more information about service tunnel configuration.

29.3 Workflow to configure MPLS

1 Enable and configure IS-IS, RIP and/or OSPF to include the system interface on all NEs that are to participate in the MPLS network.

2 Enable MPLS on the routing instances of all NEs that are to participate in the MPLS network. RSVP is enabled by default.

3 Assign Layer 3 interfaces, including the system management interface, to the MPLS instances and perform additional MPLS interface configuration as required.

4 Create a mesh of MPLS paths.

5 Create a mesh of LSPs.

Note 1 — Only static LSPs are supported on the OS 9700E and OS 9800E NEs.

Note 2 — Static FRR LSPs are supported on the OS 9700E and OS 9800E NEs.

Note 3 — RSVP is not supported on the OS 9700E and OS 9800E NEs.

Note 4 — Label actions cannot be modified on NEs after the labels are created by the 5620 SAM.

29.4 MPLS procedures

Use the following 5620 SAM procedures to manage MPLS.

Procedure 29-1 To enable MPLS on a routing instance

1 Choose Routing from the 5620 SAM navigation tree view selector.

2 Navigate to a routing instance. The path is Routing→NE→Routing Instance.

3 Right click on the routing instance and choose Properties from the contextual menu. The Routing Instance (Edit) form opens.

4 Click on the Protocols tab button.

5 Select the MPLS Enabled parameter. RSVP is enabled by default and cannot be disabled using the 5620 SAM.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Routing Instance (Edit) form closes.

The 5620 SAM creates an MPLS instance and displays it below the routing instance in the navigation tree.

Procedure 29-2 To configure an MPLS instance

Note 1 — The MPLS instance on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, must be enabled using the CLI.

Note 2 — The only parameter that you can configure on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, is the Dynamic Bypass parameter.

Note 3 — The following tab buttons are supported on the OS 9700E and OS 9800E NEs for MPLS configuration at the site level:

- General
- Interfaces
- In Segments
- Cross Connects
- Out Segments
- Static Label Maps
- Faults

1 Enable MPLS on an NE, as described in Procedure 29-1.

2 Choose Routing from the 5620 SAM navigation tree view selector.

3 Navigate to an MPLS instance. The path is Routing→NE→Routing Instance→MPLS.

4 Right-click on the MPLS icon in the navigation tree, and choose Properties from the contextual menu. The MPLS (Edit) form opens with the General tab displayed.

5 Configure the parameters.

- Administrative State
- Fast Reroute
- Dynamic Bypass
- Static LSPs Fast Retry Timer (seconds)
- In the LSP Resignal panel:
  - Enable
  - Resignal Timer (min)
- In the P2MP LSP Resignal panel:
  - Enable
  - Resignal Timer (min)
- In the Hold Timer panel:
  - Enable
  - Hold Timer (seconds)
- In the Shared Risk Link Group panel:
  - Enable SRLG for FRR
  - Strict
- In the Least-Fill panel:
  - Least Minimum Threshold
  - Least Reoptimization Threshold
- In the TTL Propagate panel:
  - Shortcut Local TTL Propagate
  - Shortcut Transit TTL Propagate
- In the Auto Bandwidth Multipliers panel:
  - Sample Multiplier
  - Adjust Multiplier

6 If you are configuring an MPLS instance on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to step 7. Otherwise, if you need to configure OAM diagnostics for the MPLS instance, click on the Tests tab button. See chapter 35 for more information about configuring OAM diagnostics.

7 To configure MPLS interfaces on the MPLS instance, click on the Interfaces tab button. See Procedure 29-3 for more information about configuring MPLS interfaces. If you are configuring an MPLS instance on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to step 14.

8 To configure the collection of ingress accounting statistics for the MPLS instance, click on the Accounting tab button.

9 Click on the Add button. The IngStatsPolicy, Routing Instance (Create) form opens.

10 Configure the parameters in the LSP Information block:

- LSP Name
- Sender Address

11 Configure the parameters in the Ingress Accounting Statistics block:

- Click on the Select button. The Select Accounting Policy - IngStatsPolicy - Routing Instance form opens. Choose the required accounting policy and click on OK. Only accounting policies with the CombinedMplsLspIngressStats stats type are available for selection.
- Collect Accounting Statistics
- Administrative State

Note — The collection of egress accounting statistics is configured in Procedure 29-8.

See the 5620 SAM Statistics Management Guide for more information on the collection of statistics.

12 Click on the following tab buttons to view information about the MPLS instance, as required.

- In Segments to view the MPLS ingress segment information, such as label assignments
- Cross Connects to vie w the LSP cross-connection information
- Out Segments to view the MPLS egress segment information, such as label assignments
- Static Label Maps to view static hop mapping information
- Statistics to view MPLS site and interface statistics
- Faults to view alarm information for the MPLS instance

13 Click on the View RSVP Site button to view the associated RSVP instance on the NE.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The MPLS (Edit) form closes.

Procedure 29-3 To create an MPLS interface

Perform this procedure to create an MPLS interface by assigning a network interface to an MPLS instance.

This procedure requires the existence of an L3 network interface on the NE that hosts the MPLS instance. See section 27.1 for more information about configuring network interfaces.

Note — The following tab buttons are supported on the OS 9700E and OS 9800E NEs for MPLS configuration at the interface level:

- General
- In Segments
- Static Label Maps
- Cross Connects
- Out Segments
- Faults

1 Choose Routing from the 5620 SAM navigation tree view selector.

2 Navigate to an MPLS instance icon. The path is Routing→NE→Routing Instance→MPLS.

3 Right-click on the MPLS icon and choose Create Interface from the contextual menu. The MPLS Interface (Create) form opens with the General tab displayed.

4 Assign an L3 network interface as the MPLS interface.

i Click on the Select button. The Select Interface form opens.

ii Choose an interface from the list and click on the OK button.The interface is displayed in the Interface panel on the MPLS Interface (Create) form.

5 Configure the parameters:

- Description
- Administrative State

If you are creating an MPLS interface on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to 7.

6 In the TE Metric block, configure the parameters:

- Enable
- TE Metric

7 Click on the Apply button. The form displays additional tabs, and the 5620 SAM creates the MPLS interface and displays it below the MPLS instance in the navigation tree.

If you are creating an MPLS interface on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to 10.

8 Configure a Shared Risk Link Group, if required.

i Click on the Shared Risk Link Groups tab button. The Shared Risk Link Group list page opens.

ii Click on the Add button. The SharedRiskLinkGroup (Path/Routing Management: MPLS) Select form opens.

iii Click on the Search button. The available SRLGs are displayed.

iv Select the required SRLGs and click OK. Up to 64 SRLGs can be associated with a specific MPLS interface. The SharedRiskLinkGroup (Path/Routing Management: MPLS) Select form closes and the selected SRLG is displayed in the Shared Risk Link Group list page.

9 Configure a static label map, if required. A static label map is required when there are intervening unmanaged NEs between the managed NEs in an MPLS path.

Note — Alcatel-Lucent recommends that you use a static label mapping only to specify unmanaged NEs.

i Click on the Static Label Maps tab button.

ii Click on the Add button. The Static Label Map (Create) form opens. Alternatively, you can choose a Static Label Map from the list and click on the Properties button to edit the Static Label Map properties.

iii Configure the Label Action parameter. When you change the Label Action parameter from unspecified to Pop or Swap, the Static Label Map (Create) form changes to include other parameters. Configure the other parameters as required:

- Ingress Label
- Egress Label
- Egress Label Protect Swap
- Enable Implicit Null Label
- Next Hop
- Next Hop Protect Swap
- Administrative State

The Egress Label, Next Hop and Enable Implicit Null Label parameters are only configurable when the Label Action parameter value is set to Swap.

The Egress Label Protect Swap and Next Hop Protect Swap parameters are configurable only when the Label Action parameter value is set to Swap/Protect-Swap.

The 5620 SAM sets the Label Action parameter value to Pop when the hop destination matches the destination LSP.

iv Click on the OK button. A dialog box appears.

v Click on the OK button.

10 Click on the Administrative Groups tab button to assign MPLS administrative groups to the interface, as required. After you assign administrative groups to an MPLS interface, the total value of the groups is displayed in a bit mask format by the Groups Included (bitmask) indicator on the General tab.

11 Click on the following tab buttons to view information about the MPLS interface, as required.

- In Segments to view the MPLS ingress segment information, such as label assignments
- Cross Connects to vie w the LSP cross-connection information
- Out Segments to view the MPLS egress segment information, such as label assignments
- Statistics to view the MPLS site and interface statistics
- Faults to view alarm information for the MPLS interface

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The MPLS Interface properties form closes.

Procedure 29-4 To create an MPLS path

1 Choose Manage→MPLS→MPLS Paths from the 5620 SAM main menu. The Manage MPLS Paths form opens.

2 Click on the Create button. The Create MPLS Path form opens with the Name the MPLS Path step displayed.

3 Configure the parameters.

- Name
- Description

4 Click on the Next button. The Define Source Site step displayed.

5 Perform one of the following actions to specify a 5620 SAM-managed NE for the Starting Network Element parameter value.

a Choose an NE from a list.

i Click on the Select button. The Select a Network Element - Select Source Site form opens.

ii Select an NE in the list and click on the OK button. The management IP address of the NE is displayed as the source site of the MPLS path.

b Enter the management IP address of the port.

6 Click on the Next button. The Define the provisioned Path step is displayed.

7 Click on the Insert Hop button to insert an MPLS path hop. The Hop for New MPLS Path (Create) form opens.

8 Configure the Specify Site parameter. Perform one of the following actions.

a Specify the IP address of an unmanaged NE.

i Choose Manually.

ii Configure the IP Address parameter.

b Select a managed NE.

i Choose By Selection.

ii Click on the Select button. The Select a Network Element - New MPLS Path form opens.

iii Select an NE in the list and click on the OK button. The management IP address of the NE is displayed as the Network Element and IP Address values.

iv Specify an alternative interface on the NE to be used as the hop point, if required, by manually configuring the IP Address parameter.

9 Configure the Hop Type parameter.

Note — The Hop Type parameter is set to a value of strict and is not configurable for any of the hops on a path that originate from or terminate on a 7250 SAS-ES 2.0.

10 Click on the Apply button.

11 Insert an additional hop, if required, by repeating steps 8 to 10.

12 Click on the OK button. The Create MPLS Path form reappears.

13 To change the hop sequence, choose a hop and click the Move Up or Move Down button. The first hop in the list is the first hop, and the last hop in the list becomes the destination site when the form changes are saved.

14 Click on the Next button. The Set Initial State step is displayed.

15 Configure the Administrative parameter. This parameter is set to Up and is not configurable if the path originates on 7250 SAS-ES or 7250 SAS-ESA NEs.

16 Click on the Finish Button to save the configuration. You are prompted to view the MPLS path.

17 Enable the View the newly created MPLS path parameter to view the MPLS path configuration after closing the form, if required.

18 Click on the Close button. The Create MPLS Path form closes.

19 If the View the newly created MPLS path parameter in step 16 is enabled, the MPLS Path (Edit) form opens with the newly created MPLS path configuration displayed.

i View the configuration, if required.

ii Close the MPLS Path (Edit) form.

20 Close the Manage MPLS Paths form.

Procedure 29-5 To view an MPLS path

1 Choose Manage→MPLS→MPLS Paths from the 5620 SAM main menu. The Manage MPLS Paths form opens.

2 Configure the filter criteria. A list of MPLS paths is displayed.

3 View the MPLS path information as required. The information includes the following:

- name and description
- ID
- source and destination sites
- administrative and operational states

Procedure 29-6 To create a static LSP

Note — When LSP on-demand resynchronization is enabled, manually resynchronize all of the planned hops in the static LSP before you create a static LSP. This is to ensure that validations on the static LSP can be run properly. See chapter 5 for information about enabling LSP on-demand resynchronization.

1 Choose Manage→MPLS→Static LSPs from the 5620 SAM main menu. The Manage Static LSPs form opens.

2 Click on the Create button. The Static LSP (Create) form opens.

3 Configure the parameters:

- Name
- Description
- ID
- Auto-Assign ID
- Source Site ID
- Egress Label
- Enable Implicit Null Label
- Next Hop
- Administrative
- Destination Site ID

Note 1 — If a range policy is applied to a service tunnel, a grey text box appears beside the Service ID parameter to indicate that a range policy is in effect.

If a format policy is applied to a service tunnel, a combo box appears beside the object field during object creation, to indicate that a format policy is enforced. When there is only one matching policy, the combo box is greyed out. When there are multiple matching policies the combo box is used to select a policy. The items in the combo box are ordered by the policy's Priority Value parameter.

Note 2 — The Administrative parameter applies to the source NE only, not to the entire static LSP

4 Click on the Static Hops tab button.

5 Click on the Add button. The Static Hop (Create) form opens.

6 Configure the Hop Index parameter.

7 Click on the Select button in the Site panel to configure the Site ID parameter. The Select Site - Static Hop form opens with a list of the available hop sites.

8 Select a site in the list and click on the OK button. The Select Site - Static Hop form closes and the Static Hop (Create) form displays the site information.

9 Click on the Select button in the Interface panel to configure the Interface Name parameter. The Select Interface - Static Hop form opens with a list of the available interfaces on the hop site.

10 Select an interface in the list and click on the OK button. The Select Interface - Static Hop form closes and the Static Hop (Create) form displays the interface name.

11 Configure the parameters.

- Label Action
- Ingress Label
- Egress Label
- Egress Label Protect Swap
- Enable Implicit Null Label
- Next Hop
- Next Hop Protect Swap
- Administrative State

The Egress Label, Enable Implicit Null Label and Next Hop parameters are configurable when the Label Action parameter value is set to Swap.

The Egress Label Protect Swap and Next Hop Protect Swap parameters are configurable only when the Label Action parameter value is set to Swap/Protect-Swap.

12 Click on the OK button. The Static Hop (Create) form closes and a dialog box appears.

13 Click on the OK button. Static LSP (Create) form reappears.

14 Insert an additional hop, if required, by repeating steps 5 and 13.

15 Click on the OK button. The Static LSP (Create) form closes and a dialog box appears.

16 Click on the Yes button. The Static LSP (Create) form closes and the Manage Static LSPs form reappears.

17 Close the Manage Static LSPs form.

Procedure 29-7 To view and configure a static LSP

The following procedure applies only to the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7450 ESS, 7750 SR, and 7710 SR. See the device documentation for related information specific to the 7250 SAS-ES and 7250 SAS-ESA if required.

1 Choose Manage→MPLS→Static LSPs from the 5620 SAM main menu. The Manage Static LSPs form opens.

2 Configure the filter criteria and click on the Search button. A list of static LSPs is displayed.

3 Select an LSP in the list and click on the Properties button. The Static LSP (Edit) form opens.

4 Click on the following tab buttons to view information about the static LSP, as required.

- Static Hops to view and configure LSP hops
- Service Tunnels to view a list of service tunnels associated with the static LSP
- LDP Tunneling to view a list of LDP-over-RSVP tunnels associated with the static LSP
- Statistics to view the static LSP site and interface statistics
- Faults to view alarm information for the static LSP

5 Close the Static LSP (Edit) form.

6 Close the Manage Static LSPs form.

Procedure 29-8 To create a Dynamic LSP

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Click on the Create button. The Create Dynamic LSP form opens with the Identification step displayed.

3 Configure the parameters.

- Name
- Description
- ID
- Auto-Assign ID
- Preference

Note — When a range policy is applied to a dynamic LSP, a dimmed text field appears beside the Service ID parameter to indicate that a range policy is in effect.

If a format policy is applied to a dynamic LSP, a combo box appears beside the object field during object creation, to indicate that a format policy is in effect. When there is only one matching policy, the combo box is greyed out. When there are multiple matching policies the combo box is used to select a policy. The sequence of the options in the combo box are specified by the policy Priority Value parameter.

4 Click on the Next button. The Define Source and Destination Sites step is displayed.

5 Specify the source and destination sites for the dynamic LSP.

Note — You can also manually specify an IP address for each parameter in this step.

i Click on the Source Site ID parameter Select button. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

ii Select a site in the list and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the source site information, which includes the Source IP Address parameter value. This parameter is automatically populated with the system IP address of the site.

iii Click on the Destination Site ID parameter Select button. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

iv Select a site in the list and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the destination site information. The displayed destination interface is the system interface because an LSP can terminate only on a system interface.

6 Click on the Next button. The Auto Select Hop-Less MPLS Path form opens.

7 Configure the parameters.

- Auto Select Hop-less Path
- Reserved Bandwidth.

The Reserved Bandwidth. parameter is configurable when the Auto Select Hop-less Path parameter is enabled.

8 If the Auto Select Hop-less Path parameter in step 7 is enabled, go to step 10.

9 Click on the Next button. The Add MPLS Paths form opens. This step binds the LSP to the MPLS path to create an MPLS path.

i Configure the Path Destination Matching parameter.

ii Click on the Add button. The LSP-Path Binding form opens with the Choose Path Type step displayed.

iii Configure the Type parameter.

iv Click on the Next button. The Choose MPLS Path step is displayed. Select an MPLS path in the list to associate with the LSP. You can also create an MPLS path by clicking on the Create MPLS Path button. See Procedure 29-4 for more information.

v Click on the Next button. The Set Traffic Options form opens.

vi Configure the parameters.

- Reserved Bandwidth (Mbps)
- Inherit Value
- Hop Limit
- Record Actual Path
- Path Preference

The Path Preference is only configurable on Standby LSP paths (Type parameter set to standby).

vii Click on the Next button. The Set Initial States form opens.

viii Configure the Administrative parameter.

ix Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

x Click on the OK button. The Create Dynamic LSP form reappears.

10 Click on the Next button. The Properties - Traffic Engineering and Protection step is displayed.

11 Configure the parameters.

- Fast Reroute
- Hop Limit
- IGP Shortcut Enabled
- Diff-Serv Class Type
- Main Class Type Retry Limit

12 Click on the Next button. The Properties - Fast Reroute step is displayed.

13 Configure the parameters:

- Backup Type
- Hop Limit
- Reserved Bandwidth (Mbps)
- Node Protect

14 Click on the Next button. The Properties - Signalling step is displayed.

15 Configure the parameters.

- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP

16 Click on the Next button. The Properties - Make before Break step is displayed.

17 Configure the Make Before Break parameter.

18 Click on the Next button. The Properties - CSPF form opens.

19 In the CSPF block, configure the parameters:

- Enable CSPF
- Enable TE Metric

20 Click on the Next button. The Properties - Route Selection step is displayed.

21 Configure the parameters:

- Metric
- Least-Fill Path Selection

The Least-Fill Path Selection parameter can only be enabled when the Enable CSPF parameter is enabled in step 19.

22 Click on the Next button. The Properties - Administrative Groups step is displayed.

23 Assign one or more MPLS administrative groups to the dynamic LSP.

i Select the required MPLS administrative groups in the Unassigned list.

ii Click on the right arrow button. The groups are assigned to the dynamic LSP and moved to the Assigned list.

After you assign administrative groups to an MPLS interface, the total value of the groups is displayed in a bit mask format by the Groups Included (bitmask) indicator on the General tab.

24 Click on the Next button. The Properties - LDP Tunneling step is displayed.

25 Configure the LDP over RSVP include parameter.

26 Click on the Next button. The Properties - Auto-Bind step is displayed.

27 Configure the Enable Auto-Bind parameter.

Note — The Enable Auto-Bind parameter is configurable only on a Release 7.0 or later 7710 SR or 7750 SR.

28 Click on the Next button. The Set Initial State step is displayed.

29 Configure the Administrative parameter.

30 Click on the Finish button. The 5620 SAM prompts you to view the dynamic LSP.

31 Enable the View the newly created Dynamic Lsp parameter to view the dynamic LSP configuration after closing the form, if required.

Note — If you enable the View the newly created Dynamic Lsp parameter you can configure the collection of egress accounting statistics using the dynamic LSP configuration form.

32 Click on the Close button. The Create Dynamic LSP form closes.

33 If the View the newly created Dynamic Lsp parameter is enabled in step 31, the Dynamic LSP (Edit) form opens with the newly created dynamic LSP configuration displayed.

i View the configuration, if required.

ii If you need to enable the collection of egress accounting statistics, go to step iv. Otherwise go to step ix.

iii If you need to configure auto-bandwidth for the dynamic LSP, go to step vi. Otherwise, go to step ix.

iv Click on the Accounting tab button.

v Configure the parameters in the Egress Accounting Statistics panel:

- Click on the Select button. The Select Accounting Policy - Dynamic LSP form opens. Choose the required accounting policy and click on the OK button. Only accounting policies with the CombinedMplsLspEgressStats stats type are available for selection.
- Collect Accounting Statistics
- Administrative State

Note 1 — The Ingress Accounting Statistics panel displays a read-only view. If an ingress accounting statistics record exists, you can click on the Properties button to view the record.

Note 2 — The collection of ingress accounting statistics is configured in Procedure 29-2.

See the 5620 SAM Statistics Management Guide for more information on about the collection of statistics.

vi Click on the Properties tab button.

vii Set the Auto Bandwidth parameter in the Traffic Engineering And Protection panel to true to view and configure the auto-bandwidth parameters.

viii Configure the parameters in the Auto Bandwidth panel.

- Adjust Up Threshold (percent)
- Adjust Down Threshold (percent)
- Minimum Bandwidth (mbps)
- Monitor Bandwidth
- Sample Multiplier
- Overflow Limit
- Adjust Up Bandwidth (mbps)
- Adjust Down Bandwidth (mbps)
- Maximum Bandwidth (mbps)
- Adjust Multiplier
- Overflow Limit Threshold (percent)
- Overflow Limit Bandwidth (mbps)

ix Click on OK to close the Dynamic LSP (Edit) form.

34 Click on OK to close the Manage Dynamic LSPs form.

Procedure 29-9 To create a dynamic LSP from a tunnel template

Before you can create an LSP from a tunnel template, you must create the tunnel template. You can use an existing LSP to create a tunnel template. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Click on the Create from Template button. A Create Dynamic LSP from Template window opens with a list of tunnel templates.

3 Choose a template from the list.

4 Click on the OK button. A Create Dynamic LSP from Template form opens.

5 Configure the parameters.

- Name
- Description
- ID
- Auto-Assign ID
- Preference
- Administrative

6 Specify the source sites for the dynamic LSP.

i Click on the Select button beside the Source Site ID parameter. The Select Network Element form opens with a list of the available sites.

ii Choose a site from the list and click on the OK button. The Select a Network Element form closes and the Create Dynamic LSP from Template form displays the source site information.

iii Click on the Select button beside the Source IP Address parameter. The Select Network Element form opens with a list of the available sites.

iv Choose a site from the list and click on the Ok button. The Select a Network Element form closes and the Create Dynamic LSP from Template form displays the source IP address information.

7 Configure the Destination Site ID and the Destination IP Address parameters.

8 Configure the Show created object parameter.

9 Click on the Accounting tab button.

10 Click on the Select button beside the Accounting Policy parameter. A Select Policy window opens.

11 Choose a policy from the list.

12 Click on the OK button.

13 Configure the Collect Accounting Statistics and the Administrative State parameters.

14 Click on the Properties tab button.

15 Configure the parameters:

Note — The number of parameters that can be configured depends on how the template was created. All of the following parameters are configurable when the template is based on an object. A subset of the following parameters can be configured when the template is based on an object class.

- Guarding LSP
- Guarded Destination
- Fast Reroute
- Hop Limit
- Diff-Serv Class Type
- Backup Type
- Hop Limit
- Reserved Bandwidth (Mbps)
- Node Protect
- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP
- Make Before Break
- Enable CSPF
- Enable TE Metric
- Metric
- Least-Filled Path Selection
- Groups Included (bitmap)
- Groups Excluded (bitmap)
- Persistent
- Permit Merge
- Record Actual Route
- Record Label
- Committed Rate
- Peak Rate
- Setup Priority
- Hold Priority
- Backup Setup Priority
- Backup Hold Priority
- LDP over RSVP include
- Enable Auto-Bind

16 Click on the OK button. When the LSP configuration is successful, the Create Dynamic LSP from Template form closes and the Dynamic LSP (Edit) form reappears.

If the LSP configuration is unsuccessful, the Create Dynamic LSP from Template form remains open and an error message appears.

17 Close the Manage Dynamic LSPs form.

Procedure 29-10 To create a 7250 SAS-ES or 7250 SAS-ESA guarding LSP

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form appears.

2 Click on the Create button. The Create Dynamic LSP form opens with the Identification step displayed.

3 Configure the parameters:

- Name
- Description
- ID
- Auto-Assign ID
- Preference

4 Click on the Next button. The Define Source and Destination Sites step is displayed.

5 Specify the source and destination sites for the dynamic LSP.

Note — You can also specify an IP address for each parameter in this step.

i Click on the Select button beside the Source Site ID parameter. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

ii Choose a site in the list and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the source site information, which includes the Source IP Address parameter. The parameter is automatically configured with the system IP address of the site.

iii Click on the Select button beside the Destination Site ID parameter. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

iv Choose a destination site and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the destination site information. The displayed destination interface is the system interface and cannot be changed.

6 Click on the Next button. The Guarding LSP step is displayed.

7 Enable the Guarding Lsp parameter.

8 Configure the Guarded Destination parameter.

9 Click on the Next button. The Add MPLS Paths step is displayed.

i Configure the Path Destination Matching parameter.

ii Click on the Add button. The LSP-Path Binding form opens with the Choose Path Type step displayed. The Type parameter is set to primary and cannot be configured.

iii Click on the Next button. The Choose MPLS Path step is displayed. Choose an MPLS path to associate with the LSP. If required, create an MPLS path by clicking on the Create MPLS Path button. See Procedure 29-4 for more information.

iv If the guarding LSP originates on a 7250 SAS-ES or 7250 SAS-ESA, Release 2.0, go to step 9ix.

v Click on the Next button.The Set Traffic Engineering Parameters step is displayed.

vi Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Path
- Record Label

vii Click on the Next button. The Set Path Parameters step is displayed.

viii Configure the parameters:

- Enable CSPF
- Setup Priority
- Hold Priority

ix Click on the Next button. The Set Initial State form is displayed.

x Configure the Administrative parameter. If the LSP originates on a 7250 SAS-ES or 7250 SAS-ESA, Release 2.0, the Administrative parameter cannot be configured.

xi Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

xii Click on the OK button.

10 If the guarding LSP originates on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to step 14, click on the Next button. The Properties - Session Attributes step is displayed.

11 Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Route
- Record Label

12 Click on the Next button. The Properties - Path Parameters step is displayed.

13 Configure the parameters:

- Committed Rate
- Setup Priority
- Backup Setup Priority
- Peak Rate
- Hold Priority
- Backup Hold Priority

14 Click on the Next button. The Set Initial State step is displayed.

15 Configure the Administrative parameter. The Administrative parameter is set to Up and cannot be configured if the guarding LSP originates on a 3.0 NE.

16 Click on the Finish button. The 5620 SAM prompts you to view the dynamic LSP.

17 Enable the View the newly created Dynamic Lsp parameter to view the dynamic LSP, if required. Otherwise, go to step 19.

18 When the View the newly created Dynamic Lsp parameter is enabled, the Dynamic LSP (Edit) form appears with the newly created dynamic LSP configuration displayed.

i View the configuration.

ii Close the Dynamic LSP (Edit) form and go to step 20.

19 Click on the Close button. The Create Dynamic LSP form closes.

20 Close the Manage Dynamic LSPs form.

Procedure 29-11 To create a 7250 SAS-ES or 7250 SAS-ESA dynamic LSP

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form appears.

2 Click on the Create button. The Create Dynamic LSP form opens with the Identification step displayed.

3 Configure the parameters:

- Name
- Description
- ID
- Auto-Assign ID
- Preference

4 Click on the Next button. The Define Source and Destination Sites step is displayed.

5 Specify the source and destination sites for the dynamic LSP.

Note — You can also specify an IP address for each parameter in this step.

i Click on the Select button beside the Source Site ID parameter. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

ii Choose a site in the list and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the source site information, which includes the Source IP Address parameter. The parameter is automatically configured with the system IP address of the site.

iii Click on the Select button beside the Destination Site ID parameter. The Select a Network Element - Create Dynamic LSP form opens with a list of the available sites.

iv Choose a destination site and click on the OK button. The Select a Network Element - Create Dynamic LSP form closes and the Create Dynamic LSP form displays the destination site information. The displayed destination interface is the system interface because an LSP can terminate only on a system interface.

6 Click on the Next button. The Guarding LSP step is displayed.

7 Click on the Next button. The Add MPLS Paths... step is displayed.

8 Configure the Path Destination Matching parameter.

9 Click on the Add button. The LSP-Path Binding form opens with the Choose Path Type step displayed. You cannot configure the Type parameter, the value is set to primary.

10 Click on the Next button. The Choose MPLS Path step is displayed. Choose an MPLS path to associate with the LSP. If required, create an MPLS path by clicking on the Create MPLS Path button. See Procedure 29-4 for more information.

11 If the LSP originates on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, go to step 25.

12 Click on the Next button. The Set Initial State step is displayed.

13 Configure the Administrative parameter. The Administrative parameter is set to Up and cannot be configured.

14 Click on the Finish button. The LSP-Path Binding closes and a dialog box appears.

15 Click on the Yes button. The Create Dynamic LSP form is displayed.

16 Click on the Next button. The Properties - Traffic Engineering and Protection step is displayed.

17 Configure the Fast Reroute parameter. If you selected False, go to step 20.

18 Click the Next button. The Properties - step is displayed.

19 Configure the Hop Limit parameter. The Backup Type parameter is displayed but is not configurable.

20 Click on the Next button. The Properties - Session Attributes step is displayed.

21 Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Route
- Record Label

These parameters are read-only when the LSP originates from a 7250 SAS-ES or 7250 SAS-ESA, Release 2.0, and the Fast Reroute parameter is True.

22 Click on the Next button. The Properties - Path Parameters step is displayed.

23 Configure the parameters:

- Committed Rate
- Setup Priority
- Backup Setup Priority
- Hold Priority
- Peak Rate
- Backup Hold Priority

24 Go to step 48.

25 Click on the Next button. The Set Fast Reroute step opens.

26 Configure the Fast Reroute parameter. If you selected False, go to step 29.

27 Click on the Next button. The Set Fast Reroute Backup Properties step is displayed.

28 Configure the parameters:

- Fast Reroute Hop Limit
- Backup Setup Priority
- Backup Hold Priority

The Fast Reroute Backup Type parameter is displayed, but is not configurable.

29 Click on the Next button. The Set Traffic Engineering Parameters step is displayed.

30 Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Path
- Record Label

The parameters are read-only when the Fast Reroute parameter is True.

31 Click on the Next button. The Set Path Parameters step is displayed.

32 Configure the parameters:

- Enable CSPF
- Setup Priority
- Hold Priority

33 Click on the Next button. The Set Initial States step is displayed.

34 Configure the Administrative parameter.

35 Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

36 Click on the OK button.

37 If you do not need to add a secondary LSP path, go to step 48.

38 Click on the Add button. The LSP-Path Binding opens and the Choose Path Type step is displayed. The Type parameter is set to secondary if a primary path exists.

39 Click on the Next button. The Choose MPLS Path step is displayed. Choose an MPLS path to associate with the LSP. If required, create an MPLS path by clicking on the Create MPLS Path button. See Procedure 29-4 for more information.

40 Click on the Next button. The Set Traffic Engineering Parameters step is displayed.

41 Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Path
- Record Label

42 Click on the Next button. The Set Path Parameters step is displayed.

43 Configure the parameters:

- Enable CSPF
- Setup Priority
- Hold Priority

44 Click on the Next button. The Set Initial State step opens.

45 Configure the Administrative parameter.

46 Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

47 Click on the OK button.

48 Click on the Next button. The Set Initial State step opens.

49 Configure the Administrative parameter. The Administrative parameter is Up and you cannot configure the value if the LSP originates on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0.

50 Click on the Finish button. The 5620 SAM prompts you to view the dynamic LSP.

51 Enable the View the newly created Dynamic Lsp parameter to view the dynamic LSP configuration, if required. Otherwise, go to step 53.

52 When the View the newly created Dynamic Lsp parameter is enabled, the Dynamic LSP (Edit) form appears with the newly created dynamic LSP configuration displayed.

i View the configuration.

ii Close the Dynamic LSP (Edit) form, and go to step 54.

53 Click on the Close button. The Create Dynamic LSP form closes.

54 Close the Manage Dynamic LSPs form.

Procedure 29-12 To configure a 7250 SAS-ES or 7250 SAS-ESA LSP

Perform the following procedure to configure an LSP that originates on a 7250 SAS-ES or 7250 SAS-ESA.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Configure the filter criteria and click on the Search button. A list of dynamic LSPs is displayed.

3 Choose an LSP in the list and click the on Properties button. The Dynamic LSP (Edit) form opens with the General tab displayed.

4 Click on the LSP-Path Bindings tab button. A list of LSP paths is displayed.

5 You can add a secondary LSP path on a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, if required. Otherwise, go to step 15.

6 Click on the Add button. The LSP-Path Binding opens and the Choose Path Type step is displayed. The Type parameter is set to secondary if a primary path exists.

7 Click on the Next button. The Choose MPLS Path step is displayed. Choose an MPLS path to associate with the LSP. You can also create an MPLS path by clicking on the Create MPLS Path button. See Procedure 29-4 for more information.

8 Click on the Next button. The Set Traffic Engineering Parameters step is displayed.

9 Configure the parameters:

- Persistent
- Permit Merge
- Record Actual Path
- Record Label

10 Click on the Next button. The Set Path Parameters step is displayed.

11 Configure the parameters:

- Enable CSPF
- Setup Priority
- Hold Priority

12 Click on the Next button. The Set Initial States step opens.

13 Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

14 Click on the OK button.

15 Choose an LSP path in the list and click on the Properties button. The LSP-Path Binding (Edit) form opens with the General tab displayed.

16 Configure the parameters.

- Type
- Administrative
- Setup Priority
- Hold Priority
- Fast Reroute
- Backup Type
- Hop Limit
- Record Actual Path
- Record Label
- Persistent
- Permit Merge
- Backup Setup Priority
- Backup Hold Priority
- Enable CSPF

The configurable parameters depend on:

- the type of LSP path
- the software version of the originating NE
- whether fast reroute is enabled

17 Click on the Administrative Groups tab button.

18 Assign an MPLS administrative group to the LSP path.

i Choose an MPLS administrative group in the Unassigned list.

ii Click on the right arrow button. The group is assigned to the LSP path and moves to the Assigned list.

19 View a list of hops or an LSP topology map, if required.

i Click on the following tab buttons to list the path hops or to view a topology map of the hops:

- Provisioned Path
- Actual Path

ii Click on the Topology View button to view the topology map for the path. See chapter 4 for information about using topology maps.

20 Click on the OK button. The LSP-Path Binding (Edit) form closes.

21 Click on the OK button. The Dynamic LSP (Edit) form closes.

Procedure 29-13 To list dynamic LSPs

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Configure the filter criteria. A list of dynamic LSPs is displayed.

3 Select an LSP in the list and click on the Properties button. The Dynamic LSP (Edit) form opens.

4 To view LSP path information:

i Click on the LSP Paths tab button.

ii Double-click on an LSP path in the list.

iii Review the state information.

LSP path information includes whether the bypass tunnel for the LSP is active, or whether the LSP is in a fast reroute state.

Procedure 29-14 To create a Point-to-Multipoint LSP

1 Choose Manage→MPLS→Point-to-Multipoint LSPs from the 5620 SAM main menu. The Manage Point-to-Multipoint LSPs form opens.

2 Click on the Create button. The P2MP LSP (Create) form opens with the General tab displayed.

3 Configure the parameters.

- Name
- ID
- Auto-Assign ID
- P2MPid
- Administrative
- System ID (Loopback IP Address)
- IP Address

When you configure the System ID (Loopback IP Address) parameter, the Management IP Address and Site Name parameters are automatically populated with the values associated with that node. The IP Address parameter is also automatically populated, however, you can specify a new value for the parameter, if required.

4 Click on the Properties tab.

5 Configure the following parameters in the Traffic Engineering and Protection panel.

- Fast Reroute
- Hop Limit
- Diff-Serv Class Type

6 Configure the following parameters in the Fast Reroute panel.

- Backup Type
- Hop Limit
- Reserved Bandwidth (Mbps)
- Node Protect

The Node Protect parameter is only configurable when the Reserved Bandwidth (Mbps) parameter is set to a value greater than 0.

7 Configure the Make Before Break parameter.

8 Configure the following parameters in the CSPF panel.

- Enable CSPF
- Enable TE Metric

9 Configure the following parameters in the Signalling panel.

- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP

10 Click on the P2MP Primary Instance tab.

11 Click the Add button. The P2MP Instance (Create) form opens on the General tab.

12 Configure the parameters.

- Name
- ID
- Auto-Assign ID
- Administrative

13 Click on the Properties tab.

14 Configure the following parameters in the Traffic Engineering Properties panel.

- Reserved Bandwidth (Mbps)
- Hop Limit
- Inherit Value
- Record Actual Path
- Record Label

When you enable the Inherit Value parameter, the Hop Limit parameter for the P2MP Instance is set to the same value as you configured for the parent P2MP LSP.

15 Configure the following parameters in the Make Before Break panel.

- Make Before Break
- Inherit Value
- Resignal

When you enable the Inherit Value parameter, the Make Before Break parameter for the P2MP instance is set to the same value as you configured for the parent P2MP LSP.

16 Configure the following parameters in the Administrative Groups panel.

- Inherit Value (for Groups Included)
- Inherit Value (for Groups Excluded)

When you enable the Inherit Value parameters, the Included and/or Excluded Groups for the P2MP instance are set to the same values you configure for the parent P2MP LSP. If you do not enable the Inherit Value parameters, you can configure the Included Groups and Excluded Groups for the P2MP Instance independently from the parent P2MP LSP. (See step 21.)

17 Click on the S2L Paths tab.

18 Click the Add button. The S2L Path (Create) form opens. Each S2L Path object represents a root-to-leaf (S2L) sub-LSP path for the primary instance of the P2MP LSP.

19 Configure the parameters.

- Name
- ID
- Destination Site ID
- Administrative

20 Repeat steps 18 and 19 to configure another S2L Path, if required.

21 Click on the Administrative Groups tab.

22 Assign one or more MPLS administrative groups to the P2MP Instance.

i Choose the required Included Groups in the Unassigned list.

ii Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.

iii Select the required Excluded Groups in the Unassigned list.

iv Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.

After you assign the Included and Excluded Groups, the total value of the groups is displayed in a bit mask format by the Groups Included and Groups Excluded indicators on the P2MP Instance Properties tab.

23 Click on the OK button. The P2MP Instance (Create) form closes.

24 Click on the S2L Paths tab in the main P2MP LSP (Create) form.

25 Click on the Search button to populate the table. The S2L Paths you configured in step 18 appears. You can select an entry from the list and click on Properties to edit it, if required.

26 Click on the Administrative Groups tab in the main P2MP LSP (Create) form.

27 Assign one or more MPLS administrative groups to the P2MP LSP.

i Select the required Included Groups in the Unassigned list.

ii Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and move to the Assigned list.

iii Select the required Excluded Groups in the Unassigned list.

iv Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and move to the Assigned list.

After you assign the Included and Excluded Groups, the total value of the groups is displayed in a bit mask format by the Groups Included (bitmap) and Groups Excluded (bitmap) indicators on the P2MP LSP Properties tab.

28 Click OK to close the P2MP LSP (Create) form.

29 Close the Manage Point-to-Multipoint LSPs form.

30 To complete the configuration of the Point-to-Multipoint LSP, you must:

a Configure the required PIM tunnel interfaces. See Procedure 27-1.

b Configure tunnel interfaces on the required IGMP routing instance. See Procedure 28-36.

c Configure tunnel interfaces on the required multicast info policy. See Procedure 46-4 for more information.

31 After you complete the configuration of the Point-to-Multipoint LSP, you can reopen the P2MP LSP form to create, configure and run OAM diagnostics, if required.

i Click on the Tests tab button. The Test Suite, P2MP Ping, and P2MP Trace tabs are displayed.

ii Create or search for the test suite or particular type of test you want to run from the tab pages. Click on either the Create or Search buttons as required.

iii Click the Execute button to run a selected test.

Refer to chapters 35 and 75 for more information about configuring OAM diagnostics.

Procedure 29-15 To create a Manual Bypass LSP

1 Choose Manage→MPLS→Manual Bypass LSPs from the 5620 SAM main menu. The Manage Manual Bypass LSPs form appears.

2 Click on the Create button. The Create Bypass-only LSP form opens with the Identification step displayed.

3 Configure the parameters.

- Name
- Description
- ID
- Auto-Assign ID

4 Click on the Next button. The Define Source and Destination Sites step is displayed.

5 Specify the source and destination sites for the manual bypass LSP.

Note — You can also manually specify an IP address for each parameter in this step.

i Click on the Source Site ID parameter Select button. The Select a Network Element - Create Bypass-only LSP form opens with a list of the available sites.

ii Select a site in the list and click on the OK button. The Select a Network Element - Create Bypass-only LSP form closes and the Create Bypass-only LSP form displays the source site information, which includes the Source IP Address parameter value. This parameter is automatically populated with the system IP address of the site.

iii Click on the Destination Site ID parameter Select button. The Select a Network Element - Create Bypass-only LSP form opens with a list of the available sites.

iv Select a site in the list and click on the OK button. The Select a Network Element - Create Bypass-only LSP form closes and the Create Bypass-only LSP form displays the destination site information. The displayed destination interface is the system interface because an LSP can terminate only on a system interface.

6 Click on the Next button. The Auto Select Hop-Less MPLS Path form opens.

7 Configure the Auto Select Hop-less Path parameter.

8 If the Auto Select Hop-less Path parameter in step 7 is enabled, go to step 10.

9 Click on the Next button. The LSP-Path Binding opens, with the Choose MPLS Path step displayed.

i Select an MPLS path in the list to associate with the LSP. You can also create an MPLS path by clicking on the Create MPLS Path button. See Procedure 29-4 for more information.

ii Click on the Next button. The Set Traffic Options step is displayed.

iii Configure the parameters.

- Hop Limit
- Inherit Value
- Record Actual Path

iv Click on the Next button. The Set Initial States step is displayed.

v Configure the Administrative parameter.

vi Click on the Finish button. The LSP-Path Binding form closes and a dialog box appears.

vii Click on the OK button. The Create Bypass-only LSP form reappears.

10 Click on the Next button. The Properties step is displayed.

11 Configure the Hop Limit parameter in the Traffic Engineering And Protection block.

12 Configure the Make Before Break parameter.

13 In the CSPF block, configure the parameters:

- Enable CSPF
- Enable TE Metric

14 Configure the following parameters in the Signalling block:

- Retry Timer (seconds)
- Retry Limit
- RSVP Reserve Style
- Include ADSPEC in RSVP

15 Click on the Next button. The Admin Groups step is displayed.

16 Assign one or more included MPLS administrative groups to the bypass-only LSP.

i Select the required MPLS administrative groups in the Included Groups - Unassigned list.

ii Click on the right arrow button. The groups are assigned to the bypass-only LSP and move to the Assigned list.

Note — When you assign included administrative groups to an MPLS interface, the assigned groups are displayed in bit mask form by the Groups Included (bitmask) indicator on the General tab.

17 Assign one or more excluded MPLS administrative groups to the bypass-only LSP, if required.

i Select the required MPLS administrative groups in the Excluded Groups - Unassigned list.

ii Click on the right arrow button. The groups are assigned to the bypass-only LSP and move to the Assigned list.

Note — When you assign excluded administrative groups to an MPLS interface, the assigned groups are displayed in bit mask form by the Groups Excluded (bitmask) indicator on the General tab.

18 Click on the Next button. The Set Initial State step is displayed.

19 Configure the Administrative parameter.

20 Click on the Finish button. The 5620 SAM prompts you to view the bypass-only LSP.

21 Enable the View the newly created Bypass Only Lsp parameter to view the bypass-only LSP configuration after closing the form, if required.

22 Click on the Close button. The Create Bypass-only LSP form closes.

23 If the View the newly created Bypass Only Lsp parameter in step 21 is enabled, the Bypass-only LSP (Edit) form opens with the newly created bypass-only LSP configuration displayed.

i View the configuration, if required.

ii Close the Bypass-only LSP (Edit) form.

24 Close the Manage Manual Bypass LSPs form.

Procedure 29-16 To view and configure a Manual Bypass LSP

1 Choose Manage→MPLS→Manual Bypass LSPs from the 5620 SAM main menu. The Manage Manual Bypass LSPs form opens.

2 Configure the filter criteria and click on the Search button. A list of Bypass-only LSPs is displayed.

3 Select an LSP in the list and click on the Properties button. The Bypass-only LSP (Edit) form opens with the General tab displayed.

4 Click on the desired tab buttons to view or configure information about the bypass-only LSP, as required.

5 If you have made any configuration changes, click on Apply or OK in the Bypass-only LSP (Edit) form and a dialog box appears.

6 Click on the Yes button. The Bypass-only LSP (Edit) form closes.

7 Close the Manage Manual Bypass LSPs form.

Procedure 29-17 To configure an LSP path

The following procedure applies to dynamic LSPs and Bypass-only LSPs, unless otherwise noted. Dynamic LSPs are used to demonstrate the steps.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs form opens.

2 Configure the filter criteria and click on the Search button. A list of dynamic LSPs is displayed.

3 Select a dynamic LSP from the list.

4 Click the on Properties button. The Dynamic LSP (Edit) window opens with the General tab displayed.

5 Click on the LSP-Path Bindings tab button. A list of LSP paths is displayed.

6 If you are accessing this form to update the MPLS path for a Dynamic LSP, then go to step 10. Otherwise, go to step 7.

7 Select an LSP-Path Binding from the list and click on the Properties button. The LSP-Path Binding (Edit) form opens with the General tab displayed.

8 Configure the parameters:

- Type
- Administrative
- Backup Type
- Reserved Bandwidth (Mbps)
- Hop Limit
- Inherit Value
- Record Actual Path
- Record Label
- Diff-Serv Class Type
- Inherit Value
- Diff-Serv Backup Class Type
- Make before Break
- Inherit Value
- Resignal
- Enable CSPF
- Groups Included
- Inherit Value
- Groups Excluded
- Inherit Value

The Diff-Serv Backup Class Type parameter is only applicable to Dynamic LSPs.

9 Replace the existing MPLS path for a primary or secondary LSP with another MPLS path, if required, by proceeding as follows:

Note — You can update the existing MPLS path only for a primary or secondary LSP path that has the Make before Break parameter enabled, and that has a release 8.0 or later source NE. The MPLS path you want to use must already exist on the NE, and must not be used by any other LSP paths under the parent LSP.

i Click on the Update MPLS Path... button at the bottom of the form. The Choose MPLS Path form opens and displays the eligible MPLS paths.

ii Select the required MPLS path from the list.

iii Click on the OK button. The Choose MPLS Path form closes and the LSP-Path Binding (Edit) form is refreshed with the parameters related to the updated MPLS path selection.

iv Click on the OK button. The The LSP-Path Binding (Edit) form closes and the LSP-Path Binding list is refreshed with the updated MPLS path selected.

v Go to step 14.

10 Select the MPLS path from the list that you want to use to replace the existing path. Refer to the Note in step 9 for restrictions.

11 Click on the Update MPLS Path... button at the right side of the LSP-Path Binding tab page. The Choose MPLS Path form opens and displays the eligible MPLS paths.

12 Select the required MPLS path from the list.

13 Click on the OK button. The Choose MPLS Path form closes and the LSP-Path Binding list is refreshed with the updated MPLS path selected.

14 Click the Set as Secondary or Set as Standby buttons for a selected LSP-Path Binding to change its Type to one of these choices, if required.

15 Click on the Administrative Groups tab button.

16 Assign an MPLS administrative group to the dynamic LSP.

i Select an MPLS administrative group in the Unassigned list.

ii Click on the right arrow button. The group is assigned to the dynamic LSP and moves to the Assigned list.

After you assign administrative groups to an MPLS interface, the total value of the assigned groups is displayed in a bit mask format by the Groups Included (bitmask) indicator on the General tab.

17 Click on the General Tab and in the Shared Risk Link Group panel, configure the Enable SRLG for FRR or Enable SRLG parameter, if available and required.

18 Click on the Tests tab button to configure OAM diagnostics for the LSP path, if required. The supported test type tab buttons appear. See chapter 35 for more information about configuring OAM diagnostics.

19 View a list of hops or an LSP topology map, if required.

i Click on the following tab buttons to list the path hops or to view a topology map of the hops, if required:

- Provisioned Path
- Actual Path
- CSPF Path

ii Click on the Topology View button to view the topology map for the path, if required. See chapter 4 for information about using topology maps.

20 Click on the OK button. The LSP-Path Binding (Edit) form closes.

21 Click on the OK button. The Dynamic LSP (Edit) form closes.

Procedure 29-18 To create an LSP path using a tunnel template

Before you can create an LSP path from a tunnel template, you must create the tunnel template. You can use an existing LSP path to create a tunnel template. See the *5620 SAM Scripts and Templates Developer Guide* for more information.

1 Choose Manage→MPLS→Dynamic LSPs from the 5620 SAM main menu. The Manage Dynamic LSPs window opens.

2 Click on the Create from Template button. A Create Dynamic LSP from Template form opens with a list of previously created templates.

3 Choose a LSP template from the list. The template must be one where you associated a child LSP Path template to the parent LSP template. See Procedure 5-2 for information about creating parent and child objects for tunnel templates.

4 Click on the OK button. A Create Dynamic LSP from Template window opens. See Procedure 29-9 for information about creating a dynamic LSP from a template.

5 Click on the OK button. The Dynamic LSP (Edit) form opens.

6 Click on the LSP-Path Bindings tab button.

7 Click on the Create from Template button. A pop-up menu appears with an LSP path template.

8 Click on the template that you want to use for the LSP path.

9 Configure the parameters:

- Type
- Administrative
- Fast Re-Route
- Backup Type
- Hop Limit
- Backup Setup Priority
- Backup Hold Priority
- Maximum Transmitted Frame Size
- Committed Rate
- Peak Rate
- Setup Priority
- Hold Priority
- Reserved Bandwidth
- Hop Limit
- Record Actual Path
- Record Label
- Persistent
- Permit Merge
- IGP Shortcut Enabled
- Diff-Serv Class Type
- Diff-Serv Backup Class Type
- Main Class Type Retry Limit
- Make before Break
- Resignal
- Enable CSPF
- Rebuild Timer
- Groups Included (bitmap)
- Groups Excluded (bitmap)
- Groups Included (all) (bitmap)
- Enable SLRG
- Show Created Object

The IGP Shortcut Enabled, Diff-Serv Backup Class Type, and Main Class Type Retry Limit parameters are configurable for LSPs that have source NEs at Release 8.0 or later.

10 Click on the Inheritance tab button.

11 Configure the Overridden Properties parameter.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The Create LSP Path From Template form closes.

14 Close the Manage Dynamic LSPs window.

Procedure 29-19 To configure an LSP Path optimization policy

1 Choose Manage→MPLS→LSP Path Optimization from the 5620 SAM main menu. The Manage LSP Path Optimization window opens.

2 Choose LSP Path Optimization Policy (Path/Routing Management: MPLS) from the drop-down menu.

3 Click on the Create button. A drop-down menu appears.

4 Choose Create Optimization Policy. The LSP Path Optimization Policy (Create) window opens with the General tab displayed.

5 Configure the parameters:

- ID
- Auto-Assign ID
- Description

6 Click on the Candidate Definition tab button to apply filters to define eligible LSP Paths for optimization. When no filters are applied, all eligible LSP Paths are listed in the Execution Candidates window.

7 To further limit the number LSP Paths that are listed in the Execution Candidate window, define rule-based groups and add only those NEs that contain the LSP Paths that you need include.

i Click on Select button beside the Filter Name parameter in the LSP Path Filter panel. A Select LSP Path Filter dialog box appears.

ii Apply a filter, or create and apply a filter and click on the Search button. A list of LSP Path filters is displayed.

iii Choose an LSP Path filter from the list.

iv Click on the OK button. The LSP Path Filter panel is refreshed with the selected LSP Path Filter.

v Click on Select button beside the Filter Name parameter in the Dynamic LSP Filter panel.

vi Apply a filter, or create and apply a filter and click on the Search button. A list of dynamic LSP filters is displayed.

vii Choose a dynamic LSP filter from the list

viii Click on the OK button. The Dynamic LSP Filter panel is refreshed with the selected dynamic LSP filter.

ix Click on Select button beside the Group Name parameter in the Rule-Based Group panel. A list of rule-based groups is displayed

x Choose a rule-based group from the list.

xi Click on the OK button. The Rule-Based Group panel is refreshed with the selected rule-based group.

8 Click on the Execution Rules tab button. Configure the parameters:

- Sequencing Target
- Sequencing Order
- Pacing Interval (seconds)

9 Click on the Apply button, the window is refreshed with schedule information.

Note 1 — The Schedule Optimization button does not appear during LSP path optimization policy creation. The LSP path optimization policy must be created first before a schedule can be applied. You must click on the Apply button.

Note 2 — After a schedule is applied to a LSP Optimization Policy, you cannot make changes to the schedule from the Optimization Scheduled Task window.

10 Click on the Schedule Optimization button. An Optimization Scheduled Task (Create) form opens.

11 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

12 Click on the Select button beside the ID parameter. A Select Schedule - Optimization Scheduled Task window opens.

13 Perform one of the following:

a Click on the Create button to create a schedule. A SAM Schedule Create form opens. See Procedure 74-1 for more information about creating a schedule.

b Choose a previously created schedule.

14 Click on the OK button. The Optimization Scheduled Task window refreshes with the schedule and optimization information.

15 Click on the OK button. The Select Schedule - Optimization Scheduled Task window closes and the LSP Path Optimization Policy window reappears.

16 Click on the Execution Candidates tab button.

17 Click on the Refresh button to display only the eligible LSP Paths that were filtered in step 7. If a filter was not applied, all eligible LSP Paths are listed.

18 Click on the Optimize button. To view the results of optimization, see Procedure 29-21.

19 Close the LSP Path Optimization Policy window.

Procedure 29-20 To terminate an LSP Path optimization policy that is in progress

1 Choose Manage→MPLS→LSP Path Optimization from the 5620 SAM main menu. The Manage LSP Path Optimization window opens.

2 Choose LSP Path Optimization Policy (Path/Routing Management: MPLS) from the drop-down menu.

3 Create a filter to search for optimization policies that are in progress. Click on the Search button. A list of LSP Path optimization policies that are in progress appears.

4 Choose a LSP Path optimization policy from the list.

5 Click on the Properties button. The LSP Path Optimization Policy (Edit) window opens with the General tab displayed.

6 Click on the Stop Current Optimization button. The Optimization parameter value changes from In Progress to Not In Progress.

7 Close the LSP Path Optimization Policy (Edit) window.

Procedure 29-21 To view LSP Path optimization policy results

Use the following procedure to view the re-signaling information as a result of the LSP Path optimization policy execution. See Procedure 29-19 for more information about configuring a LSP Path optimization policy.

1 Choose Manage→MLPS→LSP Path Optimization from the 5620 SAM main menu. The Manage LSP Path Optimization window opens.

2 Select LSP Path (Path/Routing Management MPLS) from the drop-down menu.

3 Click on the Search button. A list of LSP Paths appears.

4 Choose the LSP Path on which you executed a LSP optimization policy.

5 Click on the Properties button. An LSP-Path Binding (Edit) window opens.

6 View the following parameters, as described in section 29.1.

- Resignal Eligible
- Last Performed Type
- Last Performed
- Last Performed State

7 Close the LSP-Path Binding window.

8 Close the Manage LSP Path Optimization window.

Procedure 29-22 To view detour and bypass path information

Perform this procedure to view information regarding detour and bypass tunnel paths and their protected LSPs. Detour and bypass paths are typically configured for fast-reroute-enabled LSPs on NEs for service protection against NE or link failure. The RSVP protocol is used to detect an NE or link loss.

Note 1 — This procedure applies to dynamic LSPs only.

Note 2 — Detours are employed in One-to-One backup configurations. A separate backup LSP is established for each LSP that is backed up.

Bypass Tunnels are employed in Many-to-One backup configurations in which a single backup LSP is used to back up multiple original LSPs.

Whether a path is a detour or bypass path is determined by the Backup Type value specified during LSP creation. The Backup Type parameter can be set only when Fast Reroute for the LSP is set to true.

1 Navigate to a dynamic LSP that you want to examine. The path is Manage→MPLS→Dynamic LSPs.

2 Select the required LSP and click on the Properties button. The Dynamic LSP (Edit) form opens.

3 Click on the RSVP Sessions tab button. The detour or bypass originating, transiting, and terminating RSVP sessions associated with the LSP are listed. Type, site, next and previous hop, and other related information is available.

4 Select the desired RSVP session of type detour or bypass from the list and click on the Properties button. The Session (View) form opens.

5 To view the Protected LSPs for the specific bypass or detour:

   i Click on the Protected LSP Paths tab button. All the protected LSPs for a specific bypass or detour tunnel are listed.

   ii Use the scroll bar at the bottom of the list frame to view the available information on the Protected LSPs.

6 To view the Detour or Bypass Tunnel Paths for the detour or bypass tunnel:

i Click on the Detour/Bypass Tunnel Path tab button. Information regarding the detour or bypass paths is displayed. Sufficient information is provided to permit tracing a path from its originating site, through its transit hops, and to its termination site.

ii Use the scroll bar at the bottom of the list frame to view the available information on the paths, including ID, Type, and so on.

7 To view additional specific Detour or Bypass information, perform the following steps, as appropriate:

a For a selected detour session, click on the Detour tab button. The Detour Session ID, Detour PLR ID, and Avoided Downstream Site ID are listed.

b For a selected bypass session, click on the Bypass Tunnel tab button. The Bypass Tunnel's current State is displayed.

Note — For 5620 SAM to accurately gather the information about the detour and bypass tunnel path (and the LSPs protected by a detour or a bypass tunnel), 5620 SAM must be managing all routers participating the LSP fast reroute. This is required by 5620 SAM for all SR and 7705 SAR nodes along the primary path of a fast reroute-enabled LSP.

Procedure 29-23 To create an LSP template for MVPN

1 Choose Policies→MPLS→LSP Template MVPN from the 5620 SAM main menu. The Manage LSP Template for Mvpn form opens.

2 Perform one of the following:

a Configure the Policy scope parameter to Global.

b Configure the Policy scope parameter to Local.

i Configure the Local Node IP Address parameter, if required

ii Click on the Select button and choose a device.

3 Click on the Create button. The LSP Template MVPN Policy (Create) form opens.

4 Configure the parameters:

- Displayed Name
- Description

5 Click on the Properties tab button.

6 Configure the parameters in the Traffic Engineering and Protection panel:

- Reserved Bandwidth (Mbps)
- Fast Reroute
- Hop Limit
- Record Actual Path
- Record Label

7 Configure the parameters in the Fast Reroute panel:

- Backup Type
- Hop Limit

Note — The Backup Type and Hop Limit parameters are configurable if the Fast Reroute parameter is set to true.

8 Configure the Make Before Break parameter.

9 Configure the parameters in the CSPF panel:

- Enable CSPF
- Enable TE Metric

10 Configure the parameters in the Signalling panel:

- Retry Timer (seconds)
- Retry Limit

11 Click on the Administrative Groups tab button.

12 Assign one or more MPLS administrative groups to the LSP template MVPN policy.

i Choose the required Included Groups in the Unassigned list.

ii Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.

iii Choose the required Excluded Groups in the Unassigned list.

iv Click on the right arrow button. The groups are assigned to the Point-to-Multipoint LSP and moved to the Assigned list.

After you assign the Included and Excluded Groups, the total value of the groups is displayed in a bit mask format by the Groups Included and Groups Excluded indicators on the LSP Template MVPN Policy Properties tab.

13 Click on the OK button. The LSP Template MVPN Policy, Global Policy (Create) form closes and the Manage Lsp Template for Mvpn form reappears with the LSP MVPN template displayed.

14 Choose the LSP MVPN template and click on the Properties button. The LSP Template MVPN Policy - Global Policy (Edit) form opens with the General tab displayed.

15 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when the policies are used by resources on the device.

Note 1 — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 43 for more information.

Note 2 — The MVPN LSP template cannot be used until you choose a default MPLS path and configure the Administrative parameter in the local policy definition after the global policy is distributed. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes are saved.

16 Click on the Local Definitions tab button.

17 Click on the Search button. A list of LSP MVPN templates is displayed.

18 Choose an LSP MVPN template from the list and click on the Properties button. The LSP Template MVPN Policy, Local Policy (Edit) form opens with the General tab button displayed.

19 Click on the Switch Mode button to change the configuration mode to Local Edit Only.

20 Click on the Properties tab button.

21 Click on the Select button to choose a default MPLS path. The Select Default MPLS Path - Lsp MVPN Template, Local Policy window opens with a list of default MPLS paths displayed.

22 Choose an MPLS path from the list and click on the OK button. The default MPLS path is displayed.

23 Click on the General tab button.

24 Configure the Administrative parameter.

25 Click on the OK button. A dialog box appears.

26 Click on the OK button. The LSP Template MVPN Policy, Local Policy form closes.

Procedure 29-24 To view 7250 SAS-ES and 7250 SAS-ESA dynamic bypass LSP information

You must use the 5620 SAM LSP topology map to view dynamic bypass LSPs; dynamic bypass LSPs are not displayed when you choose Manage→LSPs→Dynamic LSPs.

1 Choose Applications→LSP Topology from the 5620 SAM main menu. The LSP topology map opens. See chapter 4 for information about using topology maps.

2 Double-click on a link between two map objects. The Lsp Group List form opens with dynamic and bypass-only LSPs displayed.

3 Choose the required bypass-only LSP and click on the Properties button. The Dynamic LSP (Edit) form opens.

4 View the bypass-only LSP properties, as required.

5 Close the Dynamic LSP (Edit) form.

Note — You cannot modify the properties of a dynamic bypass LSP or the properties of any MPLS paths that are used by the dynamic bypass LSP.

6 Close the Lsp Group List form.

7 Close the LSP topology map.

Procedure 29-25 To list and view MPLS objects

1 Choose Manage→MPLS→MPLS Objects from the 5620 SAM main menu. The Manage MPLS Objects form opens.

2 Select an MPLS object type in the list and click on the Search button. A list of MPLS objects is displayed.

3 Select an object in the list and click on the Properties button. The properties form for the object appears.

4 View the information on the various tabs, as required.

5 Close the object properties form.

6 Close the Manage MPLS Objects form.

Procedure 29-26 To view the LSP topology map

1 Choose Application→LSP Topology from the 5620 SAM main menu. The LSP Topology map opens.

2 View the topology map as required. See chapter 4 for information about using topology maps.

3 Close the topology map.

30 — Service tunnels

30.1 IP/MPLS service tunnel overview

Distributed service traffic is transported between PE NEs by circuits aggregated in unidirectional service tunnels, also called SDP bindings. Service tunnels originate on a source NE and terminate on a destination NE that directs packets from the service tunnel to the correct service egress interface. Service tunnels are not used for local services because the same NE is the source and the destination.

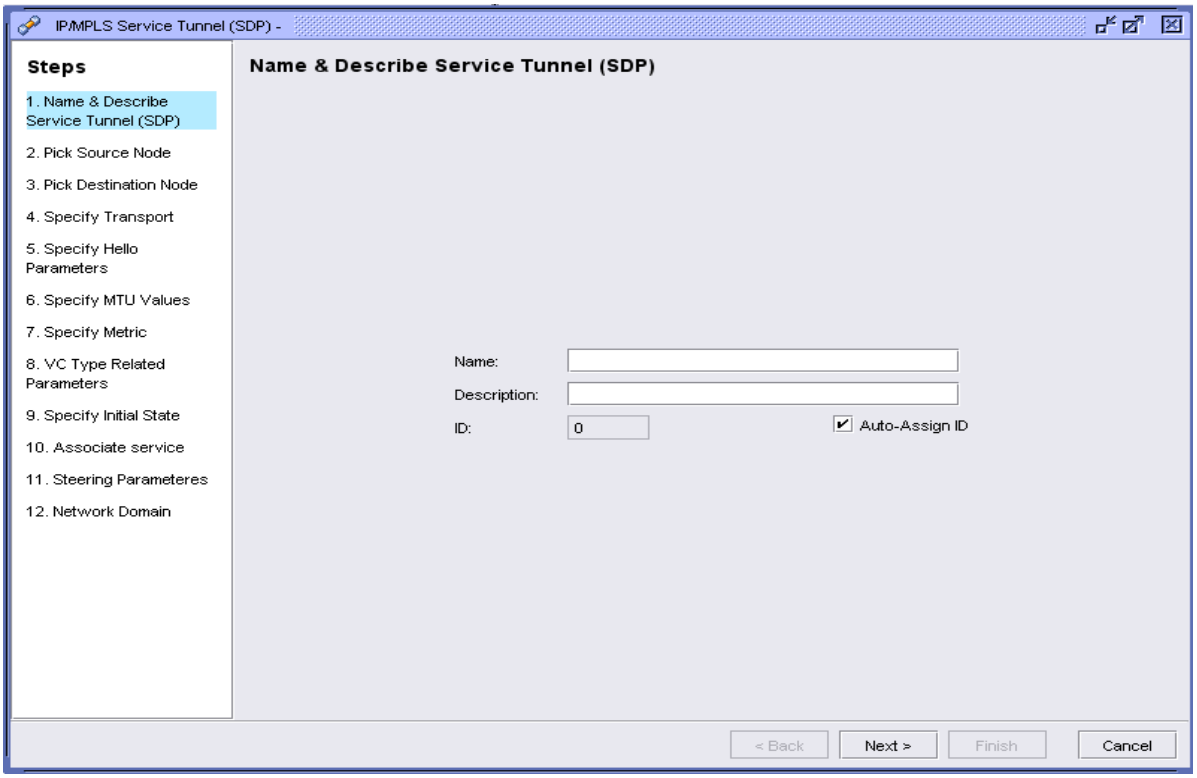
The operational theory of a service tunnel is that the encapsulation of the data between the two managed edge NEs appears like a Layer 2 path to the service data although it is really traversing an IP or IP/MPLS core.

Old tunnel policies can be converted to new template-based policies by using a "Convert" button located on the rule configuration form. You cannot configure CoS forwarding, LDP-over-RSVP, or multiple LSP bindings on SDP features.

A service tunnel uses GRE or MPLS encapsulation. For MPLS, a mesh of MPLS paths and LSPs must be present in the network core. You associate service tunnels with LSPs during service tunnel configuration. The 5620 SAM supports LSP creation using a basic LDP variant such as T-LDP, or using LDP over RSVP for tunnel-in-tunnel functionality based on traffic classification.

Figure 30-1 shows the Create Service Tunnel (SDP) form.

Figure 30-1 Create Service Tunnel (SDP) form



A 5620 SAM operator binds a service site to a service tunnel during service configuration. A service tunnel has a unique ID on an NE and cannot be deleted when it is currently associated with a service.

ACL IP and ACL MAC policy filters for service tunnels contain options for forwarding packets on a specific service tunnel based on matching criteria, as described in chapter 45.

Consider the following before you configure IP/MPLS service tunnels:

- Service tunnels are unidirectional, so they are required in both directions between the source NE and the destination NE.
- The tunnel is not specific to one service or one type of service. After a tunnel exists, multiple SDPs can be aggregated over the tunnel. The SDPs can belong to different services and different customers.
- When a tunnel already exists, 5620 SAM does not automatically create a new tunnel, even if the only available tunnel is down. This prevents the creation of multiple inoperable tunnels.
- All services that are mapped to a tunnel use the same transport encapsulation type defined for the tunnel.
- Operations on the tunnel affect all the services that are associated with the tunnel. For example, the operational and administrative states of a tunnel control the state of service circuits that are carried on the tunnel. In the case of LSP-based tunnels, an LSP can be replaced in the tunnel without reconfiguring each service bound to the tunnel.
- A service tunnel is locally unique to an NE. The same tunnel ID can appear on other NEs.
- A service tunnel uses the system IP address to identify the far-end edge NE.
- A service tunnel can be configured using a tunnel template. A user that is assigned the create tunnel template scope of command role can create a tunnel template. The template manager can also apply the tunnel template to a service tunnel. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with tunnel templates.
- An SDP tunnel template can be applied to an auto tunnel policy.

See the appropriate device documentation for more detailed information about service tunnels.

Class-based forwarding

Packets of the same CoS and service are forwarded over a specific RSVP LSP (or a static LSP), which is part of an SDP that the service (instance) is bound to. The forwarding decision is based on the forwarding class of the packet, as assigned by the ingress QoS policy defined for the SAP.

When implementing class-based forwarding, consider the following:

- Class-based forwarding is typically implemented using the service tunnel configuration forms, as detailed in Procedure 30-1. Class-based forwarding configurations can also be altered after their initial creation by editing the service tunnel configuration form as detailed in Procedure 30-9.
- An LSP can carry packets of a forwarding class for one service and at the same time, carry packets of a different forwarding class for another service. In other words, the same LSP can be used by more than one SDP, even where the forwarding class assignments are different.
- Within an SDP, only one LSP can support a specific CoS.
- A service instance (or service site) can be bound to SDPs of differing CoS configurations, as well as regular SDPs.
- One LSP in the SDP must be designated as the default LSP. The default LSP is used by the SDP if there is no available LSP that matches the packet's forwarding class. When the default LSP is down, the SDP is also brought down.
- Class-based forwarding can be applied to all services supported by the SRs. For VPLS, you can specify an LSP to forward all multicast/broadcast packets (by default, the default LSP is used). For VLL, shared queuing must be enabled on the ingress SAP to support the class-based forwarding.
- Class-based forwarding is configurable on the 7750 SR, 7710 SR, and 7450 ESS

30.2 Ethernet (G.8031) tunnel overview

The IEEE 802.1ah Provider Backbone Bridging specification employs Provider MSTP to ensure loop avoidance in a resilient native Ethernet core. With P-MSTP, failover times depend largely on the size of the network and the connectivity model used in the network. MPLS tunnels provide core scaling and fast failover times using MPLS FRR. A service based on native Ethernet backbone achieves the same fast failover times as MPLS FRR.

Core Ethernet tunnels compliant with the ITU-T G.8031 specification achieve 50 ms resiliency for backbone failures. A configured Ethernet tunnel can be selected when configuring an L2 access interface on a B-VPLS.

The 5620 SAM uses two different approaches to configure Ethernet tunnels in the network.

- Approach 1 (recommended):

  5620 SAM provisions an end-to-end Ethernet G.8031 tunnel which reduces configuration errors and aids the diagnosis of any problem in the tunnel. 5620 SAM automatically configures the Ethernet tunnel endpoint and path endpoint on each of the participating NEs. See Procedure 30-6 for more information.

  The Ethernet tunnel and path are network wide objects that provide the following benefits:

  - the Ethernet tunnel provides the aggregated State of the Tunnel and reports any inconsistency in the configuration of the endpoints or paths
  - faster and easier provisioning that allows you to configure common properties such as holdTime and revertTime at the network level and then apply them to each tunnel endpoint
  - 5620 SAM accelerates the creation of global and local MAs, and MEPs by using a continuity check
- Approach 2:

  The 5620 SAM provides the ability to provision Ethernet tunnel endpoints and path endpoints separately on each NE. See Procedure 30-5 for more information on creating Ethernet endpoints. If Ethernet tunnel endpoints are created this way (or discovered from the NE) you can associate them to a network-wide Ethernet tunnel and path, but this must be done manually.

Note — Network-wide Ethernet tunnels and paths are not automatically discovered from the NE.

30.3 Configuring service tunnel procedures

Procedure 30-1 describes how to manually create an IP/MPLS service tunnel.

Procedure 30-1 To create an IP/MPLS service tunnel

Note — The following tab buttons are supported on the OS 9700E and OS 9800E NEs for the creation of an SDP tunnel by choosing Manage→Service Tunnels:

- General
- LSPs
- Templates
- Circuits
- Customer
- Services
- Faults

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Click on the Create button and choose IP/MPLS service tunnel (SDP). The IP/MPLS service tunnel (SDP) step form opens with the Name & Describe Service Tunnel (SDP) step displayed.

3 Configure the parameters.

- Name
- Description
- Auto-Assign ID
- ID

Note — If a range policy is applied to a service tunnel, a grey text box appears beside the Service ID parameter to indicate that a range policy is in effect.

If a format policy is applied to a service tunnel, a combo box appears beside the object field during object creation to indicate that a format policy is in effect. When there is only one matching policy, the combo box is greyed out. When there are multiple matching policies the combo box is used to choose a policy. The sequence of the options in the combo box are ordered by the policy Priority Value parameter.

4 Click on the Next button. The Pick Source Node step is displayed.

5 Configure the Source Site ID parameter. Perform one of the following:

a Choose an NE from a list.

i Click on the Select button. The Select a Network Element - Pick Source Node form opens.

ii Choose an NE in the list and click on the OK button. The Select a Network Element - Pick Source Node form closes and the Create Service Tunnel (SDP) form displays the source NE IP address.

b Enter the NE IP address.

6 Click on the Next button. The Pick Destination Node step is displayed.

7 Configure the Destination Site ID parameter. Perform one of the following:

a Choose an NE from a list.

i Click on the Select button. The Select a Network Element - Pick Destination Node form opens.

ii Choose an NE in the list and click on the OK button. The Select a Network Element - Pick Destination Node form closes and the Create Service Tunnel (SDP) form displays the destination NE IP address.

b Enter the NE IP address.

8 Click on the Next button. The Specify Transport step is displayed.

a If the source or destination is a 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], or 7250 SAS-ES site, you cannot configure the Underlying Transport parameter. The 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7250 SAS-ES support only MPLS with TLDP signalling, LDP is not enabled. Go to step 11.

b When you implement class-based forwarding or specify a transport destination address, you must select MPLS as the Underlying Transport parameter. Go to step e.

Note — When you specify a transport destination address, you cannot implement class-based forwarding.

c When you configure a service tunnel whose source site is a 7705 SAR (version 3.0 or later), you may select IPv4 as the Underlying Transport parameter if the destination site is also a 7705 SAR (version 3.0 or later), a GNE, or an unmanaged IP address.

d For GRE:

i Specify GRE for the Underlying Transport parameter.

ii Configure the Signaling parameter.

iii Go to step 19.

e For MPLS:

i Specify MPLS for the Underlying Transport parameter.

ii Configure the parameters:

- Mixed Lsp Mode
- Revert Time (seconds)

The Revert Time (seconds) parameter is only displayed when the Mixed Lsp Mode parameter is set to true.

iii Configure the parameters:

- Ldp Enabled
- Bgp Tunnel Enabled

Note 1 — When you implement class-based forwarding, you must use one of the following parameter configurations:

- Set Mixed Lsp Mode to true.
- Set Mixed Lsp Mode, Ldp Enabled, and Bgp Tunnel Enabled parameters to false.

Note 2 — When you specify a transport destination address, you must use the following parameter configurations:

- Set Ldp Enabled to true.
- Set Mixed Lsp Mode and Bgp Tunnel Enabled to false.

Note 3 — You cannot set Bgp Tunnel Enabled to true when Ldp Enabled or Mixed Lsp Mode is set to true.

Note 4 — You cannot create a BGP or an LDP tunnel when an LSP exists between the source and destination nodes you chose in steps 4 and 7 respectively.

iv If you set the Ldp Enabled or Bgp Tunnel Enabled parameter to true, go to step 19.

v To specify a transport destination address, go to step 17.

vi Configure the parameters:

- Underlying Transport
- Signaling

9 Click on the Next button. The Specify Class Forwarding step is displayed.

10 Configure the parameters:

- Class Forwarding Capability
- Administrative State
- Enforce Diff-Serv Lsp-Fc Map

Note — When the Class Forwarding Capability parameter is set to Off, the existing class-forwarding configurations are removed.

The Administrative State and Enforce Diff-Serv Lsp-Fc Map parameters are configurable when the Class Forwarding Capability parameter is set to On.

11 Click on the Next button. The Associate LSPs step is displayed.

12 Click on the Add button to bind an LSP to the service tunnel. The Bind LSPs to Service Tunnel form opens with the Bind LSP to Service Tunnel Stage step displayed.

13 Select an LSP and click on the Finish button.

14 Click on the Close button. The Bind LSPs to Service Tunnel form closes and the LSP is listed on the Create Service Tunnel (SDP) form.

15 If you are enabling class-based forwarding:

a Select an LSP from the list and click on the Set As Default LSP button. This is mandatory. The Default LSP Name appears in the associated field.

b For a VPLS, you can optionally specify an LSP to forward all multicast/broadcast packets. If this is not specified, the default LSP is used. If it is specified, the Multicast LSP Name appears in the associated field.

c For any LSPs used for class-based forwarding (including the default), you must select the LSP from the list and click on the Choose a Forwarding Class button. Select the desired forwarding class from the fly-out menu. Your choice appears in the Forwarding Class to LSP Mappings table.

d When you have finished configuring the LSPs, go to step 19.

16 If the source is a 7250 SAS-ES site, go to step 27.

17 Click on the Next button. The Specify Transport Destination Address step is displayed.

18 Configure the Transport Destination Address parameter.

Note — The Transport Destination Address parameter is configurable only for the 5620 SAM 8.0, R4 or later.

19 Click on the Next button. The Specify Hello Parameters step is displayed.

20 Configure the parameters.

- Keep-alive Enabled
- Hello Time
- Hello Request Timeout
- Max Drop Count
- Hello Message Length
- Hold Down Time

21 Click on the Next button. The Specify MTU Values step is displayed.

22 Configure the parameters.

- Administrative MTU
- Advertised MTU Override

23 Click on the Next button. The Specify Metric step is displayed, if applicable.

24 Configure the Metric parameter, if applicable.

25 Click on the Next button. The VC Type Related Parameters step is displayed, if applicable.

26 Configure the VLAN VC Ethertype parameters, if applicable.

27 Click on the Next button. The Specify Initial State step is displayed.

28 Configure the Administrative parameter.

29 Click on the Next button. The Booking Factor step is displayed.

Note — This step is only displayed if the Underlying Transport parameter you specified in step 8 was set to MPLS and the Ldp Enabled parameter was set to false.

30 Configure the SDP Bandwidth Booking Factor (%) parameter.

31 Click on the Next button. The Associate Service step is displayed.

32 Click on the Select button. The Select Associated Service window opens.

33 Choose a service from the list and click on the OK button. The Select Associated Service window closes. The Associated Service Name and Associated Service ID are updated.

34 Click on the Next button. The Steering Parameters step is displayed.

35 Select the Steering Parameters in the Unassigned list that you want to assign to the tunnel and click the right-pointing arrow to move them into the Assigned list.

36 Click on the Next button. The Network Domain step is displayed.

37 Click the Select button. The Select Network Domain window opens.

38 Choose a network domain from the list and click on the OK button. The Select Network Domain window closes. The Name field is updated.

Note — All SDPs are associated with a network domain. This association is done during the creation or when editing an SDP in the Tunnel (Edit) form. You can also modify the network domain in the Tunnel (Edit) form. See step 42. The Egress Interfaces Consistency State status specifies if all the interface associations to SDP belong to a particular domain.

39 Click on the Finish button to save the configuration. The 5620 SAM prompts you to view the service tunnel configuration.

40 Enable the View the newly created tunnel parameter to view the service tunnel configuration after closing the form, if required.

41 Click on the Close button. The Create Service Tunnel (SDP) form closes.

42 If the View the newly created tunnel parameter in step 40 is enabled, the Tunnel (Edit) form opens with the newly-created service tunnel configuration displayed.

i View or modify the configuration, if required.

ii Click on the Create a template button, if required. See the *5620 SAM Scripts and Templates Developer Guide* for information about creating a template.

iii Close the Tunnel (Edit) form.

43 Close the Manage Service Tunnels form.

Procedure 30-2 To create an SDP using a tunnel template

Before you can create an SDP from a tunnel template, you must create the SDP tunnel template. For more information about creating SDP tunnel templates, see the *5620 SAM Scripts and Templates Developer Guide*.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click on the Create from Template button. A Create Service Tunnel From Template window opens with a list of previously configured SDP tunnel templates.

3 Choose a tunnel template from the list.

4 Click on the OK button. A Create Tunnel from Template form opens with the General tab displayed.

5 Configure the parameters.

- Name
- Description
- Auto-Assign ID
- ID
- Underlying Transport
- PBB Ethernet Type
- Enable LDP
- Signaling
- Source Site ID
- Destination Site ID
- Transport Destination Address
- Administrative
- Administrative MTU
- Advertised MTU Override
- Metric
- VLAN VC Ethertype
- No VLAN VC Ethertype

6 Click on the SDP Bandwidth tab button. Configure the SDP Bandwidth Booking Factor (%) parameter.

7 Click on the Maintenance Tab button and configure the following parameters:

- Keep-alive Enabled
- Hello Time
- Hello Message Length
- Hello Request Timeout
- Hold Down Time
- Max Drop Count

8 Click on the Accounting tab button.

9 Click on the Select button beside the Accounting Policy parameter to assign an accounting policy to the service tunnel. A Select Policy window opens with a list of accounting policies.

10 Choose a policy from the list and click on the OK button. The Select Policy widow closes and the Accounting Policy parameter is updated

11 Configure the Show created object parameter, if required.

12 Click on the OK button. When the SDP configuration is successful, the Create SDP from Template form closes and the Tunnel (Edit) form appears.

If the SDP configuration is unsuccessful, the Create SDP from Template form remains open and an error message appears.

13 Close the Tunnel (Edit) form.

Procedure 30-3 To create a Steering Parameter

A Steering Parameter is assigned to a service tunnel and acts as a marker for the Tunnel Selection Profile. More than one Steering Parameter can be assigned to a tunnel.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Click on the Create button and choose Steering Parameter. The Steering Parameter (Create) form opens.

3 Configure the Name and Value parameters.

4 Click on the OK button. The Steering Parameter (Create) form closes.

Note — You can also examine an existing Steering Parameter by conducting a search using the Manage Service Tunnels form. Viewing an existing Steering Parameter displays Service Tunnels and Tunnel Selection Profiles tab pages. These allow you to see which of these items make use of the Steering Parameter. A Faults tab page displays any related alarms that have been logged.

5 Close the Manage Service Tunnels form.

Procedure 30-4 To create a Tunnel Selection Profile

A Tunnel Selection Profile is used by 5620 SAM to assign transport tunnels for a service when the service has been configured for automatic SDP binding creation. However, for services where the SDP binding creation is performed manually, the Tunnel Selection Profile can also still be used. In these cases, tunnels and return tunnels are chosen by the system when the automatic selection of such transport tunnels is enabled and a Tunnel Selection Profile is specified.

The Tunnel Selection Profile contains Steering Parameters. When the profile is used within a service to create SDP bindings, any tunnels tagged with the Steering Parameters included in that profile become eligible for consideration in the tunnel selection process.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Click on the Create button and choose Tunnel Selection Profile. The Tunnel Selection Profile (Create) form opens with the General tab displayed.

3 Configure the parameters.

- Profile Name
- Description
- Transport Type

4 Click on the Select button.

5 Choose an SDP Binding Template from the list, if required, and click OK. The Script ID, Name, and Description fields for the selected SDP Binding Template are populated in the Tunnel Selection Profile (Create) form.

Note — Specifying an SDP Binding Template in the profile allows the 5620 SAM to use the configuration information contained in the template for the automatic creation of SDP bindings. See the *5620 SAM Scripts and Templates Developer Guide* for information about creating a template.

6 Click on the Steering Parameters tab button.

7 Click on the Steering Parameters that you want to include in the profile in the Included Steering Parameters-Unassigned portion of the form. If you are selecting more than one, hold down the Shift key after your first selection.

8 Click the right-pointing arrow to move the selected Steering Parameters into the Included Steering Parameters-Assigned portion of the form.

You can move an assigned parameter back into the unassigned portion of the form if required, by selecting it and clicking the left-pointing arrow.

9 Click on the Steering Parameters that you want to exclude from the profile in the Excluded Steering Parameters-Unassigned portion of the form. If you are selecting more than one, hold down the Shift key after your first selection.

10 Click the right-pointing arrow to move the selected Steering Parameters into the Excluded Steering Parameters-Assigned portion of the form.

You can move an assigned parameter back into the unassigned portion of the form if required, by selecting it and clicking the left-pointing arrow.

11 Click on the OK button. The Tunnel Selection Profile (Create) form closes.

Note — When configuring an existing profile, the Tunnel Selection Profile (Edit) form displays additional tabs pages, including Services, SDP Bindings, and Spoke Connectors. These allow you to see which of these items make use of the Tunnel Selection Profile. A Faults tab page displays any related alarms that have been logged.

12 Close the Manage Service Tunnels form.

Procedure 30-5 To create or configure an Ethernet Tunnel Endpoint

Procedure 30-5 describes how to create a new Ethernet Tunnel Endpoint or configure an existing one.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 If you are configuring an existing Ethernet Tunnel Endpoint, go to step 8.

3 Click on the Create button.

4 Click on Ethernet Tunnel Endpoint on the contextual menu. The Select Network Elements window opens.

5 Choose a site on which to create an Ethernet tunnel endpoint.

6 Click on the OK button. The Ethernet Tunnel Endpoint (Create) form opens with the General tab displayed.

7 Go to step 10.

8 Select Ethernet Tunnel Endpoint (Ethernet Tunnel) on the drop-down menu in the Manage Service Tunnels window. Click on the Search button to display a list of the existing endpoints.

9 Select the endpoint you want to configure and click on the Properties button.

The Ethernet Tunnel Endpoint (Edit) form opens with the General tab displayed.

10 Configure the following parameters:

- Tunnel Endpoint ID
- Site ID
- Protection Type
- Encap Type
- Administrative State
- Hold Time Down (centiseconds)
- Hold Time Up (deciseconds)
- Revert Time (seconds)
- Access Adapt QoS
- Per FP Ingress Queue
- Operational Path Endpoint Threshold
- Description
- Configured MAC

The Tunnel Endpoint ID and Site ID are only configurable when you are creating a new Ethernet Tunnel Endpoint.

The Access Adapt QoS, Per FP Ingress Queue, and Operational Path Endpoint Threshold parameters are only displayed when the Protection Type is set to Load Sharing.

11 Click on the Path Endpoints tab button to configure the Path Endpoints.

12 Perform one of the following:

a If you are configuring an existing Ethernet Tunnel Path Endpoint, select the required path endpoint from the list and click Properties. The Ethernet Tunnel Path Endpoint (Edit) form opens with the General tab displayed.

b If you are configuring a new Ethernet Tunnel Path Endpoint, click on the Add button. The Ethernet Tunnel Path Endpoint (Create) form opens with the General tab displayed.

13 Configure the following parameters for each Path Endpoint.

- Path ID
- Description
- Administrative State
- Precedence
- APS Command

The Path ID parameter is only configurable when you are creating a new Ethernet Tunnel Path Endpoint.

The APS Command parameter is only displayed and configurable when you are configuring an existing Ethernet Tunnel Path Endpoint and when the Protection Type parameter you configured in step 10 is set to G8031 1:1. The associated "Perform APS Command" button is used to perform the selected command on the path endpoint.

14 Click on the Properties button in the Ethernet Path block if you need to view or alter parameters on the Ethernet Path or configure a CFM Test. The Ethernet Path - Properties button is only displayed and selectable when you are configuring an existing Ethernet Tunnel Path Endpoint.

15 If you are configuring an existing Ethernet Tunnel Path Endpoint, go to step 23.

16 Click on the Port tab.

17 Click on the Select button. The Select Member Port window opens.

18 Click on the Search button to list the available ports. Choose the port to use for the Ethernet tunnel path endpoint.

19 Click on the OK button. The Ethernet Tunnel Path Endpoint (Create) form displays the selected member port.

20 Configure the parameters:

- Control Tag (Outer Encapsulation Value)
- Control Tag (Inner Encapsulation Value)

21 Click on the OK button. The Ethernet Tunnel Path Endpoint (Create) form closes and the Path Endpoints tab displays the new Ethernet Tunnel Path Endpoint in the list.

22 Go to step 30.

23 Click on the MEPs tab, if you need to create a MEP for the existing Ethernet Tunnel Path Endpoint. Otherwise go to step 30.

24 Click on the Add button. The MEP (Create) form opens with the General tab displayed.

25 Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages
- Control MEP
- Priority Level for CCM Messages
- Low-priority Defect
- Mac Address
- Fault Propagation
- Type
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

The Control MEP parameter is only displayed if the SAP, BINDING or PATH ENDPOINT parameter is set to Ethernet Tunnel Path Endpoint.

Note — When configuring a Down MEP on a Subscriber Group Interface SAP, the Direction parameter cannot be configured.

26 If the Maintenance Domain for this MEP has a Name Type of none and its Maintenance Association has a Name Format of icc-based, then the Y.1731 TEST and the AIS tabs will also be displayed. See Procedure 64-25 for more information.

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The MEP (Create) form closes and the newly-created MEP is displayed in the list on the MEPs tab.

29 Click on the OK button. The Ethernet Tunnel Path Endpoint (Edit) form closes and the Path Endpoints tab displays the available Ethernet Tunnel Path Endpoints in the list.

30 Repeat steps 12 to 29 for any other Ethernet Tunnel Path Endpoints you need to create or configure.

31 Click OK. A dialog box appears.

32 Click Yes to close the Ethernet Tunnel Endpoint form.

Procedure 30-6 To create an Ethernet tunnel

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click on the Create button.

3 Click on Ethernet Tunnel on the contextual menu. The Ethernet Tunnel (Create) window opens.

4 Configure the following parameters:

- Tunnel ID
- Name
- Description
- Protection Type
- Encap Type
- Hold Time Down (centiseconds)
- Hold Time Up (deciseconds)
- Revert Time (seconds)
- Access Adapt QoS
- Per FP Ingress Queue
- Operational Path Endpoint Threshold

The Access Adapt QoS, Per FP Ingress Queue, and Operational Path Endpoint Threshold parameters are only displayed when the Protection Type is set to Load Sharing.

5 Click on the Apply button. The Ethernet Tunnel (Edit) window opens with the General tab displayed.

6 Click on the Components tab button. Right click on Tunnel Endpoints and choose one of the following from the contextual menu.

a Create Ethernet Tunnel Endpoint.

i Refer to Procedure 30-5 to create an Ethernet Tunnel Endpoint. The endpoint will be listed as Endpoint A on the Ethernet Tunnel form in the Tunnel Endpoints Section.

Note — The parameter values specified in step 4 are automatically applied in the Ethernet Endpoint form when creating an endpoint.

ii Repeat step i to create Endpoint B.

iii Go to step 7.

b Add Existing Endpoint.

i The Select Endpoints window opens.

ii Click on the Search button and select an endpoint.

iii Click OK.

iv The endpoint is listed as Endpoint A on the Ethernet Tunnel form in the Tunnel Endpoints Section.

Note — The parameter values specified in step 4 are not automatically applied to the selected Ethernet endpoint.

v Repeat steps i to iv to select Endpoint B.

7 Right click on Paths and choose Create Ethernet Paths from the contextual menu to create a path. The Ethernet Path (Create) window opens with the General tab displayed.

8 Configure the parameters:

- Auto-Assign ID
- ID
- Description

9 Click on the Endpoints tab button. Perform one of the following:

a Manually enter the following parameters for Endpoint A and B.

- Site ID
- Path ID
- Precedence
- Administrative State
- Control Tag (Outer Encapsulation Value)
- Control Tag (Inner Encapsulation Value)
- Member Port

Note — Path endpoints cannot be administratively enabled for Release 8.0 and later NEs if the following are true:

- An operationally up same-fate SAP on the Ethernet Tunnel Endpoint does not have a tag configured for the Path Endpoint.
- The Control Tag or Member Port parameters are not configured.

b Select an available path endpoint on endpoints A and B.

i Click on the Select button in the Path Endpoint section. The Select Path Endpoint window opens.

ii Click on the Search button and select an available endpoint.

iii Click OK. The endpoint parameters are automatically populated.

Note — To delete an Ethernet tunnel path endpoint click on the Search button to display a list of endpoints, select an endpoint, then click on the Delete button.

10 Click on the Intermediate Services tab button to view and specify the intermediate services for the Ethernet path. The services that you add to the list (or that already appear there) are in the order of proceeding from Endpoint A to Endpoint B. Perform the following to add an intermediate service:

i Click on the Add button. The Select Service window opens.

ii Click on the Search button to display a list of intermediate services available to include in this path. Only VLL services can be included.

iii Select the required service and click on the OK button.

The Select Service window closes and the service you chose is displayed in the list on the Intermediate Services tab page.

Note — 5620 SAM does not perform a validation to confirm whether the selected service is actually along the path between the two path endpoints.

iv Repeat steps i to iii to add another intermediate service, if required.

Note 1 — If you have an intermediate service highlighted in the list and want to add another service immediately above it, click on the Insert Component button rather than the Add button. The Add button places an additional service at the bottom of the list, whereas the Insert Component button places it directly above a highlighted service.

Note 2 — You can change the ordering of intermediate services in the list by selecting a particular service and using the Move Up or Move Down buttons.

11 Click on the CFM Continuity Check tab button to configure a CFM Continuity Check test for each path.

It is mandatory to have the following steps completed before selecting a test:

- Create a Maintenance Domain. The Name Type must be None. See chapter 76 for more information.
- Create a CFM Continuity Check Test. See Procedure 35-4 for information.

12 Click on the Select button. The Select CFM Test window opens.

13 Click on the Search button to list the available CFM tests. Select a CFM test.

14 Click on the OK button. The CFM Test is listed and the MEP Auto Creation checkboxes are activated.

15 Perform one of the following:

a Enable one of the MEP Auto Creation buttons:

i Click on the Run Continuity Check Protocol button to create Maintenance Associations and local and remote MEPs. Any existing Remote MEPs that do not match the local MEPs are deleted. MEPs are turned up and CCM Messages are enabled, and the control MEP property is set on the MEPs.

ii Click on the Create MEPs button to create local MEPs. Any existing Remote MEPs that do not match the local MEPs are deleted.

b Continue to step 16 and select the Run Continuity Check Protocol button or Create MEPs button at a later date.

16 If required, click on the MEP tab button to display the MEP form and select the check box to set the Control MEP parameter.

17 Click on the OK button. The Ethernet Tunnel window is displayed with the new Path information.

18 If the Protection Type parameter in step 4 was set to G8031 1:1, then repeat steps 7 to 17 for the other path.

19 If the Protection Type parameter in step 4 was set to Load Sharing, then repeat steps 7 to 17 for all paths.

20 Click Apply. The Path Id, Operational State, and CC Protocol State are updated and the path endpoints with this specific configuration are sent to the NEs.

Note — The CC protocol state appears under the global path (in the component tree and on the CFM Continuity Check form). The CC protocol state displays the state of the continuity check protocol running between the MEPs of the two endpoints of the path.

21 Click OK. A dialog box appears.

22 Click Yes to close the Ethernet Tunnel (Create) form.

Procedure 30-7 To create or configure an Ethernet Ring Element

This procedure describes how to create a new Ethernet Ring Element or configure an existing one.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 If you are configuring an existing Ethernet Ring Element, go to step 8.

3 Click on the Create button.

4 Click on Ethernet Ring Element on the contextual menu.

5 Choose a site from the Select Network Elements window to create an Ethernet Ring Element.

Note — You can create multiple ring elements at this point if you select more than one site here.

6 Click on the OK button. The Ethernet Ring Element (Create) form opens with the General tab displayed.

7 Go to step 10.

8 Select Ethernet Ring Element (Ethernet Ring) on the drop-down menu in the Manage Service Tunnels window. Click on the Search button to display a list of the existing ring elements.

9 Select the ring element you want to configure and click on the Properties button.

The Ethernet Ring Element (Edit) form opens with the General tab displayed.

10 Configure the following parameters:

- ID
- Auto-Assign ID
- Site ID
- Description
- Administrative State
- CCM Hold Time Down (deciseconds)
- CCM Hold Time Up (deciseconds)
- Guard Time (deciseconds)
- Revert Time (seconds)
- Ring Protection Link Type
- Ring Node ID

The ID and Site ID are only configurable when you are creating a new Ethernet Ring Element.

11 Click on the Path Endpoints tab button to configure the Path Endpoints.

12 Perform one of the following:

a If you are configuring an existing Ethernet Ring Path Endpoint, select the required path endpoint from the list and click Properties. The Ethernet Ring Path Endpoint (Edit) form opens with the General tab displayed.

b If you are configuring a new Ethernet Ring Path Endpoint, click on the Add button. The Ethernet Ring Path Endpoint (Create) form opens with the General tab displayed.

13 Configure the following parameters for each Path Endpoint.

- Path ID
- Description
- Administrative State
- Path Endpoint Type

The Path ID parameter is only configurable when you are creating a new Ethernet Ring Path Endpoint.

14 If you are configuring an existing Ethernet Ring Path Endpoint, go to step 22.

15 Click on the Port tab.

16 Click on the Select button. The Select Member Port window opens.

17 Click on the Search button to list the available ports. Choose the port to use for the Ethernet ring path endpoint.

18 Click on the OK button. The Ethernet Ring Path Endpoint (Create) form displays the selected member port.

19 Configure the parameters:

- R-APS Tag (Outer Encapsulation Value)
- R-APS Tag (Inner Encapsulation Value)

20 Click on the OK button. The Ethernet Ring Path Endpoint (Create) form closes.

The Path Endpoints tab displays the new Ethernet Ring Path Endpoint in the list.

21 Repeat steps 3 to 20 for the other Ethernet Ring Path Endpoint you need to create, if required.

22 Click OK. A dialog box appears.

23 Click Yes to close the Ethernet Ring Element form.

Procedure 30-8 To create an Ethernet Ring

This workflow and procedure describes how to create an Ethernet Ring and its associated Control VPLS and data services.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click on the Create button.

3 Click on Ethernet Ring on the contextual menu. The Ethernet Ring (Create) window opens.

4 Configure the following parameters:

- Mgr ID
- Auto-Assign ID
- Element ID
- Name
- Description
- Hold Time Down (deciseconds)
- Hold Time Up (deciseconds)
- Revert Time (seconds)
- Guard Time (deciseconds)

5 Click on the Apply button. The Ethernet Ring (Edit) window opens with the General tab displayed.

6 Click on the Components tab button.

7 Right click on Ring Elements and choose one of the following items from the contextual menu.

a Create Ethernet Ring Element.

i Perform steps 5 to 20 in Procedure 30-7 to create an Ethernet Ring Element.
When you are done, the element will be displayed on the Components tab in Ethernet Ring form.

Note 1 — You must create a ring element for each site that will be part of the ethernet ring.

Note 2 — The ethernet ring can only have one element configured as an RPL owner and one element configured as an RPL neighbor. This is configured using the element's Ring Protection Link Type parameter.

Note 3 — The parameter values specified in step 4 are initially populated in the Ethernet Ring Element form when creating a ring element from the Components tab. However, you can change these as required.

ii Repeat step i to create the other required ring elements.

Note — You can create all the ring elements required for the ring in one step. See step 5 in Procedure 30-7.

iii Go to step 8.

b Add Existing Element.

i The Select Element window opens.

ii Click on the Search button and select an element.

iii Click OK.

The element will be displayed on the Components tab in Ethernet Ring form.

Note 1 — You must select a ring element for each site that will be part of the ethernet ring.

Note 2 — The ethernet ring can only have one element configured as an RPL owner and one element configured as an RPL neighbor. This is configured using the element's Ring Protection Link Type parameter.

Note 3 — When you add an existing Ethernet endpoint, the parameter values specified in step 4 are not populated into the properties of that endpoint.

iv Repeat steps i to iii to select the other required ring elements.

8 Right click on Paths and choose Create Ethernet Ring Path from the contextual menu to create a path. The Ethernet Path (Create) window opens with the General tab displayed.

Note — You must create a path for each element in the ring. Each element (site) in the ring will therefore have two endpoints (from two different paths) associated with it.

9 Configure the parameters:

- Auto-Assign ID
- ID
- Description

10 Click on the Endpoints tab button to configure the endpoints for the path.

Perform one of the following:

Note — One and only one endpoint within the entire ethernet ring must have its Ring Protection Link Type parameter configured as Ring Protection Link End. All other endpoints in the ethernet ring must have this parameter set to a value of Normal.

a Manually enter the following parameters for Endpoints A and B.

- Path ID
- Ring Protection Link Type
- Administrative State
- R-APS Tag (Outer Encapsulation Value)
- R-APS Tag (Inner Encapsulation Value)
- Member Port

Note — Path endpoints cannot be administratively enabled if:

- the R-APS Tag or Member Port parameters are not configured
- a MEP is not configured on the path endpoint

b Select an available path endpoint on endpoints A and B.

i Click on the Select button in the Path Endpoint section. The Select Path Endpoint window opens.

ii Click on the Search button and select an available endpoint.

iii Click OK. The endpoint parameters are automatically populated.

11 Click on the CFM Continuity Check tab button to configure a CFM Test for the path.

12 Click on the Select button. The Select CFM Test window opens. Perform one of the following:

a Click on the Search button to list the available CFM tests.

i Select the required CFM test.

ii Click OK.

The Select CFM Test window closes and the Global ID and ID parameters for the selected test appear on the CFM Continuity Check tab.

b Click on the Create button to create the required CFM test. The Global Maintenance Entity Group (Create) form opens, with the General tab displayed.

Note — The Initial CCM Interval for the CFM test you select or create must be set to either 10 ms or 100 ms, otherwise the subsequent MEP creation will fail. The 7210 SAS-E, 7210 SAS-M and 7210 SAS-X do not support the 10 ms value.

Refer to Procedure 35-4 for information on creating the test.

13 Click on the Intermediate Services tab button to view and specify the intermediate services for the ethernet path. The services that you add to the list (or that already appear there) are in the order of proceeding from Endpoint A to Endpoint B. Perform the following to add an intermediate service:

i Click on the Add button. The Select Service window opens.

ii Click on the Search button to display a list of intermediate services available to include in this path. Only VLL services can be included.

iii Select the required service and click on the OK button.

The Select Service window closes and the service you chose is displayed in the list on the Intermediate Services tab page.

Note — 5620 SAM does not perform a validation to confirm whether the selected service is actually along the path between the two path endpoints.

iv Repeat steps i to iii to add another intermediate service, if required.

Note 1 — If you have an intermediate service highlighted in the list and want to add another service immediately above it, click on the Insert Component button rather than the Add button. The Add button places an additional service at the bottom of the list, whereas the Insert Component button places it directly above a highlighted service.

Note 2 — You can change the ordering of intermediate services in the list by selecting a particular service and using the Move Up or Move Down buttons.

14 Click OK. A dialog box appears.

15 Click Yes to close the Ethernet Ring (Create) form.

16 Create a Control VPLS for the ethernet ring.

i Perform Procedure 68-1 to create the VPLS, just as you would create a regular VPLS.

ii Perform Procedure 68-3 to create an L2 Access Interface for each path endpoint in the ethernet ring. Each site in the Control VPLS must therefore have two control L2 Access Interfaces.

When creating the L2 access interfaces, ensure the following requirements:

- The Terminating Port and Encap Type must have the same values used to create the particular path endpoint in step 10.
- The Outer Encapsulation Value and Inner Encapsulation Value for the port in each L2 Access Interface must be set to the same value as the R-APS Tag (Outer Encapsulation Value) and R-APS Tag (Inner Encapsulation Value) respectively that you used for the particular path endpoint in step 10. This defines the interface as a Control SAP for the ethernet ring.

17 Create the VPLS data services required for the Ethernet Ring.

i Perform Procedure 68-1 to create the VPLS, just as you would create a regular VPLS. The VPLS data service must be a regular VPLS, I-VPLS, or B-VPLS type.

ii Perform Procedure 68-3 to create an L2 Access Interface for each path endpoint in the ethernet ring. Each site in the VPLS data service must therefore have at least two L2 Access Interfaces.

When creating the L2 access interfaces, the Terminating Port and Encap Type must have the same values used to create the particular path endpoint in step 10.

Procedure 30-9 To manage IP/MPLS service tunnels

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens

2 Configure the filter criteria and click on the Search button. A list of service tunnels is displayed.

3 Select a service tunnel in the list and click on the Properties button. The Tunnel (Edit) form opens with the General tab displayed.

4 Configure the parameters on the General tab, as required.

5 View the States and State Cause indicators for valuable troubleshooting information, for example, a failed OAM diagnostic.

6 Click on the tab buttons to view information or modify the parameters.

Note — The following tab buttons are not available if the source is a 7250 SAS-ES:

- Tests
- Maintenance
- Accounting
- Statistics

7 Save the changes and close the Tunnel (Edit) form.

8 Close the Manage Service Tunnels form.

Procedure 30-10 To run an OAM validation test

An OAM validator test suite must be created for the tested entity. See chapter 75 for more information about how to create an OAM validator test suite.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens

2 Configure the filter criteria and click on the Search button. A list of service tunnels is displayed.

3 Select a service tunnel in the list and click on the Properties button. The Tunnel (Edit) form opens with the General tab displayed.

4 Click on the Validate button.

If an OAM validator test suite is not associated to the service tunnel, a dialog box appears. Perform the following steps:

i Click on the OK button to associate the service tunnel with an existing OAM validator test suite. The Choose Validator Test Suite form appears.

ii Configure the filter criteria. A list of OAM validator test suites appears.

iii Select a OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab button.

7 Click on the Validation Result tab button.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab button to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise, go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result (Edit) form.

14 Close the Tunnel (Edit) form.

15 Close the Manage Service Tunnels form.

Procedure 30-11 To view the service tunnel topology

1 Choose Application→Service Tunnel Topology from the 5620 SAM main menu. The Service Tunnel Topology map opens.

2 View the topology map as required. See chapter 4 for information about using topology maps.

3 Close the topology map.

31 — Lawful Intercept

31.1 Overview

Lawful Intercept, or LI, is a term that describes the interception and monitoring of network subscriber traffic by authorized agencies for law-enforcement purposes. A subscriber whose traffic is intercepted using LI is called a target. LI target traffic is replicated by a service mirror that uses subscriber information as the match criteria. LI has the following characteristics.

- LI is not detectable by a target subscriber.
- LI-related traffic is delivered separately from other network traffic.
- LI-related alarms only appear for authorized LI users.
- LI configuration information is stored in a separate and encrypted file.
- LI uses SSL security for data encryption, server authentication and message integrity between the 5620 SAM server and the single-user GUI clients or client delegate servers.

LI functions are managed separately from other 5620 SAM functions. LI mirroring is a special type of service mirroring that requires the following:

- on each LI NE in a mirror service:
  - SSH user security
  - an LI user profile
  - a user account that has LI privileges
- on the 5620 SAM:
  - SSL on the single-user GUI clients, client delegate servers and JMS server
  - a user account that has LI privileges
  - an assigned liMgmt scope of command role
  - an LI mediation policy

LI management requires a dedicated user authorization level. The 5620 SAM LI configuration forms, parameters, mirror services, and mirrored traffic appear only for a user with LI privileges, who can perform the following:

- create, configure, and view LI sources that use IP, MAC, SAP, and subscriber filters
- view LI-related alarms
- configure LI mediation policies
- modify the LI user password

Caution — An LI user password cannot be modified unless it is known. When an LI user password is not known, the LI user account is unavailable.

See chapter 69 for more information about mirror service management. See chapter 8 for more information about user privileges and scope of command roles.

Security

The 5620 SAM admin user, or an operator with an assigned admin scope of command role, must create an LI user account to be used for LI configuration. A user with the admin scope of command can perform only the following LI functions:

- Create an LI user scope of command profile and associate a non-admin user account with the LI profile.
- Configure an LI user profile that is restricts the LI user to LI activities only and does not allow system administrator activities.
- Create a password for the LI user.
- Configure CLI and SNMP access for the LI user account.

The 5620 SAM admin user cannot perform the following LI functions:

- Assign LI privileges to a user that is associated with the admin profile.
- View LI-related alarms.
- Delete an LI user.
- View, create, modify, or delete LI objects.
- View or modify LI mediation policies.

The following conditions apply to LI users and LI user groups:

- LI configuration requires the liMgmt scope of command role.
- The liMgmt role can be assigned to only one scope of command profile.
- A scope of command profile that has an assigned liMgmt role can include other roles except for the admin role.
- You cannot change the scope of command profile assignment for a user group when the profile includes the liMgmt role.
- An LI user group must be created as an LI user group; you cannot change a non-LI user group to an LI user group
- You cannot change an LI user group to a non-LI user group.
- A user account can have the liMgmt or the admin role, but not both.
- A user that belongs to an LI user group cannot be changed to a non-LI user.
- An LI span of control profile restricts LI user access to specific NEs.

31.2 Workflow to configure LI

The following is the sequence of high-level activities required to configure LI for the 5620 SAM.

1. Enable SSH security on each NE that is to perform an LI function. For more information about configuring SSH, see chapter 13.

2. Enable SSL security between the 5620 SAM main server and single-user GUI clients, and between the 5620 SAM main server and client delegate servers. For more information about configuring SSL security, see chapter 9.

3. Plan the 5620 SAM LI user-account creation according to the requirements for LI user access to other 5620 SAM functional areas.

4 As the 5620 SAM admin user, perform the following steps to create an LI user on the 5620 SAM. See Procedure 31-1 for more information.

   i Create a 5620 SAM LI scope of command profile that has an assigned liMgmt role.

   ii Create a 5620 SAM LI user group that is associated with the new scope of command profile.

   iii Create a 5620 SAM LI user account and assign it to the new user group.

5 Provide the credentials for the 5620 SAM LI user account to the authorized LI administrator, or LI user.

6 The LI user changes the password of the 5620 SAM LI user account so that it is unknown to the 5620 SAM admin user.

7 As the NE admin user, perform the following steps using a CLI to create an LI user on the NE.

   i Create an LI user profile on the NE. See Procedure 31-2 for information about creating an NE user profile using a CLI.

   ii Create an LI user account on the NE that is associated with the LI user profile. See Procedure 31-3 for information about creating an NE user account using a CLI.

8 Provide the credentials for the LI NE user account to the LI user.

9 The LI user changes the password of the LI NE user account so that it is unknown to the NE admin user. See Procedure 31-4 for more information.

10 The LI user creates a 5620 SAM LI mediation policy for the NE that uses SSH for CLI sessions and secure file transfers. See Procedure 31-5 for more information.

11 The LI user specifies whether the NE stores the LI source configuration locally or reconfigures the LI sources after a reboot. See chapter 9 for information about saving LI source configurations.

12 The LI user uses the 5620 SAM to enable NE discovery for LI. See Procedure 31-6 for more information.

13 Configure LI mirror services. See chapter 69 for information about configuring mirror services.

14 View LI user and system logs, as required.

31.3 5620 SAM LI configuration procedures

This section describes how to configure LI on the 5620 SAM and on an NE.

Procedure 31-1 To create an LI user account on the 5620 SAM

Note — You require 5620 SAM admin user privileges to perform this procedure.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab button.

3 Choose Profile (security) from the object drop-down list.

4 Click on the Create button. The Scope of Command Profile (Create) form opens with the General tab displayed.

5 Configure the parameters:

- Auto-Assign ID
- Profile ID
- Profile Name
- Description

6 Assign one or more scope of command roles to the profile. Perform the following steps.

i Click on the Roles tab button.

ii Click on the Add button. The Select Scope Of Command Role(s) - ScopeOfCommandProfile form opens.

iii Select one or more roles to include in the scope of command profile.

Note 1 — One of the roles you choose must be the liMgmt role.

Note 2 — You cannot include the admin role in an LI scope of command profile.

Note 3 — The 5620 SAM allows the creation of only one scope of command profile that contains the liMgmt role.

iv Click on the OK button. The Select Scope of Command Role(s) - ScopeOfCommandProfile form closes and a dialog box appears.

v Click on the OK button.

vi Click on the OK button. The Scope of Command Profile (Create) form closes.

7 Click on the User Groups tab button.

8 Click on the Create button. The User Group (Create) form opens with the General tab displayed.

9 Configure the parameters:

- User Group
- Description
- User Group State
- Apply Local Authentication Only
- Account Expiry
- Password Expiry
- Override Global Timeout
- Client Timeout (minutes)

10 Perform the following steps to assign the new LI scope of command profile to the user group.

i Click on the Select button beside the Profile ID field in the Scope of Command panel. The Select Scope of Command Profile - User Group form opens.

ii Select a profile from the list and click on the OK button. The Select Scope of Command Profile - User Group list form closes and the User Group (Create) form is refreshed with the scope of command profile information.

11 Perform the following steps to assign a span of control profile to the user group.

i Click on the Select button beside the Profile ID field in the Span of Control panel. The Select Span of Control Profile - User Group form opens.

ii Select a profile from the list and click on the OK button. The Select Span of Control Profile - User Group list form closes and the User Group (Create) form is refreshed with the span of control profile information.

12 Click on the OK button. The User Group (Create) form closes and the 5620 SAM User Security - Security Management (Edit) form reappears.

13 Click on the Users tab button. The User (Create) form opens.

14 Configure the parameters:

- User Name
- Description
- User State
- E-mail Address
- First Time Login Password Change
- User Password
- Confirm Password
- Valid Client IP address
- Enable IP Address validation

15 Perform the following to associate the user with the newly created LI user group.

i Click on the Select button beside the User Group parameter. The groupName - User list form opens.

ii Choose the new LI user group from the list and click on the OK button. The groupName - User list form closes and the User (Create) form is refreshed with the user group information.

16 Click on the OK button. The User (Create) form closes and the 5620 SAM User Security - Security Management (Edit) form reappears.

17 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 31-2 To create an NE LI user profile using CLI

Note — You require NE admin user privileges to perform this procedure.

1 Open an SSH session on the NE as described in chapter 14.

2 Enter the following commands in sequence at the prompt to create an NE user profile. The following is a sample configuration:

```
configure system security profile li-prof ↵
default-action deny-all ↵
li ↵
 entry 10 ↵
 match "configure li" ↵
 action permit ↵
 exit ↵
 entry 20 ↵
 match "exit" ↵
 action permit ↵
 exit ↵
 entry 30 ↵
 match "help" ↵
 action permit ↵
 exit ↵
 entry 40 ↵
 match "back" ↵
 action permit ↵
 exit ↵
 entry 50 ↵
```

```
match "show li" ↵
action permit ↵
exit ↵
entry 60 ↵
match "info" ↵
action permit ↵
exit ↵
entry 70 ↵
match "configure system security user" ↵
action permit ↵
exit ↵
entry 80 ↵
match "admin save" ↵
action permit ↵
exit ↵
exit ↵
admin save ↵
```

3 Close the SSH session.

4 Right-click on the NE in the 5620 SAM topology map and choose Resync from the contextual menu to update the NE configuration in the 5620 SAM.

Procedure 31-3 To create an LI user account on an NE using a CLI

Note — You require NE admin user privileges to perform this procedure.

1 Open an SSH session on the NE as described in chapter 14.

2 Enter the following commands in sequence at the prompt to create an LI user:

```
configure system security snmp ↵

access group LI_group security-model usm security-level privacy
context li exact read li-view write li-view notify iso ↵

exit all ↵

configure system security user LI_username ↵

password LI_password ↵

access console li snmp ↵

snmp group LI_group ↵

console member LI_profile ↵

console no member default ↵

exit all ↵

admin save ↵
```

where
LI_usename is the name of the LI user account on the NE
LI_password is the password for the LI user account on the NE
LI_group is the name of the LI user group on the NE
LI_profile is the name of an LI user profile; see Procedure 31-2 for information about creating an LI user profile

3 Close the SSH session.

4 Right-click on the NE in the 5620 SAM topology map and choose Resync from the contextual menu to update the NE configuration in the 5620 SAM.

Procedure 31-4 To configure NE LI user security

Perform this procedure to change the password for an LI user account on an NE and to configure LI user authentication and SNMP data encryption on the NE.

Note — You require NE LI user privileges to perform this procedure.

1 Use the NE LI user account to open an SSH session on the NE. See chapter 14 for information about opening an SSH session on an NE.

2 Enter the following command to obtain the SNMP engine ID of the NE.

`show system info` ↵

The SNMP engine ID is displayed.

3 Record the SNMP engine ID for use in the following steps.

4 Log in to a 5620 SAM main server, client delegate server, or single-user client station using an appropriate user account.

Note 1 — If you are logging on to a 5620 SAM main server on Solaris or a client delegate server station, you must log in as the samadmin user.

Note 2 — If you are logging on to a 5620 SAM single-user client station, you must log in as a local administrator or as the user that installed the client.

5 Open a console window.

6 Navigate to the *install_dir*/nms/bin directory

where *install_dir* is the 5620 SAM installation location, typically /opt/5620sam/server or /opt/5620sam/client on Solaris, or C:\5620sam\server or C:\5620sam\client on Windows

7 Perform the following steps to generate an MD5 authentication key for the NE LI user account. An authentication key is used to create an encrypted authentication password.

i Perform one of the following.

- If the 5620 SAM server is installed on Solaris, enter the following at the CLI prompt:

`./nmsclient.bash MD5 password engine_ID` ↵

- If the 5620 SAM server is installed on Windows, enter the following at the CLI prompt:

`nmsclient.bat MD5 password engine_ID` ↵

where
password is the ASCII password string used to generate the key
engine_ID is the SNMP engine ID obtained in step 2

The utility generates the authentication key.

ii Record the key value for use later in the procedure.

8 Perform the following steps to generate an MD5 DES privacy key for the NE LI user account. A DES privacy key is used to encrypt the SNMP packets for additional security.

i Perform one of the following.

- If the 5620 SAM server is installed on Solaris, enter the following at the CLI prompt:

./nmsclient.bash MD5 *password engine_ID* ↵

- If the 5620 SAM server is installed on Windows, enter the following at the CLI prompt:

nmsclient.bat MD5 *password engine_ID* ↵

where
password is the ASCII password string used to generate the key
engine_ID is the SNMP engine ID obtained in step 2

The utility generates the DES privacy key.

ii Record the key value for use later in the procedure.

9 Close the console window.

10 Enter the following commands in sequence at the CLI prompt to change the LI user password and to configure LI security for the user account:

configure system security user *username* ↵

password *new_LI_password* ↵

snmp ↵

authentication md5 *authentication_key* privacy des-key *DES_privacy_key* ↵

exit all ↵

admin save ↵

where
LI_group is the name of the LI user group on the NE
LI_usename is the name of the LI user account on the NE
new_LI_password is the new password for the LI user account on the NE
authentication_key is the MD5 authentication key value generated for the NE LI user in step 7
DES_privacy_key is the DES privacy key value generated for the NE LI user in step 8

11 Close the SSH session.

Procedure 31-5 To configure LI mediation

Perform this procedure to create an LI mediation policy that enables the creation of source objects for an LI service mirror.

Note — You require 5620 SAM LI user privileges to perform this procedure.

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens with the General tab displayed.

2 Click on the LI Mediation tab button.

3 Click on the Add button. The LI Mediation Policy (Create) form opens.

4 Click on the Select button beside the User Name parameter to view a list of configured users. The Select Site User For SNMP Access form opens.

5 Select the NE LI user created in Procedure 31-3 from the list and click on the OK button. The user name is displayed on the LI Mediation Policy (Create) form.

6 The SNMP passwords in the 5620 SAM mediation policy must match the encrypted passwords generated for the NE LI user in Procedure 31-4. Perform the following steps to set the mediation-policy passwords.

   i Click on the Properties button. The NE User Configuration form opens.

   ii Click on the SNMPv3 tab button.

   iii Enable the Authentication Protocol parameter.

   iv Specify the password used to generate the authentication key in Procedure 31-4 for the New Authentication Password and Confirm New Auth Password parameters.

   v Enable the Privacy Protocol parameter.

   vi Specify the password used to generate the DES encryption key in Procedure 31-4 for the New Privacy Password and Confirm New Privacy Password parameters.

   vii Click on the OK button. A dialog box appears.

   viii Click on the Yes button. The NE User Configuration form closes.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The Mediation Policy (Create) form closes and the Mediation (Edit) form reappears.

9 Click on the OK button. The Mediation (Edit) form closes.

Procedure 31-6 To enable NE discovery for LI

Perform this procedure to enable LI discovery of an NE. Before you can enable LI discovery for an NE, the NE must be successfully discovered. See chapter 13 for information about configuring NE discovery.

Note — You require 5620 SAM LI user privileges to perform this procedure.

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.

2 Click on the Managed State tab button. A list of discovered NEs is displayed.

3 Choose an NE on which Procedures 31-2 and 31-3 have been performed, and click on the Properties button. The Node Discovery Control (Edit) form opens with the General tab displayed.

4 Click on the LI Mediation Security tab button.

5 Click on the Select button in the Dual Read Access Mediation Policy panel. The Configure Mediation Security - Node Discovery Control list form opens.

6 Choose the LI mediation policy created in Procedure 31-5 and click on the OK button. The Configure Mediation Security - Node Discovery Control list form closes.

7 Click on the Select button in the Dual Write Access Mediation Policy panel. The Configure Mediation Security - Node Discovery Control list form opens.

8 Choose the LI mediation policy created in Procedure 31-5 and click on the OK button. The Configure Mediation Security - Node Discovery Control list form closes.

9 Click on the Select button in the Dual Trap Access Mediation Policy panel. The Configure Mediation Security - Node Discovery Control list form opens.

10 Choose the LI mediation policy created in Procedure 31-5 and click on the OK button. The Configure Mediation Security - Node Discovery Control list form closes.

11 Click on the OK button. The Node Discovery Control (Edit) form closes and the Discovery Manager (Edit) form reappears.

12 Click on the Resync button. The Resync Options form opens.

13 Select Choose MIB Entries and click on the Next button. The Choose MIB Entries list form opens.

14 Select the TIMETRA_MIRROR_MIB entry in the list and click on the Finish button.

Note — Resynchronizing only the TIMETRA_MIRROR_MIB entry resynchronizes only LI source objects and keeps the resynchronization time to the minimum required.

15 Click on the Close button. The Resync Options form closes and the Discovery Manager (Edit) form reappears.

16 Click on the OK button. The Discovery Manager (Edit) form closes.

Procedure 31-7 To create an additional NE LI user account using the 5620 SAM GUI

Note 1 — You require 5620 SAM LI user privileges to perform this procedure.

Note 2 — Before you can perform this procedure, at least one LI user account must exist on the NE.

Note 3 — Before you can perform this procedure, a 5620 SAM LI user must enable LI discovery for the NE using Procedure 31-6.

1 Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens.

2 Click on the Create button. The NE User (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- User Name
- Description
- Access

You must specify the li, snmp, and console values for the Access parameter.

Additional configurable parameters are displayed.

4 Configure the additional parameters:

- Password
- Confirm Password
- Home Directory
- Restrict to Home
- Console Login Exec File
- Console Cannot Change Password
- Console New Password At Login

Specify an MD5 authentication key for the Password parameter. See Procedure 31-4 for information about generating a user authentication key.

5 Perform the following steps to assign a console profile, if required.

i Click on the Console Profiles tab button. The list of profiles numbered one through eight appears. A user can have up to eight console profiles.

ii Use the Select button beside one of the Profile 1 through Profile 8 parameters to choose a console profile. See chapter 18 for information about creating console profiles.

6 Click on the SNMPv3 tab button.

i Enable the Authentication Protocol parameter.

ii Specify an authentication key generated using Procedure 31-4 for the New Authentication Password and Confirm New Auth Password parameters.

iii Enable the Privacy Protocol parameter.

iv Specify a DES encryption key generated using Procedure 31-4 for the New Privacy Password and Confirm New Privacy Password parameters.

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The NE User (Create) form closes and the NE User Configuration form reappears.

7 Close the NE User Configuration form.

32 — IPsec

32.1 IPsec overview

The 5620 SAM supports the configuration of IPsec VPRN services, which are generically called IPsec VPNs. An IPsec VPN enables the secure extension of a corporate VPN over uncontrolled or untrusted private and public networks. The ISA-IPSEC MDA on the 7750 SR, Release 6.1 or later, provides IPsec tunneling and encryption between sites.

You can use the 5620 SAM to configure IPsec sessions and the security associations that are required in a bi-directional IPsec tunnel. You can configure multiple IPsec tunnels for a VPRN.

5620 SAM IPsec session configuration supports the following:

- encryption methods such as DES, 3DES, AES-128, AES-192, and AES-256
- authentication and hashing methods such as HMAC-MD5 and HMAC-SHA1
- key distribution methods such as IKE shared secret with PFS, and manual exchange
- key generation algorithms such as Diffie-Helman
- IPsec modes
- shared secret authentication
- NAT traversal
- DPD for the IPsec tunnel

An IPsec VPN service includes IPsec tunnels that terminate on IES or VPRN IPsec gateways. These gateways support L3 forwarding through an interface that connects to an IPsec tunnel. You can use the 5620 SAM to configure VPRN services to which individual hosts connect over the Internet to an IES or VPRN IPsec gateway. You can configure one or more IPsec interfaces in a VPRN service, and can configure multiple tunnel security profiles for each IPsec interface.

IKE policies are used to negotiate IPsec security associations, or SAs, between IPsec peers. AN SA is a relationship between two or more IPsec peers that defines how the peers communicate securely. IKE policies are exchanged between IPsec peers to negotiate a secure communication channel; they specify how traffic is encrypted between source and destination sites in an IPsec VPN by establishing a shared security policy using authentication keys.

IPsec transform policies specify the protocol for the IPsec authentication header and the encryption protocol for the encapsulating security payload, or ESP, and define the attributes that are used to secure the data.

After an IPsec peer initiates an IPsec session, there are two main phases:

- authentication and protection of IPsec peer identities and negotiation of matching IKE SA policies between peers to establish a secure channel for negotiating IPsec SAs in the next phase
- IPsec SA parameter negotiation and establishment of matching peer SAs

After the second phase, the IPsec peers exchange data over the IPsec tunnel according to the IPsec parameters in the IKE and IPsec transform policies.

You can create a tunnel template to configure shared IPsec transforms and IKE policies. Each IPsec peer configuration can include the following:

- one or more configured IPsec transforms
- one IKE policy
- one unique IPsec tunnel
- one tunnel filter defined in the IPsec tunnel configuration

Each IPsec tunnel between IKE peers is identified by a unique remote peer IP address or a unique local IP address.

You can use the IPsec Application Function Manager to create and manage end-to-end IPsec components to form a secure VPN. See section 32.2 for more information.

The 5620 SAM OSSI supports IPsec VPN configuration.

IPv6 IPsec

OSPFv3 authentication requires IPv6. IPv6 IPsec requires the following:

- IPsec transport mode —required because the NE acts as an OSPFv3 authentication host
- IPsec static security association—defines the SPI values, algorithms, protocol and keys to be used, and requires the same configuration at each end of the tunnel
- AH and ESP
- MD5 and SHA1

BFD

You can use BFD for static LAN-to-LAN IPsec tunnels on the 7750 SR-c4, 7750 SR-7, 7750 SR-12, and 7750 SR-c12. The following is the configuration information for implementing BFD over static LAN-to-LAN IPsec tunnels:

- You can have only one BFD session between a source/destination address pair.
- Each tunnel can be associated with only one BFD session. However, one or more tunnels, to a maximum of 500, can be associated with same BFD session.
- If one BFD session is associated with multiple tunnels, the tunnel that carries the BFD traffic must be operationally up before any of the other tunnels can be operationally up.
- When the 5620 SAM does not receive BFD packets from a peer before the detection time expires or a signal down notification is sent from a remote peer, the BFD session is considered down. When the 5620 SAM sets the associated IPsec tunnels in a down state, 5620 SAM performs the following:
  - sends a Delete Payload message to each remote peer from each associated tunnel and SA
  - removes the state and table entries from each associated tunnel and SA

32.2 IPsec VPN

You can create and manage the association between IPsec components, public and private services, to form a secure VPN. See "Typical applications for IPsec corporate services" in this section for the typical applications of an IPsec VPN.

You use the IPsec VPN step forms to perform the following:

- Configure the corporate service type.
- Enable the link between the corporate and secure service.
- Choose an NE service site.
- Configure the secure VPRN service.
- Configure the delivery service.
- Choose the IPsec group.
- Create the policy.
- Deploy the IPsec VPN.

Tunnel types

Table 32-1 lists the tunnel types that you can create for an IPsec VPN.

Table 32-1 Tunnel types

Tunnel type	7750 SR, Release 6.0	7750 SR, Release 7.0 or later	7210 SAS
Dynamic (site-to-site)		✓	
Dynamic (soft client)		✓	
Static	✓	✓	✓

The 5620 SAM creates the following after the successful creation of an IPsec VPN, regardless of the tunnel type:

- a secure VPRN service and NE sites
- the IES or VPRN delivery service and NE sites
- if you specify that the secure and corporate services are to be linked, a composite service that contains the corporate and secure services

The 5620 SAM performs specific configuration actions after the successful creation of an IPsec VPN, depending on the tunnel type. See Procedures 32-15 to 32-17 for more information.

Typical applications for IPsec corporate services

Figure 32-1 shows one public L3 VPRN service that is associated with the corresponding private VPRN service. The private VPRN service belongs to a larger private VPRN. The public service can be a VPRN or IES service. The private service can only be a VPRN service.

Figure 32-1 Static IPsec tunnel

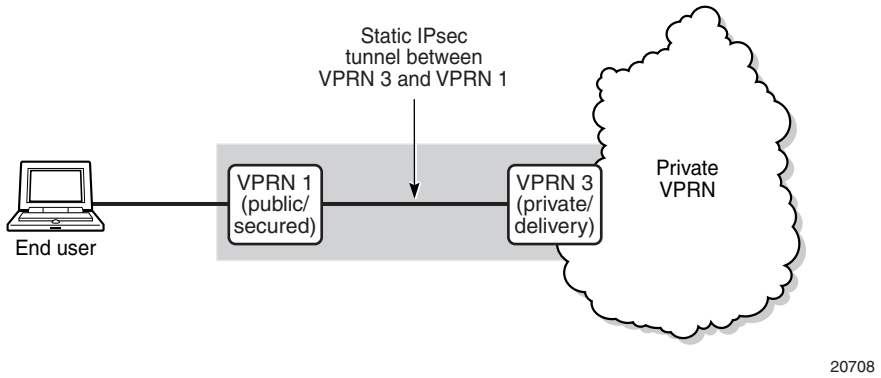


Figure 32-2 shows two public L3 VPRNs, VPRN 1 and VPRN 2, which are connected to the private, secure service VPRN 3 through an IPsec gateway. The public services can be VPRN or IES services. The private service can only be a VPRN service.

Figure 32-2 IPsec tunnels for a site

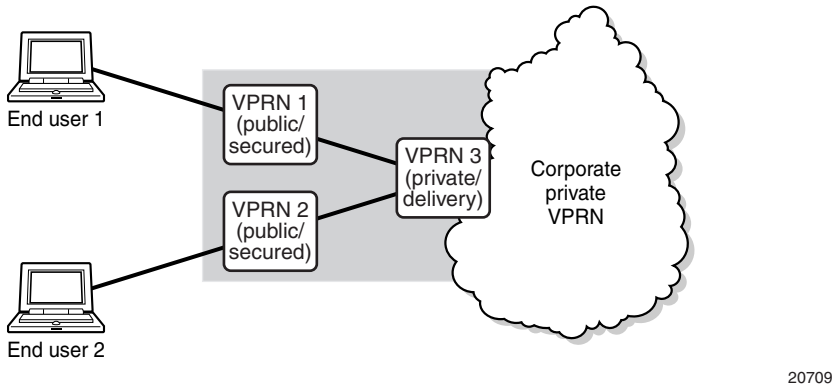


Figure 32-3 is the same as Figure 32-1, but Figure 32-3 shows IPsec tunnels across multiple sites. Site A, Site B, and Site C are part of the private service VPRN 4. For the site, there is a secure IPsec tunnel between a public service and a private service. The public services can be L3 VPRN or L3 IES services. The private service can only be a VPRN service.

Figure 32-3 IPsec tunnels for multiple sites

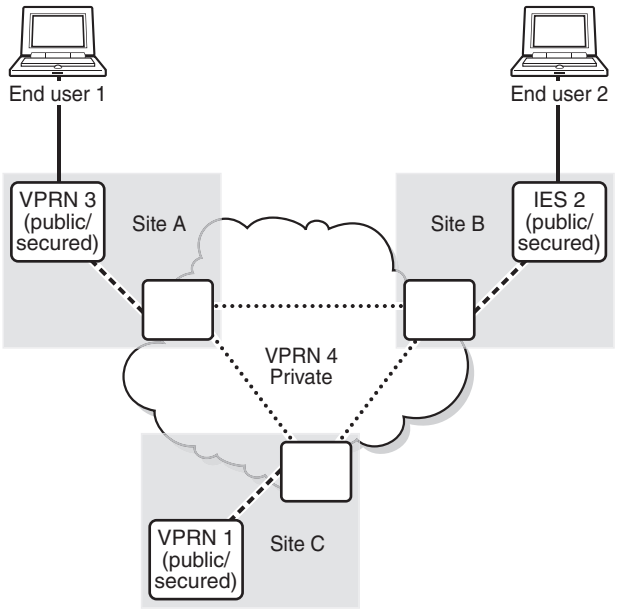
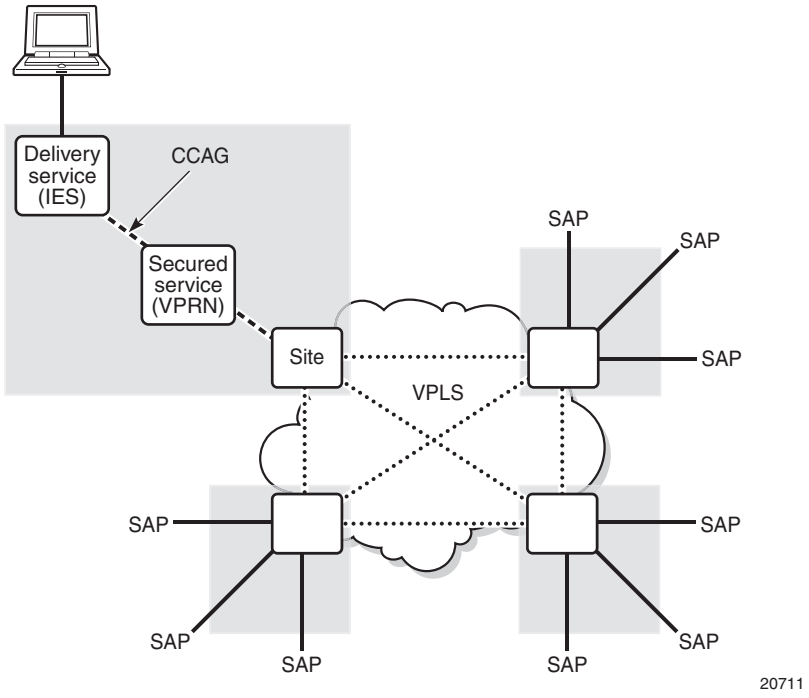


Figure 32-4 shows a private VPRN that is connected to a corporate network and a VPLS that is the corporate network. The public IES and private VPRN service are connected to VPLS network through a CCAG or SCP. CCAG connects the private VPRN to the VPLS network.

Figure 32-4 IPsec VPN in a corporate network

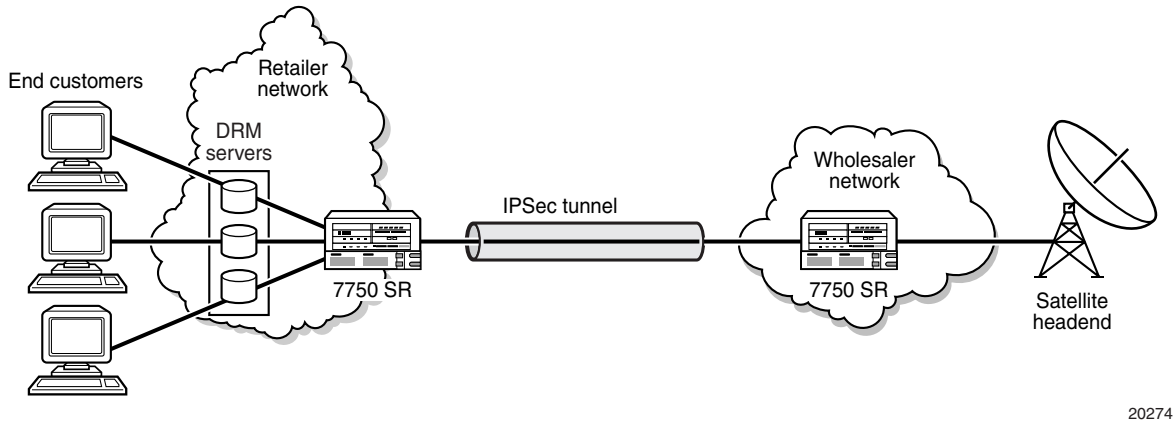


32.3 Sample video wholesale IPsec configuration

Larger providers or a cooperative of smaller providers often unite to provide a video headend to avoid the costs of investing in a satellite headend locations on their own ground station, to provide tripleplay features. Each retail subscriber can purchase content from this single station and receive it over IP. However, encryption is required so that the signal cannot be understood if intercepted.

Figure 32-5 shows a sample video wholesale configuration with a high-speed encrypted tunnel.

Figure 32-5 Sample video wholesale configuration



32.4 Workflow to configure and manage an IPsec configuration

See section 32.5 for the workflow to configure and manage an IPsec configuration using the IPsec VPN step forms.

1. Provision the ISA-IPSEC MDA on the 7750 SR, Release 6.1 or later. See chapters 15 and 17 for more information about IPsec equipment configuration.
   - i. Create or configure ISA-IPsec groups.
   - ii. Assign the active and backup IPsec group members to the ISA-IPsec groups.
2. Configure IKE policies.
3. Configure IPsec transform policies.
4. Configure IPsec tunnel templates.
5. Create a VPRN.
   - i. Configure the IPsec security policy.
   - ii. Configure the IPsec security policy entries.
6. Create the private-facing IPsec interface on the VPRN.
   - i. Create a private IPsec SAP.
   - ii. Configure ingress and egress policies.
7. Create the public side of the IPsec service.
   - i. Create an L3 access interface on an IES or VPRN.
   - ii. Define the IPsec public SAP for the L3 access interface.
   - iii. Specify the IPsec gateway, if required, on the 7750 SR, Release 7.0 or later.

8 Create IPsec tunnels on the VPRN IPsec interface.

   i Create one or more IPsec tunnels.

   ii Configure the manual or dynamic keying.

9 Configure the static route.

32.5 Workflow to configure and manage an IPsec configuration using the IPsec VPN

1 Create a corporate service. See Table 32-2.

2 If required, configure service templates for one site. See Table 32-2 and the *5620 SAM Scripts and Templates Developer Guide* for more information.

3 Configure the service type for an IPsec VPN, and if required, enable the linking of the corporate and secure service to create a composite service.

4 Select the NE service sites for the IPsec VPN.

5 Create or select the secure VPRN service for the IPsec VPN.

6 Create or select the delivery service for the IPsec VPN.

7 Select the IPsec group for the IPsec VPN.

8 Create the policy for the IPsec VPN.

9 Deploy the IPsec VPN.

32.6 Workflow to enable BFD over a static LAN-to-LAN IPsec tunnel

1 Create an IPsec interface on a VPRN, as described in Procedure 32-6.

2 Create an IPsec tunnel on the VPRN IPsec interface, as described in Procedure 32-8.

3 Enable BFD for the static LAN-to-LAN IPsec tunnel, as described in Procedure 32-9.

4 Assign a BFD service and interface that can be used for the BFD session on the IPsec tunnel.

32.7 General IPsec procedures

The following procedures describe how to perform general 5620 SAM IPsec configuration tasks, such as policy creation. See section 32.8 for IPsec VPN procedures.

Procedure 32-1 To configure an IKE policy

1 Choose Policies→ISA Policies→IKE from the 5620 SAM main menu. The IKE Policy form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy, if required, and click on the Search button. Choose a policy from the list and click on the Properties button. The IKE Policy (Edit) form opens with the General tab displayed.

b Click on the Create button. The IKE Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- ID
- Description
- Mode
- Diffie-Hellman(DH) Group
- Perfect Forward Secrecy (PFS)
- PFS DH Group
- Authentication Algorithm
- Authentication Method
- Encryption Algorithm
- Internet Security Association and Key Management Life Time (seconds)
- IPSec Life Time (seconds)

4 Click on the NAT Traversal tab button.

5 Configure the parameters:

- NAT Traversal
- Keep Alive Interval
- Force Keep Alive

6 Click on the DPD tab button.

7 Configure the parameters:

- Dead Peer Detection (DPD)
- Interval
- Max Retries

The Interval and Max Retries parameters are not configurable if the Dead Peer Detection (DPD) parameter is set to Disabled.

8 Click on the Apply button.

9 Click on the General tab button.

10 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the network elements. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions.

Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears. Click on the Yes button. The configuration mode of the policy is changed to Released.

11 Close the IKE Policy (Create) form.

12 Close the IKE Policy form.

Procedure 32-2 To configure an IPsec transform

1 Choose Policies→ISA Policies→IPSec Transform from the 5620 SAM main menu. The IPSec Transform form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy, if required, and click on the Search button. Choose a policy from the list and click on the Properties button. The IPSec Transform (Edit) form opens with the General tab displayed.

b Click on the Create button. The IPSec Transform (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Description
- Authentication Algorithm
- Encryption Algorithm

4 Click on the Apply button.

5 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the network elements. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions.

Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears. Click on the Yes button. The configuration mode of the policy is changed to Released.

6 Close the form.

7 Close the IPSec Transform form.

Procedure 32-3 To create an IPsec static security association

1 Choose Policies→ISA Policies→IPSec Static Security Association from the 5620 SAM main menu. The IPSec Static Security Association Policies form opens.

2 Click on the Create button. The IPsec Static Security Association (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Static SA Name
- Direction
- Protocol
- Authentication Algorithm
- Authentication Key Type
- Authentication Key
- Security Parameter Index
- Static SA Description

4 Click on the Apply button.

5 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the network elements. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions.

Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears. Click on the Yes button. The configuration mode of the policy is changed to Released.

6 Close the form.

7 Close the IPsec Static Security Association (Create) form.

Procedure 32-4 To create an IPsec tunnel template

1 Choose Policies→ISA Policies→IPSec Tunnel Template from the 5620 SAM main menu. The IPSec Tunnel Template Policies form opens.

2 Click on the Create button. The IPSec Tunnel Template (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Description
- Reverse Route
- Replay Window

4 Click on the IPSec Transforms tab button.

5 Click on the Select button in the Transform ID 1 to Transform ID 4 panels. The Select Transform ID *1_4* IPSec Tunnel Template list form opens.

6 Choose an entry and click on the OK button. The Select Transform ID *1_4* IPSec Tunnel Template list form closes.

7 Click on the General tab button.

8 Click on the Apply button.

9 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the network elements. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions.

Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears. Click on the Yes button. The configuration mode of the policy is changed to Released.

10 Close the form.

11 Close the IPSec Tunnel Template form.

Procedure 32-5 To create an IPsec security policy

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Sites tab.

6 Choose an entry and click on the Properties button. The VPRN Site (Edit) form opens with the General tab displayed.

7 Click on the IPSec Security Policies tab button.

8 Click on the Add button. The IPSec Security Policy (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Auto-Assign ID
- Security Policy ID

10 Click on the IPSec Security Policy Entries tab button.

11 Click on the Add button. The Security Policy Entry (Create) form opens.

12 Configure the Name parameter.

13 Configure the Local Address Option parameter.

14 Perform one of the following.

a If you set the Local Address Option parameter to IP Address in step 13, configure the following parameters:

- IP Address
- Prefix Length

b If you set the Local Address Option parameter to None or Any, go to step 15.

15 Configure the Remote Address Option parameter.

16 Perform one of the following.

a If you set the Remote Address Option parameter to IP Address in step 15, configure the following parameters:

- IP Address
- Prefix Length

b If you set the Remote Address Option parameter to None or Any, go to step 17.

17 Click on the OK button. The Security Policy Entry (Create) form closes.

18 Repeat steps 8 to 17 to add additional IPSec security policy entries.

19 Click on the OK button. The IPSec Security Policy (Create) form closes. A dialog box appears.

20 Click on the OK button.

21 Close the VPRN Site (Edit) form.

22 Close the VPRN (Edit) form.

23 Close the Manage Services form.

Procedure 32-6 To create an IPsec interface on a VPRN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the IPSec Interfaces tab button.

6 Click on the Add button. The IPSec Interface (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Configured IP MTU (Octets)

8 Configure a port for the interface.

i Click on the Port tab button.

ii Click on the Select button to choose a port to associate with the IPsec interface. The Select Terminating Port - IPSec Interface form opens.

iii Specify a filter for the search, if required, and click on the Search button.

iv Select a port from the list and click on the OK button. The Select Terminating Port - IPSec Interface form closes and the IPSec Interface (Create) form reappears with the selected port information displayed.

v Configure the parameters:

- Auto-Assign ID
- Outer Encapsulation Value
- SAP Description
- SAP Administrative State

Note 1 — You can configure the 5620 SAM to automatically assign lowest unused outer encapsulation value by enabling the Auto-Assign ID parameter.

Note 2 — You can set the Auto-Assign ID parameter to be the default parameter for dot1 Q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form.

Note 3 — Private and public IPsec connection points support only dot1 Q encapsulation.

9 Assign ingress and egress QoS policies to the interface, if required.

i Click on the QoS tab button.

ii Configure the parameters:

- Use Shared Queue
- Use Multipoint Shared Queue

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - IPSec Interface form opens.

iv Use the configurable filter and Search button to choose a policy, and click on the OK button. The Select Ingress Policy - IPSec Interface form closes and the IPSec Interface (Create) form reappears with the ingress QoS policy information displayed.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - IPSec Interface form opens.

vi Use the configurable filter and Search button to choose a QoS policy, and click on the OK button. The Select Egress Policy - IPSec Interface form closes and the IPSec Interface (Create) form reappears with the egress QoS policy information displayed.

10 Click on the Schedulers tab button to configure scheduling. Otherwise, go to step 12.

Note — The Schedulers tab is configurable only if you assign a port to the SAP in step 8.

11 Perform the following:

i Configure the Aggregate Rate Limit (kbps) parameter.

Note 1 — The Aggregate Rate Limit (kbps) parameter is configurable only when you enable the Assign Aggregate Rate Limit check box, and there is no scheduler specified in the Egress Scheduler panel.

Note 2 — You cannot specify an egress scheduler when the Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

ii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - IPSec Interface form opens.

iii Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - IPSec Interface form closes, and the IPSec Interface (Create) form refreshes with the ingress scheduler information displayed.

iv Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - IPSec Interface form opens.

v Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - IPSec Interface form closes, and the IPSec Interface (Create) form refreshes with the egress scheduler information displayed.

vi Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Policer Control Policy - IPsec Interface form opens.

vii Choose an ingress policer control policy and click on the OK button. The Select Policer Control Policy - IPsec Interface form closes and the IPsec Interface (Create) form refreshes with the ingress policer information displayed.

viii Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Policer Control Policy - IPsec Interface form opens.

ix Choose an egress policer control policy and click on the OK button. The Select Policer Control Policy - IPsec Interface form closes and the IPsec Interface (Create) form refreshes with the egress policer information displayed.

x Go to step 12.

12 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress IPv4 ACL filter. The Select Ingress Filter - IPSec Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - IPSec Interface form closes and the IPSec Interface (Create) form reappears with the ingress IPv4 ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress IPv4 ACL filter. The Select Egress Filter - IPSec Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - IPSec Interface form closes and the IPSec Interface (Create) form reappears with the egress IPv4 ACL filter information displayed.

13 Assign an IP address to the IPsec interface.

i Click on the Addresses tab button.

ii Click on the Add button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The IPSec Interface (Create) form reappears with the assigned IP addresses displayed.

14 Specify queue overrides by clicking on the Override tab button. See chapter 44 for information about how to set queue overrides.

Note — The Override tab contains four sub-tabs: Access Ingress Queue, Access Egress Queue, Access Ingress HSMDA Queue, and Access Egress HSMDA Queue. However, only two of the four are active, depending on the port type you have chosen for this interface.

If you have configured an HSMDA port, then the Access Ingress HSMDA Queue and Access Egress HSMDA Queue sub-tabs are active. If you have configured a non-HSMDA port, then the Access Ingress Queue and Access Egress Queue sub-tabs are active.

15 Click on the OK button. A dialog box appears.

16 Click on the OK button. The IPSec Interface (Create) form closes, and the VPRN Service (Create) form reappears.

17 Repeat steps 6 to 15 to create another IPsec interface for the VPRN service.

Procedure 32-7 To create an IPsec gateway on an IES or VPRN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Select an IES or VPRN.

4 Click on the Properties button. The properties form for the service opens with the general properties of the service displayed on the General tab.

5 Click on the L3 Access Interfaces tab button.

6 Click on the Search button. A list of L3 access interfaces appears.

7 Choose the L3 access interface on which you want to create the IPsec gateway and click on the Properties button. The *Service* L3 Access Interface (Edit) form opens with the General tab displayed.

Note — The port configured on the L3 access interface must be an IPsec group SAP. This is the public-facing interface for an IPsec tunnel.

8 Click on the IPSec Gateway tab button.

9 Click on the Add button. The IPSec Gateway (Create) form opens with the General tab displayed.

10 Configure the parameters:

- Name
- Pre Shared Key

11 Click on the Select button in the IKE Policy panel to associate an IKE policy with the IPSec gateway. The Select IKE Policy - IPSec Gateway list form opens.

12 Specify a filter for the search, if required, and click on the Search button. A list of IKE policies appear.

13 Choose a policy and click on the OK button. The Select IKE Policy - IPSec Gateway list form closes.

14 Click on the Select button in the IPSec Tunnel Template panel to associate an IPsec tunnel template with the IPsec gateway. The Select IPSec Tunnel Template - IPSec Gateway list form opens.

15 Specify a filter for the search, if required, and click on the Search button. A list of IPsec tunnel templates appear.

16 Choose an IPsec tunnel template and click on the OK button. The Select IPSec Tunnel Template - IPSec Gateway list form closes.

17 Select the VPRN service site to which you are creating the IPsec tunnel from the IES or VPRN by performing the following:

i Click on the Select button in the Secure Service Id panel. The Select Secure Service Id - IPSec Gateway list form opens.

ii Specify a filter for the search, if required, and click on the Search button. A list of VPRN services appears.

iii Choose an entry and click on the OK button. The Select Secure Service Id - IPSec Gateway list form closes.

18 Select the IPSec interface on the VPRN service site to which you are creating the IPsec tunnel from the IES or VPRN by performing the following:

i Click on the Select button in the IPSec Interface Name panel. The Select IPSec Interface Name - IPSec Gateway list form opens.

ii Click on the Search button. A list of IPsec interfaces appears.

iii Choose an entry and click on the OK button. The Select IPSec Interface Name - IPSec Gateway list form closes.

19 Configure the Local Gateway Address parameter.

20 Click on the States tab button.

21 Configure the Administrative State parameter.

22 Click on the OK button. The IPSec Gateway (Create) form closes. A dialog box appears.

23 Click on the OK button to close the dialog box. The *Service* L3 Access Interface (Create) form reappears.

24 Click on the OK button to save the configuration and close the form.

25 A dialog box appears. Click on the OK button to close the dialog box.

26 Click on the OK button. A dialog box appears.

27 Click on the Yes button. The properties form for the service closes.

Procedure 32-8 To create an IPsec tunnel on a VPRN IPsec interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the list filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the IPsec Interfaces tab button.

6 Choose an IPsec interface and click on the Properties button. The IPsec Interface (Edit) form opens.

7 Click on the IPsec Tunnels tab button.

Note — You must first assign a port to the IPsec interface for the IPsec Tunnels tab to appear.

8 Click on the Add button. The IPSec Tunnel (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- Replay Window
- Keying
- Local Gateway Address
- Remote Gateway Address

10 Click on the Select button beside the Security Policy ID parameter. The Select Security Policy - IPSec Tunnel list form opens.

11 Specify a filter for the search, if required, and click on the Search button. A list of policies appears.

12 Choose an entry and click on the OK button. The Select Security Policy - IPSec Tunnel form closes.

13 Click on the Select button beside the Name parameter. The Select Service Name - IPSec Tunnel list form opens.

14 Specify a filter for the search, if required, and click on the Search button. A list of services appears.

15 Choose an entry and click on the OK button. The Select Service Name - IPSec Tunnel form closes.

16 Perform one of the following.

a If you set the Keying parameter to None in step 9, go to step 19.

b If you set the Keying parameter to Dynamic in step 9, go to step 17.

c If you set the Keying parameter to Manual in step 9, go to step 18.

17 Configure dynamic keying.

i Click on the Dynamic Keying tab button.

ii Click on the Select button beside the following parameters:

- Transform ID 1
- Transform ID 2
- Transform ID 3
- Transform ID 4

The Select Transform ID - IPSec Tunnel form opens.

iii Specify a filter for the search, if required, and click on the Search button. A list of policies appears.

iv Choose an entry and click on the OK button. The Select Transform ID - IPSec Tunnel form closes.

v Click on the Select button beside the IKE Policy parameter. The Select IKE Policy - IPSec Tunnel list form opens.

vi Specify a filter for the search, if required, and click on the Search button. A list of policies appears.

vii Choose an entry and click on the OK button. The Select IKE Policy - IPSec Tunnel form closes.

viii Configure the parameters:

- Pre Shared Key
- Auto-Establish

ix Go to step 19.

18 Configure manual keying.

i Click on the Manual Keying tab button.

ii Click on the Add button. The IPSec Security Association (Create) form opens.

iii Click on the Select button in the Security Policy Entry panel. The Select Security Policy Entry - IPSec Security Association list form opens.

iv Click on the Search button. A list of policy entries appears.

v Choose an entry and click on the OK button. The Select Security Policy Entry - IPSec Security Association list form closes.

vi Configure the parameters:

- Direction
- Encryption Key
- Authentication Key
- SPI

vii Click on the Select button in the Transform panel. The Select Transform - IPSec Security Association list form opens.

viii Click on the Search button. A list of transform policies appears.

ix Choose an entry and click on the OK button. The Select Transform - IPSec Security Association list form closes.

x Click on the OK button. The IPSec Security Association (Create) form closes.

19 Click on the States tab button.

20 Configure the Administrative State parameter.

21 Click on the BFD tab button.

22 Configure the parameters:

- Designated
- Enabled

If you set the Enabled parameter to Enabled, go to step 23. Otherwise, go to step 28.

23 Click on the Select button beside the Service Name parameter. The Select BFD Service - IPsec Tunnel BFD form opens.

24 Configure the filter, if required, and choose a BFD service. The BFD service information appears for the Service Name, Service ID, and Site ID parameters.

25 Click on the Select button beside the Name parameter. The Select Interface - IPsec Tunnel BFD form opens.

26 Configure the filter, if required, and choose an interface. The interface name appears for the Name parameter.

27 Configure the Destination Address parameter.

28 Click on the OK button. The IPSec Tunnel (Create) form closes. A dialog box appears.

29 Click on the OK button.

30 Repeat steps 8 to 29 to add additional IPsec tunnels.

Procedure 32-9 To enable BFD for a static LAN-to-LAN IPsec tunnel

Note — BFD can only be enabled for the 7750 SR.

1 On the private side, use the CLI to specify a tunnel as the BFD tunnel and enable BFD on the tunnel. For example:

```
config>service>vprn>ipsec-if>sap>tun>

[no]bfd-enable [service-id] interface interface-name dst-ip
ip-addr

[no]bfd-designated
```

See the 7750 SR documentation for more information about the CLI commands.

2 On the public side, use the CLI to configure the transmit interval. For example:

```
config>service>vprn>if>

bfd transmit-interval [receive receive-interval] [multiplier
multiplier] [echo-receive echointerval]
```

See the 7750 SR documentation for more information about the CLI commands.

3 Create a VPRN service. See chapter 71 for more information.

4 Create two VPRN L3 access interfaces. See chapter 71 for more information.

5 Create an IPsec interface on a VPRN, as described in Procedure 32-6.

6 Create an IPsec tunnel on a VPRN IPsec interface, as described in Procedure 32-8.

32.8 IPsec VPN procedures

The following procedures describe how to perform 5620 SAM IPsec configuration tasks using the IPsec VPN step forms.

Procedure 32-10 To create an IPsec VPN

1 Configure a corporate service. Table 32-2 lists where to find information about each corporate service type.

Table 32-2 Corporate service types

Corporate service	See chapter
Apipe	67
Cpipe	
Fpipe	
Ipipe	
VPLS	68
IES	70
VPRN	71
VLAN	65

2 If required, configure one or more service templates. Table 32-2 lists where to find more information.

3 Choose Create→IPsec VPN from the 5620 SAM main menu. The Create IPsec VPN step form opens.

4 Configure the parameters:

- Auto-Assign ID
- IPsec VPN Name
- Description
- Service Type
- Link Corporate and Secured Service

5 To select a corporate service, perform the following, otherwise, go to step 6.

i Click on the Select button beside the Corporate Service ID parameter. The Select Corporate Service - IPsec VPN form opens. Only the specific service type, as set by the Service Type parameter, is listed.

ii Filter the corporate services, if required, and select a corporate service.

iii Click on the OK button to close the Select Corporate Service - IPSec VPN form. The Corporate Service ID and Corporate Service Name parameters display the service ID and service name for the selected corporate service on the Create IPsec VPN step form.

6 Click on the Next button on the Create IPsec VPN step form. The Select Service Sites step form opens. Perform Procedure 32-11 to select the service sites.

Procedure 32-11 To select a service NE site for an IPsec VPN

This procedure selects the NE site for the IPsec VPN.

1 Perform Procedure 32-10 to create an IPsec VPN.

2 Perform one of the following:

a To choose an existing service site, configure the filter and click on the Search button. A list of service sites appears. Go to step 7.

b To create a service site, go to step 3.

3 Click on the Add button. The Manage Equipment form opens.

4 Configure the filter, if required, and click on the Search button. A list of NEs appears.

5 Select a NE and click on the OK button. The NE appears in the Select Service Sites step form.

6 Repeat steps 3 to 5 to add another NE site.

7 Select an NE site and click on the Next button. The Create/Select Secure VPRN Service step form opens. Perform Procedure 32-12 to:

- select a service
- create a service
- create a service from a template

Procedure 32-12 To create or select a secure VPRN service for an IPsec VPN

1 Perform Procedures 32-10 and 32-11.

2 Perform one of the following:

a To select a service, go to step 3.

b To create a service, go to step 7.

c To create a service from a template, go to step 12.

Note — The template must be configured for one site. The template cannot be used if the template is configured for multiple sites.

3 Click on the Select Service button. The Select Service form opens.

4 Configure the filter, if required, and click on the Search button. A list of services appear.

5 Select a service and click on the OK button. The service appears in the Create/Select Secure VPRN Service step form.

6 Click on the Service Site tab button and configure the parameters:

- Description
- Administrative State

Go to step 15.

7 Click on the Create Service button.

8 Click on the Select button beside the Customer parameter. The Select Customer form opens.

9 Filter the customers, if required, and select a customer from the list.

10 Click on the OK button.

11 Configure the parameters:

- Service Name
- Description
- Service Tier
- Administrative State

Go to step 6.

12 Click on the Create Service From Template button. The Create Service From Template appears.

13 Filter the services, if required, and click on the Search button.

14 Select a service from the list and click on the OK button. Go to step 6.

15 Click on the Next button. The Create/Select Delivery Service(s) step form opens. Perform Procedure 32-13.

Procedure 32-13 To create or select a delivery service for an IPsec VPN

1 Perform Procedures 32-10 to 32-12.

2 Perform one of the following:

a To select a delivery service, go to step 3.

b To create a delivery service, go to step 8.

c To create a service from a template, go to step 13.

Note — The template must be configured for one site. The template cannot be used if the template is configured for multiple sites.

d To remove a service, go to step 17.

3 Click on the Select Service button. The Select Service form opens.

4 Choose IES Service (IES) or VPRN Service (VPRN) from the drop-down menu, choose a filter, if required, and click on the Search button.

5 Select a service from the list and click on the OK button. The service appears in the Create/Select Delivery Service(s) list.

6 Click on the Service Site tab button and configure the parameters:

- Description
- Administrative State

7 Repeat steps 3 to 6 to select another service. Go to:

a step 8 to create a service

b step 13 to create a service from a template

c step 17 to remove a service

d step 18 to select an IPsec group

8 Click on the Create Service button and choose VPRN or IES. The service appears in the Create/Select Delivery Service(s) list.

9 Click on the Select button beside the Customer parameter. The Select Customer form opens.

10 Choose a customer and click on the OK button.

11 Configure the parameters:

- Service Name
- Description
- Service Tier
- Administrative State

12 Repeat steps 8 to 11 to create another service. Go to:

a step 13 to create a service from a template

b step 17 to remove a service

c step 18 to select an IPsec group

13 Click on the Create Service From Template button and choose VPRN or IES. The Create Service Form Template appears.

14 Configure the filter, if required, and click on the Search button. A list of services appears.

15 Select a service template and click on the OK button.

16 Repeat steps 13 to 15 to create another service. Go to:

a step 17 to remove a service

b step 18 to select an IPsec group

17 If you perform this step, the service is removed without confirmation and there is no undo. Select a service in the Create/Select Delivery Service(s) list and click on the Remove Service button.

18 Click on the Next button. The IPsec Group Selection step form opens. Perform Procedure 32-14.

Note — The Next button is not enabled until you perform steps 9 and 10 for each delivery service in the Create/Select Delivery Service(s) step form.

Procedure 32-14 To select an IPsec group for an IPsec VPN

1 Perform Procedures 32-10 to 32-13.

2 Select a service and configure the parameters by clicking in the panel and entering values or choosing an option:

Note 1 — The parameters are not part of the XML. In OSSI, you can create the ServiceSiteStructs and in the ServiceSiteStructs, you can create the IPsec VPN objects. See the *5620 SAM-O OSS Interface Developer Guide* for more information.

Note 2 — If the tunnel type is static, the parameters that require configuration are:

- Delivery Service Interface Address
- Local Gateway Address
- Remote Gateway Address
- Static Route Address
- Static Route Prefix

If the tunnel type is dynamic site-site, the parameters that require configuration are:

- Delivery Service Interface Address
- Local Gateway Address

If the tunnel type is dynamic soft client, the parameters that require configuration are:

- Secure Service Interface Address
- Delivery Service Interface Address
- Local Gateway Address

- ISA-IPsec Group
- Tunnel Type
- Secure Service Interface Address
- Delivery Service Interface Address
- Local Gateway Address
- Remote Gateway Address
- Static Route Address
- Static Route Prefix

3 Click on the Service Site tab button and configure the parameters:

- Description
- Administrative State

4 Repeat steps 2 and 3 for each service.

5 Click on the Next button. The Create Policy step form opens.

Perform Procedure 32-15 if you chose Dynamic (Site-to-Site) for the Tunnel Type parameter in step 2.

Perform Procedure 32-16 if you chose Dynamic (Soft Client) for the Tunnel Type parameter in step 2.

Perform Procedure 32-17 if you chose Static for the Tunnel Type parameter in step 2.

Note — The Next button is not enabled until you perform step 2 for each IPsec group in the IPsec Group Selection step form.

Procedure 32-15 To assign policies and configurations for a dynamic site-to-site IPsec VPN

This procedure assumes you chose Dynamic (Site-to-Site) for the Tunnel Type parameter in step 2 of Procedure 32-14.

1 Perform Procedures 32-10 to 32-14.

2 Click on the Select button beside the IPsec Tunnel Template Policy ID parameter in the IPsec Tunnel Template panel. The Select IPsec Tunnel Template - IPsec VPN form opens.

3 Perform one of the following:

   a To select an IPsec tunnel template from the list, go to step 4.

   b To create an IPsec tunnel template, go to step 5.

4 Configure the filter, if required, click on the Search button. Go to step 10.

5 Click on the Create button. The IPsec Tunnel Template form opens. Perform steps 3 to 11 in Procedure 32-4.

6 Click on the Select button beside the Policy ID parameter in the IKE Policy panel. The Select IKE Policy - IPsec VPN form opens.

7 Perform one of the following:

   a To select an IKE Policy from the list, go to step 9.

   b To create an IKE Policy, go to step 8.

8 Click on the Create button and perform steps 3 to 12 in Procedure 32-1.

9 Select a Policy and click on the OK button.

10 Configure the Pre Shared Key parameter.

11 Click on the Finish button.

   If there is a configuration problem, the Problems Encountered form opens. Fix the problem and click on the Finish button.

If there are no configuration problems, a completed message appears. The 5620 SAM performs the following:

- a secure VPRN service and sites are created (see Code 32-1)
  - an access interface is created
  - an IPsec interface is created
  - the service name is configured
- the IES or VPRN delivery service and sites are created (see Code 32-2)
  - an access interface is created
  - the IP address of the SAP is configured
  - an IPsec group with an auto-generated outer encapsulation as a public SAP is assigned
  - an IPsec gateway is created
  - the secure service is assigned
  - the IPsec interface of the secure service is assigned
  - the tunnel template is assigned
  - the IKE policy is assigned
  - the local gateway address is configured
  - the Pre Shared key is configured
  - the service name is configured
- if the Link Corporate and Secure Service parameter is enabled, a composite service is created that contains the corporate and secure service

You can click on the View the newly created IPSec Secured VPN button. The IPsec VPN form opens.

Code 32-1: Secure VPRN service example

```
vprn 254 customer 2 create
            ipsec-interface "sam-auto-ipsec-intf-1" create
                sap ipsec-2.private:9 create
                exit
            exit
            service-name "VPRN service-310 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

Code 32-2: VPRN delivery service example

```
vprn 255 customer 2 create
            interface "sam-auto-access-intf-1" create
                address 33.33.3.3/24
                sap ipsec-2.public:11 create
                    ipsec-gw "sam-auto-gateway-1"
                        default-secure-service 254 ipsec-interface
"sam-auto-ipsec-intf-1"
                        default-tunnel-template 1
                        ike-policy 1
                        local-gateway-address 33.33.3.2
                        pre-shared-key "Test"
                        no shutdown
                    exit
                exit
            exit
```

```
        service-name "VPRN service-311 CPM_132_A (38.120.169.132)"
        no shutdown
    exit
```

Procedure 32-16 To assign policies and configurations for a dynamic soft client IPsec VPN

This procedure assumes that you chose Dynamic (Soft Client) for the Tunnel Type parameter in step 2 of Procedure 32-14.

1. Perform Procedures 32-10 to 32-14.
2. Perform steps 2 to 9 in Procedure 32-15.
3. Click on the Select button beside the Displayed Name parameter. The Select Subscriber Authentication Policy - IPsec VPN form opens.
4. Perform one of the following:
   - **a** To select a subscriber authentication policy from the list, go to step 6.
   - **b** To create a subscriber authentication policy, go to step 5.
5. Click on the Create button. The Subscriber Authentication Policy (Create) form opens. See chapter 18 for information about creating a Subscriber Authentication Policy.
6. Select a subscriber authentication policy from the list and click on the OK button.
7. Click on the Finish button.

   If there is a configuration problem, the Problems Encountered form opens. Fix the problem and click on the Finish button.

If there are no configuration problems, a completed message appears. The 5620 SAM performs the following:

- a secure VPRN service and sites are created (see Code 32-3)
  - an access interface is created
  - an IPsec interface is created
  - the IP Address of the SAP is configured
  - the service name is configured
- the IES or VPRN delivery service and sites are created (see Code 32-4)
  - an access interface is created
  - the IP address of the SAP is configured
  - the RADIUS authentication policy is assigned
  - an IPsec group with an auto-generated outer encapsulation as a public SAP is assigned
  - an IPsec gateway is created
  - the tunnel template is assigned
  - the IKE policy is assigned
  - the local gateway address is configured
  - the Pre Shared key is configured
  - the service name is configured
- if the Link Corporate and Secure Service parameter is enabled, a composite service is created that contains the corporate and secure service

You can click on the View the newly created IPSec Secured VPN button. The IPsec VPN form opens.

Code 32-3: Secure VPRN service example

```
vprn 260 customer 2 create
            ipsec-interface "sam-auto-ipsec-intf-4" create
                address 9.9.9.9/24
                sap ipsec-1.private:47 create
                exit
            exit
            service-name "VPRN service-316 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

Code 32-4: VPRN delivery service example

```
vprn 261 customer 2 create
            interface "sam-auto-access-intf-4" create
                address 40.1.1.2/24
                authentication-policy "test"
                sap ipsec-1.public:42 create
                    ipsec-gw "sam-auto-gateway-4"
                        default-tunnel-template 1
                        ike-policy 2
                        local-gateway-address 40.1.1.1
                        pre-shared-key "Test"
                        no shutdown
                    exit
                exit
            exit
```

```
        service-name "VPRN service-317 CPM_132_A (38.120.169.132)"
        no shutdown
    exit
```

Procedure 32-17 To assign policies and configurations for a static IPsec VPN

This procedure assumes that you chose Static for the Tunnel Type parameter in step 2 of Procedure 32-14.

1 Perform Procedures 32-10 to 32-14.

2 Perform steps 3 to 6 in Procedure 32-15.

3 Configure the parameters:

- Pre Shared Key
- Replay Window
- Keying

If you set the Keying parameter to Manual, go to step 4. If you set the Keying parameter to Dynamic, go to step 6.

4 Configure the Manual Keying - Inbound parameters:

- Keying Type
- Encryption Key
- Authentication Key
- SPI Inbound

5 Configure the Manual Keying - Outbound parameters:

- Keying Type
- Encryption Key
- Authentication Key
- SPI Outbound

6 Perform one of the following:

a To select an IPsec transform policy from the list, go to step 8.

b To create an IPsec transform policy, go to step 6.

7 Click on the Create button and perform steps 3 to 12 in Procedure 32-1.

8 Select an IPsec transform policy and click on the OK button.

9 Configure the Auto-Establish parameter.

Note — The Auto-Establish parameter is only configurable if dynamic keying is selected.

10 Click on the Finish button.

If there is a configuration problem, the Problems Encountered form opens. Fix the problem and click on the Finish button.

If there are no configuration problems, a completed message appears. The 5620 SAM performs the following:

- a secure VPRN service and NE sites are created (see Code 32-5)
  - the IPsec security policy is created
  - an IPsec interface is created
  - an IPsec group with an auto-generated outer encapsulation as a private SAP is assigned
  - the IPsec tunnel is created
  - the security policy is assigned to the tunnel
  - the local and remote gateway addresses are configured
  - the delivery service is configured
  - the replay window is configured
  - the keying is configured
  - if set, auto establish is enabled
  - the static route is configured
  - the service name is configured
- the IES or VPRN delivery service and NE sites are created (see Code 32-6)
  - an access interface is created
  - an IPsec group with an auto -generated outer encapsulation as a public SAP is assigned
  - the IP address of the SAP is configured
  - the service name is configured
- if the Link Corporate and Secure Service parameter is enabled, a composite service is created that contains the corporate and secure service

You can click on the View the newly created IPSec Secured VPN button. The IPsec VPN form opens.

Code 32-5: Secure VPRN service example - Keying parameter set to Dynamic

```
vprn 252 customer 2 create
            ipsec
                security-policy 1 create
                    entry 1 create
                        local-ip any
                        remote-ip any
                    exit
                exit
            exit
            ipsec-interface "sam-auto-ipsec-intf-32" create
```

```
                sap ipsec-1.private:46 create
                    tunnel "sam-auto-tunnel-32" create
                        security-policy 1
                        local-gateway-address 40.1.1.2 peer 2.2.2.2 delivery-service
253
                        replay-window 64
                        dynamic-keying
                            ike-policy 1
                            pre-shared-key "Test"
                            transform 1
                        exit
                        no shutdown
                    exit
                exit
            exit
            static-route 3.3.3.3/32 ipsec-tunnel "sam-auto-tunnel-32"
            service-name "VPRN service-308 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

Code 32-6: VPRN delivery service example

```
vprn 253 customer 2 create
            interface "sam-auto-access-intf-32" create
                address 40.1.1.1/24
                sap ipsec-1.public:41 create
                    collect-stats
                exit
            exit
            service-name "VPRN service-309 CPM_132_A (38.120.169.132)"
            no shutdown
        exit
```

33 — ISA-Video

33.1 ISA-Video overview

The 5620 SAM allows the equipment and services configuration of the following enhancements to multicast video service provided by the ISA-Video MDA module:

- Reliable Delivery/Retransmisson (RT) Proxy
- Fast Channel Change (FCC)
- Ad Insertion (ADI)

These features are supported on the 7750 SR and 7450 ESS, Release 7.0 R4 or later.

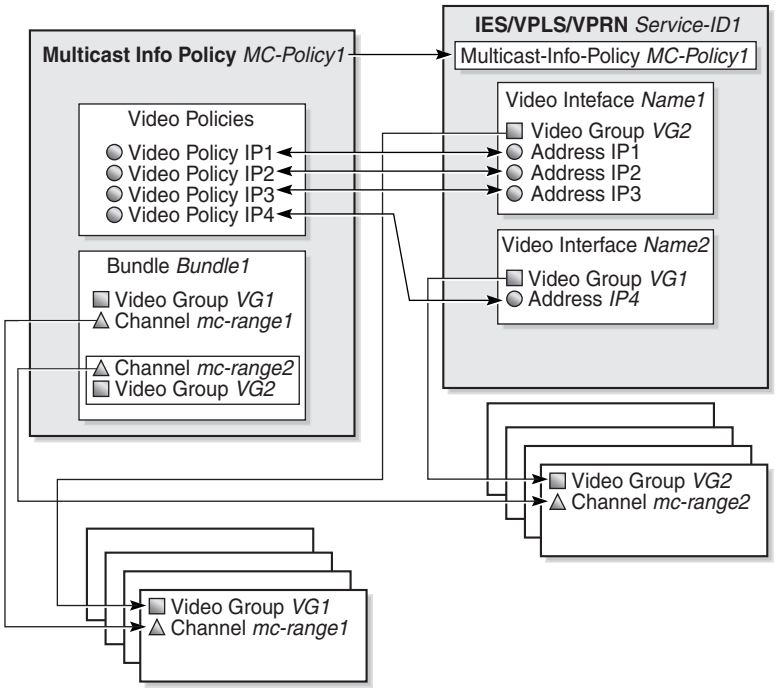
You can use the 5620 SAM to configure the required ISA-Video Groups and Members, as well as the associated multicast info policies. VPRN, IES, and VPLS services can then be configured for the customer video delivery.

These enhancements are provisioned in 5620 SAM in following three areas:

- A Video Group configuration to manage the ISA resources and service grouping.
- Multicast Information policy configuration parameters and objects to handle the RT, FCC and Ad insertion capabilities, including:
  - A Video Policy configuration under the Multicast Information Policy
  - Video parameters added to Multicast Bundles, Channels and Channel override configurations
- Video Interface configurations are added under VPRN/IES/VPLS services sites.

Figure 33-1 shows the relationship of these various elements and how they are associated through configuration.

Figure 33-1 ISA-Video configuration elements



A Video Interface within a service site can have up to eight IP addresses. The IP addresses assigned to a Video Interface determine which MultiCast Info Policy is applied. The Video Group you assign to the Video Interface determines which bundle/channel configuration inside the Multicast Info policy is applied to the interface. You also configure the ingress and egress QOS policies for the Video Interface using the Video Group.

If a request is received on a Video Interface for a channel not serviced by the Video Group associated with that specific Video Interface, then the request is considered invalid and is dropped. For example, in Figure 33-1, a request for mc-range2 received on IP1, IP2, or IP3 is invalid. A request for mc-range2 is only valid on IP4.

A Video Group manages the ISA-Video MDA resource and the configurations of the enhanced video functionality. You can assign a Video Group (for example, VG1 in Figure 33-1) for each Bundle, and this is the default Video Group for all of the channels in that Bundle. You can then apply specific configuration overrides for each channel within a Video Group assignment.

Up to four Video Groups (ID 1-4) can be configured on a single node. Each Video Group in turn, can have multiple primary video ISAs assigned to provide load balancing and redundancy protection. However, any specific video ISA can only be bound to one Video Group. The binding of a video ISA to the Video Group is referred as a Video Group Member.

Additional considerations for the Ad Insertion functionality:

- Ingress Ad Insertion channels are configured on the Video Interface configuration form.
- If Ad Insertion functionality is enabled on a Video Group, then the group can only have one Video Group Member.
- You can configure Zone Channels for egress Ad Insertion on each Ad Insertion channel configuration.
- Ad Insertion channels are not applicable to VPLS.

33.2 Workflow to configure and manage an ISA-Video configuration

1. Provision the ISA-Video MDA on the 7750 SR or 7450 ESS, Release 7.0 R4 or later. See chapters 15 and 17 for more information about ISA-Video MDA equipment configuration.
2. Create or configure ISA-Video Groups.
3. Create or configure ISA-Video Group Members under the Video Groups.
4. Configure and distribute a global Multicast Information policy.
5. Configure the channel bundle, channel range, channel overrides, and video interface for the node.

Note — Video interfaces can only be created on local policy definitions, since they are node-specific.

6. Apply the changes to the node, switch the policy distribution mode back to Sync with Global, and save it. The local video-related changes you made are not affected by the switch.
7. Create and enable a video interface for the VPLS, IES, or VPRN service.

33.3 ISA-Video procedures

The following procedures describe how to perform 5620 SAM ISA-Video configuration tasks.

Procedure 33-1 To add a Video interface to a VPRN site

The 7710 SR and 7750 SR support the configuration of a video interface in a VPRN service.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the required VPRN service and click on the Properties button. The VPRN (Edit) form opens with the General tab displayed.

4 Click on the Components tab button and choose the site to which you want to add the video interface; expand the entries for that site.

5 Right-click on the Video Interfaces and choose Create Video Interface. The Video Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Name
- Description
- Admin Status
- Group Number
- Associated Multicast Service ID
- RT Client Address
- ADI Administrative Status
- SCTE 30 Control Address
- SCTE 30 Data Address

After you choose a Group Number, the following selectable fields are also displayed:

- Ingress QoS Policy
- Egress QoS Policy
- Ingress IP Filter
- Egress IP Filter

Choose the required policies and filters by clicking on the Select button beside the corresponding fields. You can perform a search or choose the entry from the list that appears for each of these items.

7 Click on the Security tab.

8 Click on the Select button and choose the required NE DoS Protection Policy from the list. You can also perform a search from this form.

9 Click on the Addresses tab and click on the Add button. The IP Address (Create) form opens.

10 Configure the parameters:

- IP Address
- Address Type
- Prefix Length

11 Go to step 12 if you are configuring ad insertion. Otherwise go to step 25.

12 Click on the ADI Channels tab and click on the Add button. The Video ADI Channel (Create) form opens with the General tab displayed.

13 Configure the parameters:

- Name
- Description
- Multicast Channel IP Address
- Unicast Source IP Address
- SCTE 35 Action

14 Click on the Zone Channels tab and click on the Add button. The Video ADI ZoneChannel (Create) form opens.

15 Configure the parameters:

- Name
- ADI Zone Multicast Address
- ADI Zone Unicast Source Address

16 Click on the OK button. The Video ADI ZoneChannel (Create) form closes, and a dialog box appears.

17 Click on the OK button. The Video ADI Channel (Create) form reappears, with the newly-configured Zone Channels displayed in the list.

18 Repeat steps 14 to 17 to configure additional Zone Channels, if required.

19 Click on the OK button. The Video ADI Channel (Create) form closes, and a dialog box appears.

20 Click on the OK button. The Video Interface (Create) form reappears with the newly-configured ADI Channels displayed in the list.

21 Click on the ADI (SCTE 30) Server tab and click on the Add button. The ADI (SCTE 30) Server (Create) form opens.

22 Configure the Server Address parameter.

23 Click on the OK button. The ADI (SCTE 30) Server (Create) form closes and a dialog box appears.

24 Click on the OK button. The ADI (SCTE 30) Server form reappears with the newly-configured ADI (SCTE 30) Server displayed in the list.

25 Click on the OK button. The Video Interface (Create) form closes and a dialog box appears.

26 Click on the OK button. The newly-configured Video Interface is displayed for the site.

27 Close the Manage Services form.

Procedure 33-2 To add a Video interface to an IES site

The 7710 SR and 7750 SR support the configuration of a video interface in an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the required IES service and click on the Properties button. The IES (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Choose the site to which you want to add the video interface and expand the entries for that site.

6 Right-click on the Video Interfaces and choose Create Video Interface. The Video Interface (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Name
- Description
- Admin Status
- Group Number
- Associated Multicast Service ID
- RT Client Address
- ADI Administrative Status
- SCTE 30 Control Address
- SCTE 30 Data Address

After you select a Group Number, the following selectable fields are also displayed:

- Ingress QoS Policy
- Egress QoS Policy
- Ingress IP Filter
- Egress IP Filter

Choose the required policies and filters by clicking on the Select button adjacent to the corresponding fields. You can conduct a search or choose the required entry from the list that appears for each of these items.

8 Click on the Security tab.

9 Click on the Select button to select the required NE DoS Protection Policy from the list displayed in the form. You can also conduct a search from this form.

10 Click on the Addresses tab and click on the Add button. The IP Address (Create) form opens.

11 Configure the parameters:

- IP Address
- Address Type
- Prefix Length

12 Go to step 13 if you are configuring ad insertion. Otherwise go to step 26.

13 Click on the ADI Channels tab and click on the Add button. The Video ADI Channel (Create) form opens with the General tab displayed.

14 Configure the parameters:

- Name
- Description
- Multicast Channel IP Address
- Unicast Source IP Address
- SCTE 35 Action

15 Click on the Zone Channels tab and click on the Add button. The Video ADI ZoneChannel (Create) form opens.

16 Configure the parameters:

- Name
- ADI Zone Multicast Address
- ADI Zone Unicast Source Address

17 Click on the OK button. The Video ADI ZoneChannel (Create) form closes and a dialog box appears.

18 Click on the OK button. The Video ADI Channel (Create) form reappears, with the newly-configured Zone Channels displayed in the list.

19 Repeat steps 15 to 18 to configure additional Zone Channels, if required.

20 Click on the OK button. The Video ADI Channel (Create) form closes and a dialog box appears.

21 Click on the OK button. The Video Interface (Create) form reappears with the newly-configured ADI Channels displayed in the list.

22 Click on the ADI (SCTE 30) Server tab and click on the Add button. The ADI (SCTE 30) Server (Create) form opens.

23 Configure the Server Address parameter.

24 Click on the OK button. The ADI (SCTE 30) Server (Create) form closes and a dialog box appears.

25 Click on the OK button. The ADI (SCTE 30) Server form reappears with the newly-configured ADI (SCTE 30) Server displayed in the list.

26 Click on the OK button. The Video Interface (Create) form closes and a dialog box appears.

27 Click on the OK button. The newly-configured Video Interface is displayed for the site.

28 Close the Manage Services form.

Procedure 33-3 To add a Video interface to a VPLS site

The 7710 SR and 7750 SR support the configuration of a video interface in a VPLS.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the required VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Choose the site to which you want to add the video interface and expand the entries for that site.

6 Right-click on the Video Interfaces and select Create Video Interface. The Video Interface (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Name
- Description
- Admin Status
- Group Number
- Associated Multicast Service ID
- RT Client Address
- Gateway Address

After you select a Group Number, the following selectable fields are also displayed:

- Ingress QoS Policy
- Egress QoS Policy
- Ingress IP Filter
- Egress IP Filter
- Ingress Mac Filter
- Egress Mac Filter

Choose the required policies and filters by clicking on the Select button adjacent to the corresponding fields. You can conduct a search or choose the required entry from the list that appears for each of these items.

8 Click on the Security tab.

9 Click on the Select button to select the required NE DoS Protection Policy from the list displayed in the form. You can also conduct a search from this form.

10 Click on the Addresses tab and click on the Add button. The IP Address (Create) form opens.

11 Configure the parameters:

- IP Address
- Address Type
- Prefix Length

12 Click on the OK button. The Video Interface (Create) form closes, and a dialog box appears.

13 Click on the OK button. The newly-configured Video Interface is displayed for the site.

14 Close the Manage Services form.

34 — Alarm management

34.1 Alarm management overview

The 5620 SAM converts SNMP traps from NEs and 5620 SAM events to alarms that are associated with the managed equipment, configured services and policies.

The alarm-based fault management system provides the following:

- the conversion of SNMP traps from NEs to alarms using the X.733 standard
- the correlation of alarms with equipment- and service-affecting faults
- updates to the managed-object operational status in near-real-time
- alarm policy control that allows a network administrator to specify how to process alarms and how to create and store the alarm logs
- point-and-click alarm management using the 5620 SAM GUI dynamic alarm list and object properties forms
- the ability to log the actions taken to correct the associated fault by adding notes to the alarm
- an alarm history for performing trend analysis

Figure 34-1 shows how the 5620 SAM manages alarms.

Figure 34-1 Alarm management

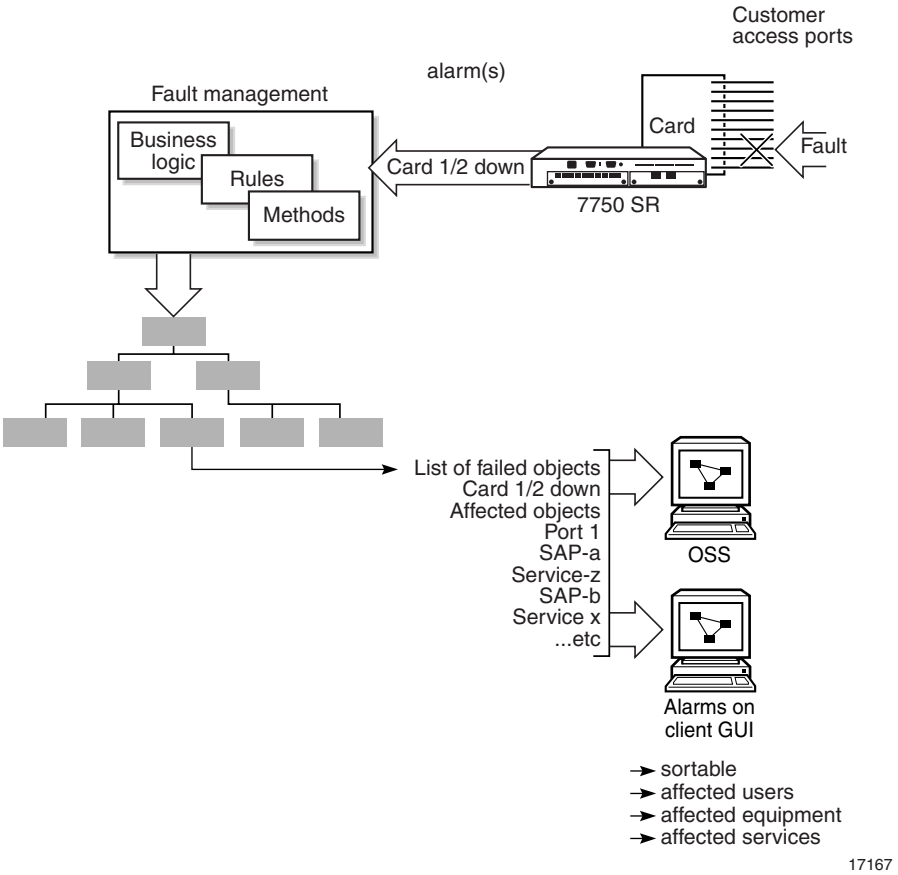
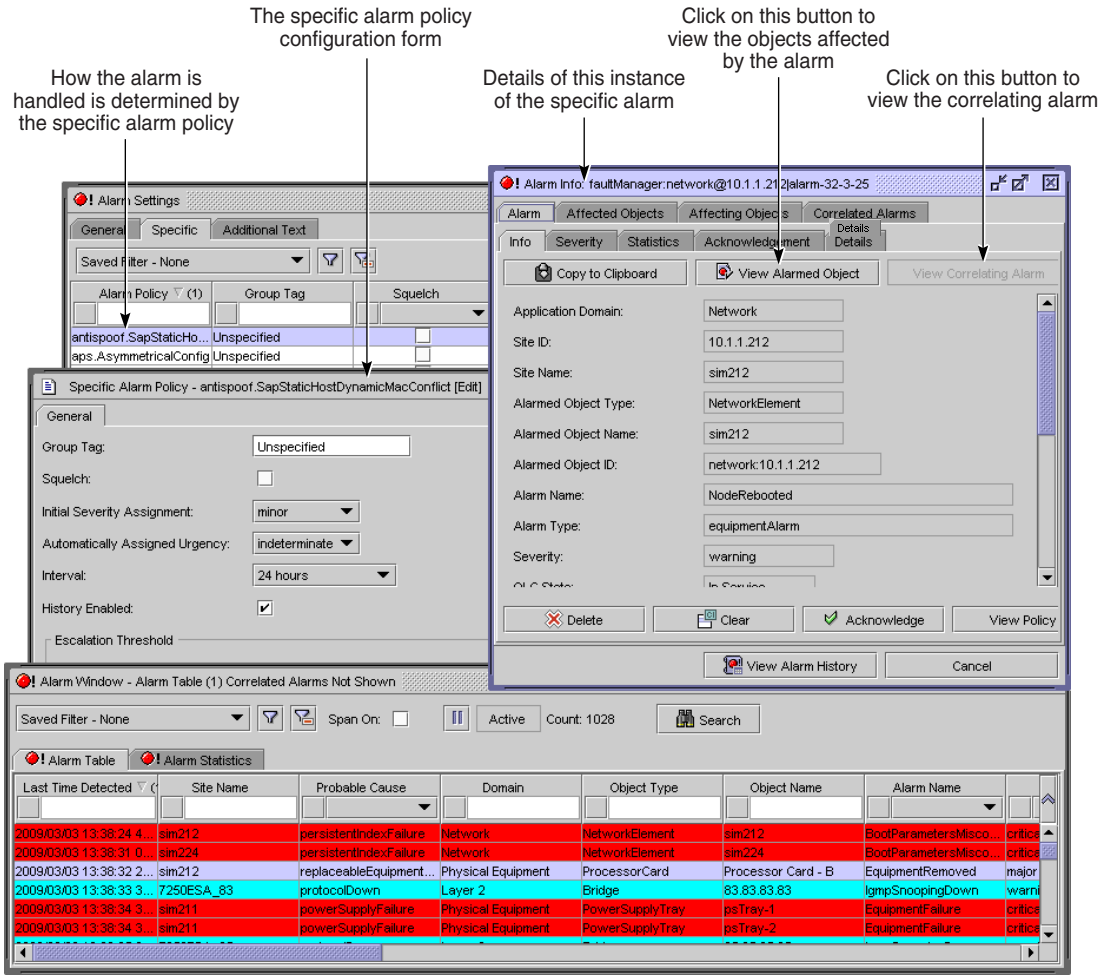


Figure 34-2 shows the following related alarm objects in the 5620 SAM GUI:

- an incoming alarm in the dynamic alarm list
- the alarm policy
- the alarm information form

Figure 34-2 Alarm relationships on the GUI



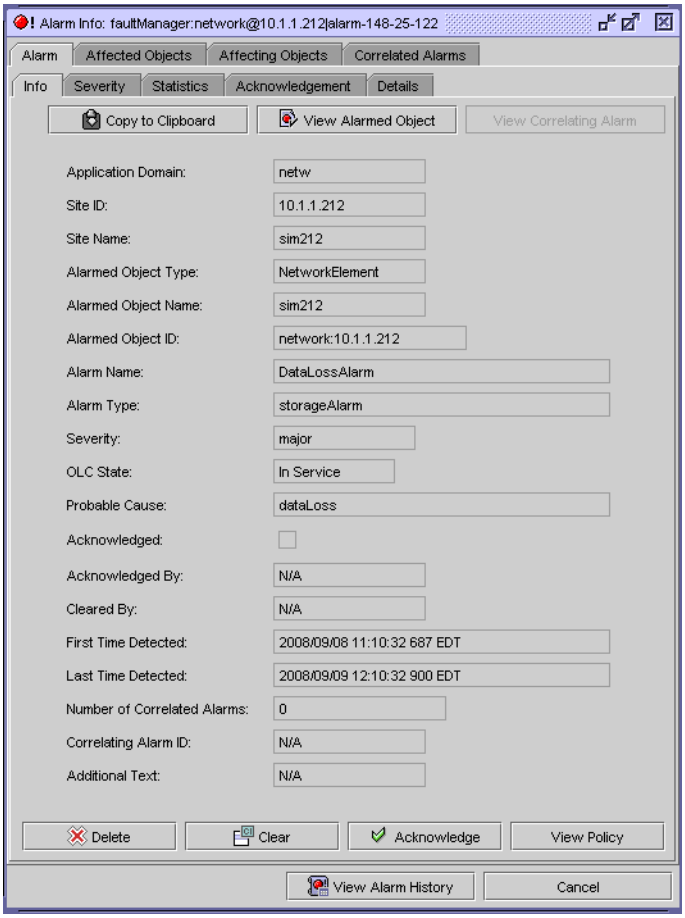
19620

You can view the history of one or more alarms using a 5620 SAM menu option, from the Alarm Info form, and using the View Alarm(s) History contextual menu option in the Alarm Window. From the Alarm Window, you can use the Historical Alarms button to open the Historical Alarms form, and can view the alarm history of an object by choosing the View Object(s) Alarm History contextual menu option.

Note — The View Alarm(s) History and View Object(s) Alarm History menu options are unavailable when more than 20 alarms are selected.

Figure 34-3 shows the Alarm Info form.

Figure 34-3 Alarm Info form



The following information is displayed on an Alarm Info form.

- Alarm tab—contains alarm information that includes the object, severity, statistics, and acknowledgement status.
- Affected Objects tab—contains a list of objects that are affected by the alarm. All alarms list the affected objects, even when correlation alarm suppression is enabled. See Figure 34-4 for how affected objects are determined.
- Affecting Objects tab—contains a list of objects that directly affect the object in alarm. See Figure 34-4 for how affecting objects are determined.
- Correlated Alarms tab—contains a list of correlated alarms. Correlated alarms are raised against other objects that are dependent on the alarmed object.

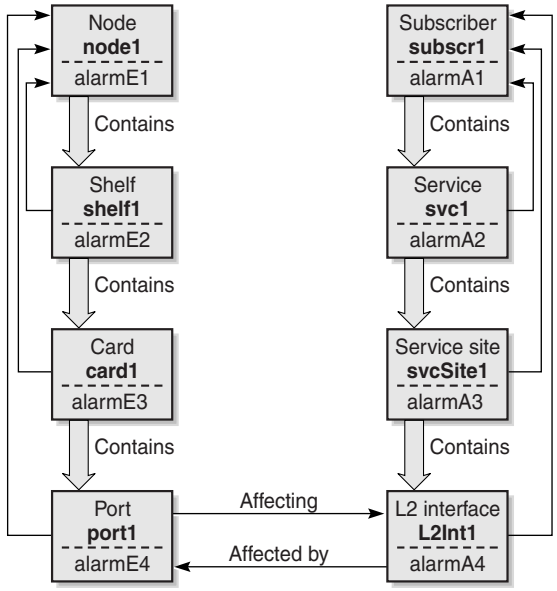
Alarm status, severity, and aggregation

Alarm status for the network is indicated in the navigation tree, the dynamic alarm list, and on the topology maps. You can use the navigation tree to view the status of an alarm raised against a specific object and to view the aggregated alarm status. The aggregated alarm status is also available on the Faults tab of an object property form.

Alarms are considered related or affecting when there is a relationship between objects. The 5620 SAM business logic determines that, for example, if a port goes down and the port is used by a SAP, a customer is affected by the port down alarm.

Figure 34-4 shows how aggregation, affecting, and affected alarms are determined.

Figure 34-4 Aggregation, affecting, and affected alarm inheritance



- **L2Int1** depends on the **port1**.
- **port1** affects **L2Int1**
- alarmE4 affects **L2Int1**

18023

Table 34-1 shows the alarm relationships based on the example in Figure 34-4.

Table 34-1 Alarm relationships

Object	Object alarms	Affecting alarms	Aggregated alarms	Related object alarms
NE1	alarmE1	—	alarmE2 alarmE3 alarmE4	—
shelf1	alarmE2	—	alarmE3 alarmE4	—
card1	alarmE3	—	alarmE4	—
port1	alarmE4	—	—	alarmA4
subscr1	alarmA1	—	alarmA2 alarmA3 alarmA4	—

(1 of 2)

Object	Object alarms	Affecting alarms	Aggregated alarms	Related object alarms
svc1	alarmA2	—	alarmA3 alarmA4	—
svcSite1	alarmA3	—	alarmA4	—
L2Int1	alarmA4	alarmE4	—	—

(2 of 2)

The 5620 SAM GUI uses color to indicate alarm severity. The color code is used consistently throughout the GUI, for example, in the navigation tree, dynamic alarm list, and topology maps. Table 34-2 lists the default alarm colors.

Table 34-2 Default 5620 SAM alarm colors

Alarm severity	Default color
Critical	Red
Major	Orange
Minor	Yellow
Warning	Cyan
Condition	Mocha
Cleared/Normal	Green
Indeterminate	White
Information	Light blue

The following tabs are on the Faults tab of an object properties form.

- Object Alarms—contains information about the alarm as viewed from the dynamic alarm list. For example, shelf1 is the object, and alarmE2 is the object alarm.
- Affecting Alarms—contains information about the alarms on objects that are directly affecting this object. For example, alarmE4 on object port1 is affecting object L2Int1, because of the relationship between the L2 interface and port1.
- Aggregated Alarms—contains alarm information for objects below the listed object in the containment hierarchy. For example, object shelf1 contains two propagated alarms, alarmE3 and alarmE4, because the shelf contains card1 and port1.
- Alarms on Related Objects—contains information about the alarms that have an indirect relationship with the object. For example, alarmA4 is displayed in the Alarms on Related Objects tab for port1, because it is related to the fault condition on port1.

Figure 34-5 shows the alarm status information for an object in the navigation tree, the object properties form, and the associated alarm information form. You can use the alarm information form to view the affected objects, the affecting objects, and the correlated alarms.

Note — In the navigation tree, an aggregated alarm may be present when no child object in the tree has an alarm. This is because the navigation tree is a filter for different views. When you change the view using the drop-down menu; for example, from Equipment to Network, the aggregated alarm on the child object may appear.

Figure 34-5 Alarm status information in the navigation tree

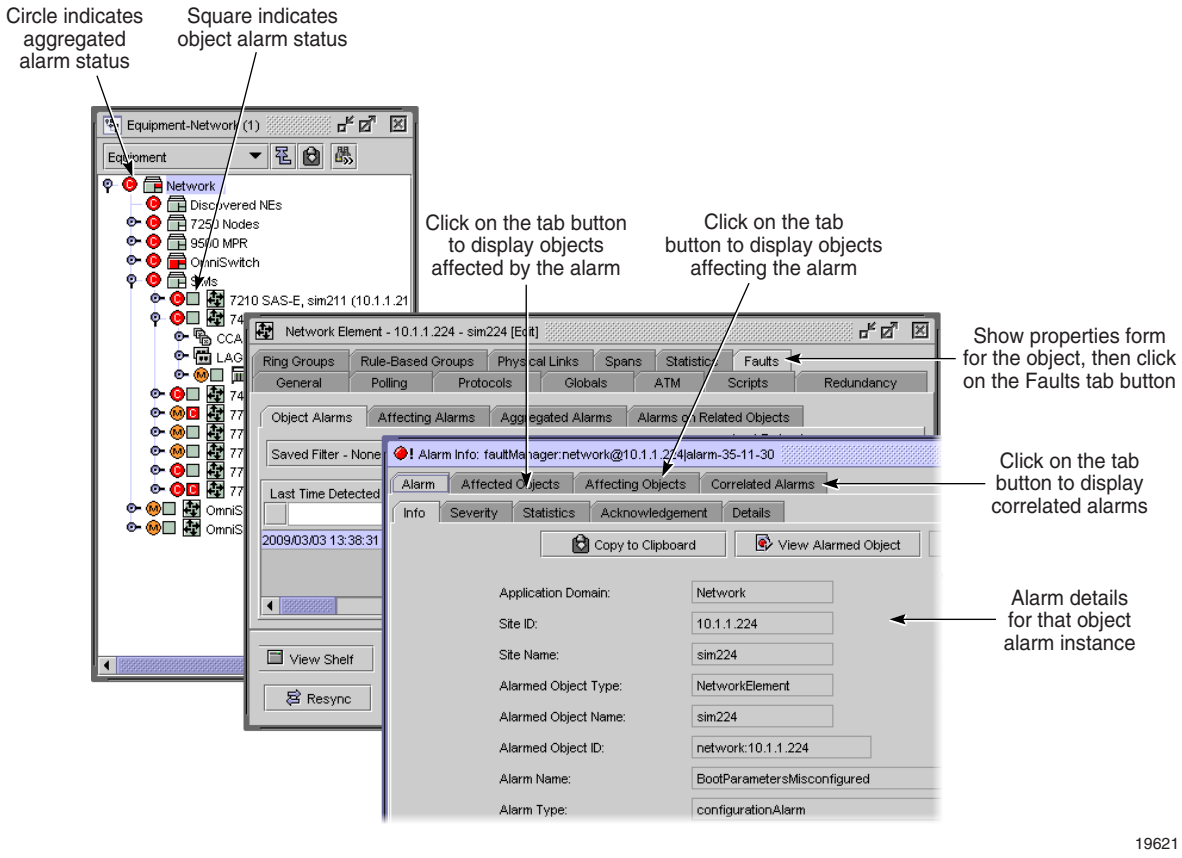
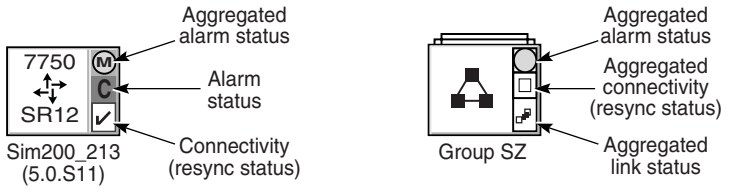


Figure 34-6 shows alarm and status information on a topology-map icon. See the *5620 SAM Troubleshooting Guide* for information about using topology maps for alarm management.

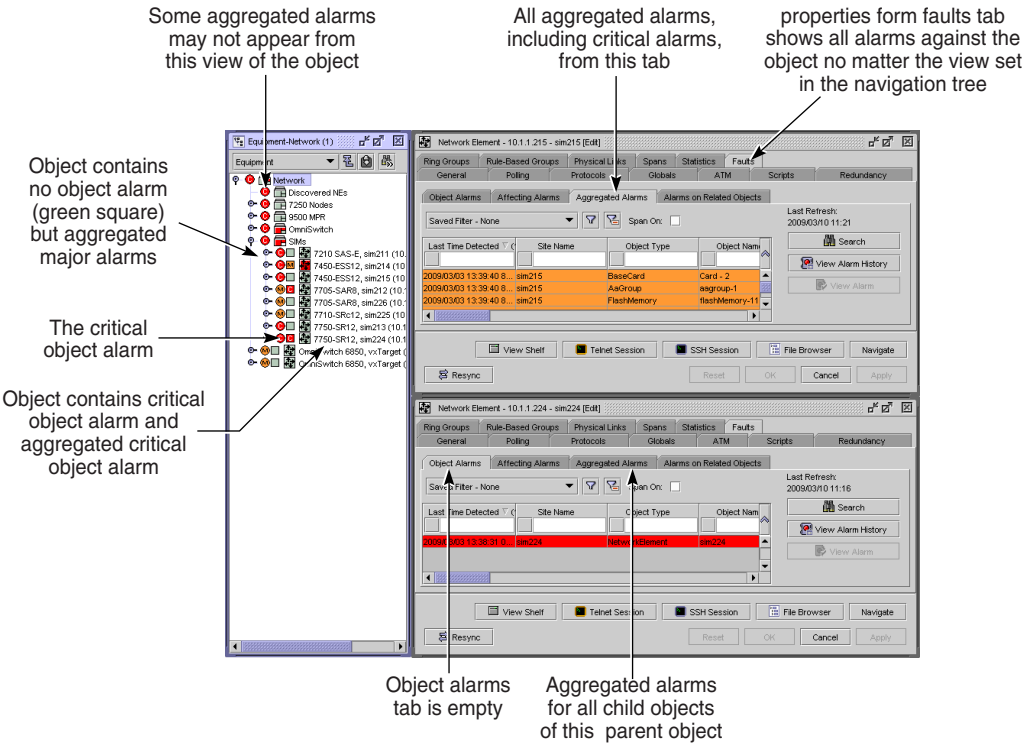
Figure 34-6 Alarm and status information on topology map icons



18022

Figure 34-7 shows how to navigate from the aggregated or object alarms in the navigation tree to the Faults tab of an object properties form.

Figure 34-7 Navigating from the navigation tree to Faults tab on a properties form



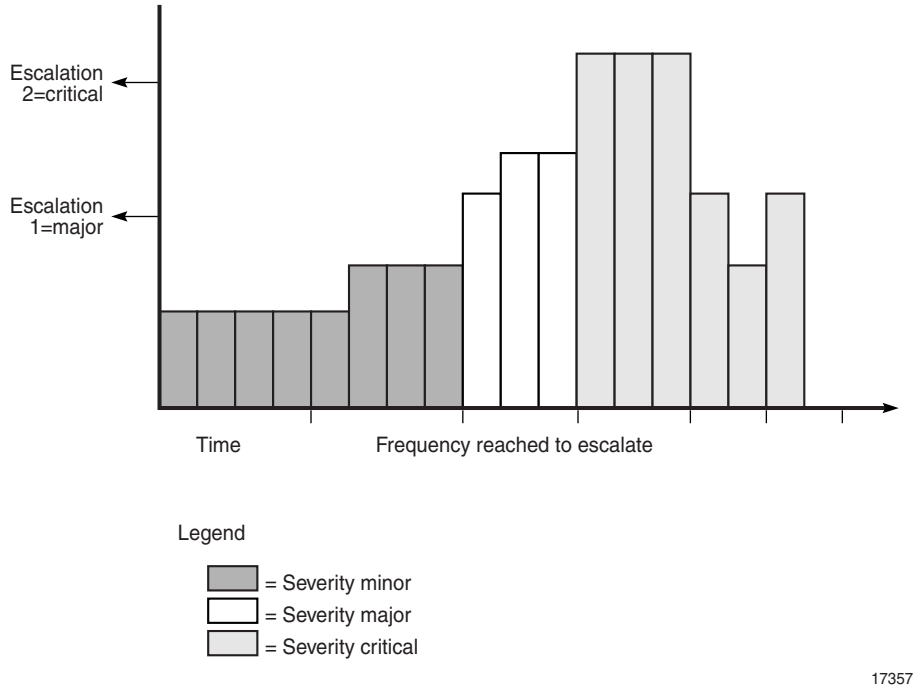
19622

Alarm thresholds

The 5620 SAM provides tools to escalate and de-escalate the severity of alarms using alarm threshold measures that are configurable using specific alarm parameters, as described in Procedure 34-3.

Figure 34-8 shows an example of what happens when an alarm threshold escalation is reached, and a policy is applied. Figure 34-9 shows two escalation and two de-escalation policies applied to an alarm.

Figure 34-8 Alarm thresholds without de-escalation policies

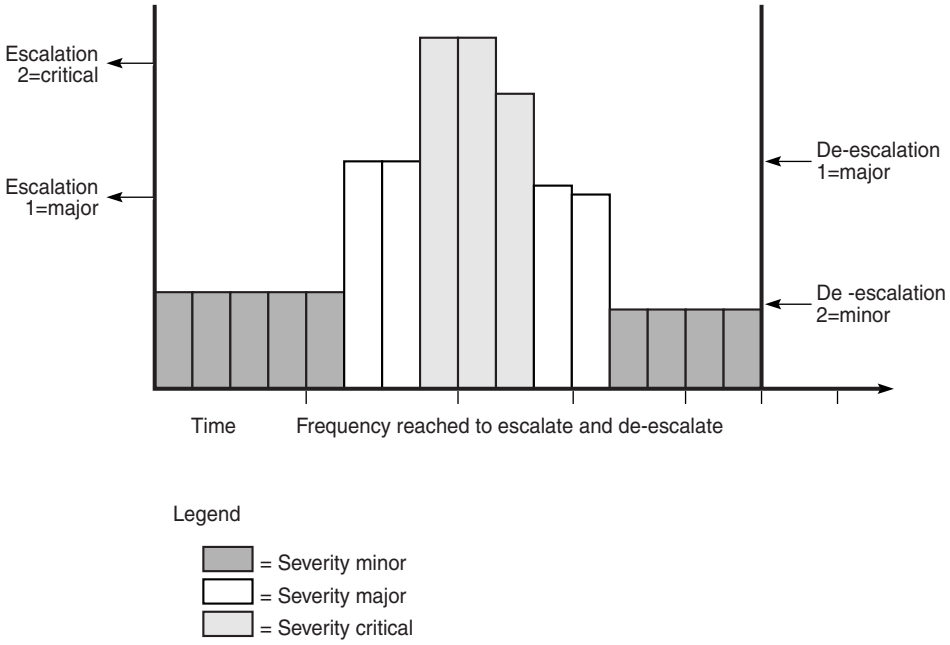


The preceding figure shows two escalation policies applied to an alarm. Escalation rules are applied when the number of instances of the alarm, also called the frequency, reaches the configured value. De-escalation rules are applied when the number of instances of the alarm drops below the configured frequency value. When the escalation value is reached, the alarm is escalated to the configured value. As shown in the figure, the first escalation is to major priority and then to critical priority. When the appropriate frequency to escalate and de-escalate is reached, the alarm is first escalated in severity and then de-escalated. However, if the alarm is deleted, then the frequency calculation is affected.

Note — When no de-escalation policy is applied, escalated alarms are not de-escalated once the frequency of the alarm drops below the alarm escalation threshold.

Figure 34-9 shows two escalation and two de-escalation policies applied to an alarm.

Figure 34-9 Alarm thresholds with de-escalation policies



Escalation policies are affected by the auto parameter of the global alarm deletion policy. See Procedure 34-1 for more information. When an escalation policy uses the "default when cleared" option, the escalation policy does not work. You must configure the parameter to a value other than "when cleared" to ensure the escalation policy is successful.

Alarm suppression

The 5620 SAM is designed to not raise alarms when numerous SNMP traps are sent in quick succession for the same type of event. This prevents alarm storms during intermittent outages in the network caused by bouncing NEs; for example, when links go up and down rapidly. The 5620 SAM continues to resynchronize the network, and if the bouncing NEs continue to send down state SNMP traps, the 5620 SAM eventually receives the trap and generates the appropriate alarm.

To indicate how often an alarm is raised, the number of occurrences of each instance of the alarm is tracked within the alarm record of the initial alarm. Click on the Statistics tab of an individual Alarm Info form to see how often the alarm was raised.

To cause alarm severity to escalate if an alarm reoccurs a specific number of times, use the threshold crossing alert functionality, as described in Procedure 34-3 using the escalation parameter or the de-escalation parameter.

The 5620 SAM uses a process called trap throttling to prevent the 5620 SAM system from being overloaded with traps when a failure occurs. Trap throttling does not affect the sequencing of traps. The trap throttling process allows the 5620 SAM software to process traps when it has the time. As a result, the 5620 SAM software knows which traps the software missed and resynchronizes only those traps. Trap throttling is supported and configured through the CLI on each Alcatel-Lucent NE. See the Alcatel-Lucent NE System Management Guides for configuration instructions.

Correlated alarms

The 5620 SAM raises a correlated alarm when a fault condition on one object causes an alarm condition on another object. For example, when a port goes down, an alarm is raised against the port, which is the affected object, and each service that uses the port generates an alarm.

The alarm information for the affected object includes the correlated alarms. See Procedure 34-9 for information about viewing correlated alarms.

When the event that triggers an affected-object alarm is corrected and the alarm clears, the correlated alarms also clear. If a correlated alarm does not clear after the affected-object alarm clears, the source of the correlated alarm is an event other than the trigger event. In this case, the alarm correlation is removed and the alarm is displayed in the dynamic alarm list.

You can suppress the display of correlated alarms to reduce the number of alarms that appear in the dynamic alarm list. Correlation alarm suppression is enabled by default. See Procedure 34-6 for more information.

Note — Correlation alarm suppression does not affect the alarm status displayed in the navigation tree and topology map.

You can configure the 5620 SAM to automatically delete correlated alarms when the correlating alarm is deleted. You can also configure 5620 SAM alarm settings to specify whether a user notification is displayed when one or more correlated alarms is about to be deleted. See Procedure 34-1 for information about configuring the automatic deletion of correlated alarms.

Note — A correlated alarm remains after the deletion of the correlating alarm if there is another correlating alarm associated with it. For this reason, the number of correlated alarms that are automatically deleted may be fewer than the number stated in the warning notification presented to a GUI operator.

Service and transport alarm correlation

The 5620 SAM provides limited service and transport alarm correlation. When an LSP goes out of service, the 5620 SAM raises an alarm against the LSP and raises a correlated alarm against each LSP path that is a child object of the LSP. The LSP alarm is listed as an aggregated alarm for each SDP that uses the LSP. A 5620 SAM operator can use the aggregated LSP alarm for SDP troubleshooting.

Because there is not necessarily a direct relationship between an LSP and the SDPs that use it, for example, when LDP over RSVP is the transport mechanism, the 5620 SAM does not correlate SDP alarms with LSP alarms.

Automatic purging of alarms

Large numbers of outstanding alarms can affect system performance. Therefore, outstanding alarms are purged based on the severity, correlation status, and age of the alarm. If the system limit of 60 000 is reached, alarms are purged to the historical alarm log until the alarm count drops to 45 000. Other automatic purging of alarms is not necessary when historical alarm logging and purging policies are configured, as described in Procedure 34-2.

The alarm purge algorithm sorts alarms based on the following criteria:

- correlated alarms are deleted before the root alarms are deleted
- lower severity alarms are deleted before higher severity alarms are deleted
- oldest alarms are deleted first

When alarm policies are not configured, the system purges alarms in this sequence:

1 When the outstanding alarm count reaches 50 000, non-critical and non-root alarms are purged to the historical alarm log until the alarm count drops to 45 000.

2 An alarm is raised to indicate an alarm purge is in process.

3 When the outstanding alarm count reaches 60 000, alarms are purged to the historical alarm log until the alarm count drops to 45 000.

4 An alarm is raised to indicate an alarm purge.

To ensure purged alarms are logged, you must set up historical alarm logging, as described in Procedure 34-2.

34.2 Workflow to manage alarms

1 Set up the managed NEs to send SNMP traps of managed NE faults and events to the 5620 SAM. See the appropriate NE documentation for more information.

2 Set alarm policies on the 5620 SAM using Administration→Alarm Settings.

i Set global policies for incoming alarms.

ii Set specific policies for each alarm type.

iii Set additional text policies.

iv Set alarm history database behavior for the storage of historical alarm records.

3 Set alarm user preferences.

4 Monitor alarms:

i For SLAs by monitoring SAP and service alarms from the appropriate properties form or manage services form.

ii For each piece of equipment or logical component using the Faults tab button from each equipment form, logical component form, or from the navigation tree equipment view.

iii For the network from the dynamic alarm list.

iv For incoming SNMP traps from managed NEs by viewing logs.

For information about troubleshooting using alarms see the *5620 SAM Troubleshooting Guide*.

5 Reload alarms to ensure the alarm service cache is refreshed, as required by the system administrator. This step can only be performed by a user with an account that is assigned the administrator scope of command role or a scope of command role with write access permissions to the fm.FaultManager class, and should only be done when necessary.

6 Reset alarm policy based on changing network and new alarm support requirements.

7 Review historical alarm records in the alarm history log database for trends and store the alarms for record-keeping.

34.3 Alarm management procedures

Use the following procedures to perform fault management tasks.

Procedure 34-1 To set global alarm policies

Global alarm policies affect all network alarms and can be set by users who are assigned an account with either the administrator scope of command role or a scope of command role with write access permissions to the fm.GlobalPolicy class.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens with the General tab displayed.

2 Click on the Alarm Behavior tab button.

3 Set the severity policies by clicking on the Severity tab button.

i Enable the Severity Alterable parameter to enable setting the severity parameters. When you enable severity alterable functionality, you can specify whether to allow automatic changes to severity based on individual alarm policies or manual changes to severity based on operator actions.

Severity settings cannot be altered unless the check box is enabled.

ii Configure the parameters.

- manual severity alterations
- severity promotion
- severity demotion
- clearing (if self-clearing alarm)
- automatic severity alterations
- implicit severity promotion
- implicit severity demotion
- escalation (defined by specific policy)
- de-escalation (defined by specific policy)

4 Set the deletion policies by clicking on the Deletion tab button:

i Enable the Alarm deletion parameter to allow the creation of a deletion policy.

Deletion policies cannot be changed unless the check box is enabled.

ii Choose the appropriate deletion policy. When you enable deletion functionality, you can specify whether to allow operators to delete alarms or allow the automatic deletion of alarms.

Configure the parameters.

- manual
- auto
- automatic deletion of correlated alarms

Caution — Deleting an alarm resets the frequency of an alarm to 1. This may cause conflicts with configured alarm escalation and de-escalation policies.

5 Click on the Apply button to save the changes. A dialog box appears.

6 Click on the Yes button to proceed.

7 Click on the Cancel button to close the form.

Procedure 34-2 To set alarm history behavior

The 5620 SAM stores new and old alarms in the alarm history database for record-keeping and trend analysis. You can specify how alarms are stored in the database.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens with the General tab displayed.

2 Click on the Alarm History DB Behavior tab button.

3 Set the alarm history behavior.

a Configure the parameters.

- Max Log Size (records)
- Administrative State
- Log On Change
- Log On Deletion

Note — Alcatel-Lucent recommends enabling the Log on Deletion parameter to ensure historical log records of all deleted alarms exists.

b Purge alarms from the historical alarm database using the Purge All or Purge Range button. The Purge Range button can be used when a filter policy is applied by selecting the Set Purge Range button.

Caution — Using the Purge All button removes all alarm history records from the historical alarm database.

i Click on the Set Purge Range button. The Alarms Settings Filter form appears.

ii Specify a filter that to be used as the purge criteria. For example, to purge the alarm history database of all minor alarms, set the Severity filter to equal minor.

iii Click on the OK button. The Alarms Settings Filter form closes.

iv Click on the Purge Range button.

v A dialog box appears. Click on the Yes button to proceed.

The historical alarm database is purged of those alarm history records which met the purge criteria.

When the maximum number of alarms allowed in the alarm history database is reached, the oldest alarms are deleted. If you want to save information about those alarms, save a file containing the alarm log information, as described in Procedure 34-18.

Procedure 34-3 To set specific alarm policies

Specific alarm policies allow you to modify the behavior of one or more specific types of alarms, if you want that alarm to behave differently than the default.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens.

2 Click on the Specific tab button. A list of alarm types appears.

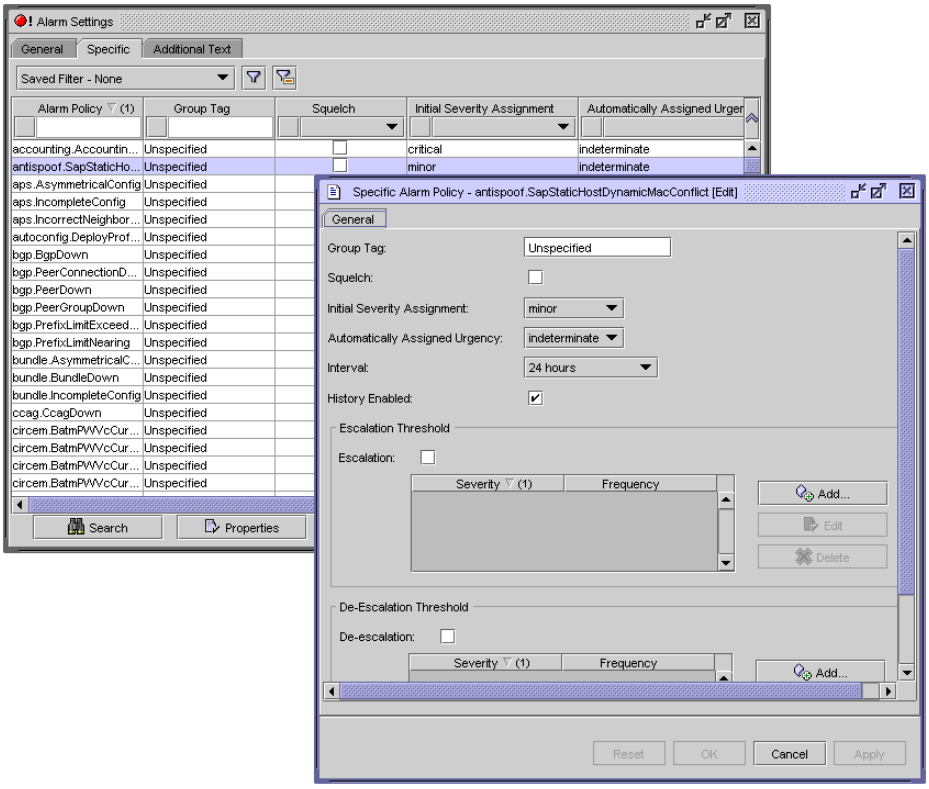
3 Choose an alarm type. Alternatively, you can select multiple alarms at the same time.

The alarm types are listed by *domain.alarm name*.

4 Click on the Properties button. The SpecificPolicy form for that alarm type opens.

Figure 34-10 shows a single alarm type (bgp.PeerDown) selected in the list, and its sample configuration form.

Figure 34-10 Alarm type configuration form opened from the Alarm Policy specific tab button



5 Configure the general alarm type parameters.

- Group Tag
- Squelch
- Initial Severity Assignment
- Automatically Assigned Urgency
- Interval
- History Enabled

6 Configure the alarm type escalation parameters. Select the Escalation or De-escalation check boxes to escalate or de-escalate the severity of an alarm based on how frequently that alarm is processed by the 5620 SAM.

i Select the Escalation parameter or the De-Escalation parameter.

ii Click on the Add button.

iii Configure the Frequency parameter. This is the threshold in a 24-hour period of how often the alarm must arrive before the severity is escalated or de-escalated.

The alarms are analyzed at faster, non-configurable intervals to verify whether the Frequency value is reached.

iv Configure the Severity parameter to specify the new severity applied against the alarm if the escalation or de-escalation threshold is reached.

v Click on the OK button.

The new escalation or de-escalation policy is applied to the alarm.

7 Click on the OK button to save the changes and close the SpecificPolicy form. A dialog box appears.

8 Click on the Yes button to proceed.

Procedure 34-4 To configure audible alarms

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Turn on Audible Alarms parameter.

3 Click on the OK button. The User Preferences form closes, and the audible alarm option is applied.

Procedure 34-5 To configure alarm flags

The Monitoring Flag panel under the Alarm Table tab indicates the number of alarms, color-coded by severity, that have been detected since the flag was reset. The time the last alarm for that severity was detected is also displayed. You can show or hide alarm flags the Monitoring Flag panel using the User Preferences form.

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Show Alarm Flags parameter.

3 Click on the OK button. The User Preferences form closes, and the Monitoring Flag panel appears in the dynamic alarm list Alarm Window.

Procedure 34-6 To enable or disable the display of correlated alarms

Note 1 — The display of correlated alarms may slow GUI performance while the 5620 SAM adds the alarms to the dynamic alarm list.

Note 2 — When you disable the display of correlated alarms in the dynamic alarm list, the correlated alarms are still listed in the Correlated Alarms tab of the Alarm Info form.

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Show Correlated Alarms parameter.

Note — The Alarm Window title bar displays Correlated Alarms Not Shown when correlated alarm display is disabled.

3 Click on the OK button. The User Preferences form closes, and the correlated alarm option is applied.

Procedure 34-7 To create additional text policies

Create an additional text policy to display specific information about an alarmed object in the additional text field of the dynamic alarm list and on the Alarm Info form.

1 Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form opens with the General tab displayed.

2 Click on the Additional Text tab button.

3 Configure the additional text policies. Perform the following steps:

i Click on the Create button. The Additional Text Policy (Create) form opens with the General tab displayed.

ii Click on the Select button beside the Domain parameter. The Select affected object's domain form opens.

iii Select a domain from the list and click on the OK button. The Select affected object's domain form closes and the Additional Text Policy (Create) form reappears.

iv Click on the Select button beside the Object Type parameter. The Select affected object's object type form opens.

v Select an object type from the list and click on the OK button. The Select affected object's object type form closes and the Additional Text Policy (Create) form reappears.

vi Configure the parameters:

- Description
- Overwrite existing

4 Configure the additional text attributes. Perform the following steps:

i Click on the Additional Text Attributes tab button.

ii Click on the Create button. The Additional Text Attribute (Create) form opens.

iii Click on the Select button beside the Attribute Name parameter. The Select affected object attribute form opens.

iv Select an object attribute from the list and click on the OK button. The Select affected object attribute form closes and the Additional Text Attribute (Create) form reappears.

v Configure the Order parameter.

vi Click on the OK button. The Additional Text Attribute (Create) form closes and a dialog box appears.

vii Click on the OK button to confirm the action.

viii Click on the OK button to save the configuration. The Additional Text Policy (Create) form closes and the text policy appears in the list on the Alarm Settings form.

5 Close the form.

Procedure 34-8 To view alarms raised against equipment, logical components, and services

Alarms raised against network objects allow you to view faults on each NE in the network down to the service, path, or port level. The 5620 SAM analyzes all incoming alarms to ensure that the alarms are listed against the appropriate equipment or service. This feature is useful when you troubleshoot an equipment or service problem.

Objects that can have alarms issued against them contain a Faults tab button. The tables in the Faults tab button list the alarms issued against the specific equipment or service. For some forms, the Faults tab is further broken down into the Object Alarms, Affecting Alarms, Aggregated Alarms, and Alarms on Related Objects tabs. These tabs show alarms against specific objects, such as ports, and related problems, such as services that use the ports.

1 Choose:

   a Application→Equipment Window from the 5620 SAM main menu to view equipment alarms. The Equipment Window form opens. Choose an NE from the drop-down list.

   b Another menu that displays a path, logical component or service form.

2 Click on the Faults tab button. A list of alarms appears under the appropriate tabs. Click on an appropriate tab button to display alarms of interest.

3 Review the alarm information. See Table 34-3 for the type of information available in an alarm. Scroll across each line to view the information contained in the alarm.

4 To view a specific alarm, double-click on the line or click on the View Alarm button to open the Alarm Info form. See Table 34-3 for the alarm information available under all tabs in the form.

5 Click on the View Alarmed Object button to open the properties form for the alarmed object.

6 Handle alarms according to your fault management policies. For information about troubleshooting using alarm information guidelines see the *5620 SAM Troubleshooting Guide*.

Procedure 34-9 To view alarm information

Alarm information is available from:

- the dynamic alarm list
- the equipment window fault tab alarm list
- the navigation tree
- policy, service, and other properties form Fault tabs
- the Manage Services and service properties forms, to use in conjunction with the service ID to determine which customer is affected by which service alarms
- the Alarm Info form that opens when you double-click on a row in the alarm list

You must ensure that you are on the correct form to view alarms. For example, you cannot view ping management connection alarms from the Discovery Manager configuration form even through that is the form on which you perform the pings, or the NE discovery control form, even though that is the form on which you choose the ping policy. You must navigate to the appropriate object form to find the alarms, which, in this example, is an NE properties form.

1 Click on the Faults tab button of an NE properties form to list the alarms.

2 Click on the appropriate fault tab button.

The fault tabs contain other tabs that list alarms against the specific object, alarms on objects that are directly affecting the object, aggregated alarms, and alarms against related objects that affect the specific object.

3 Open a listed alarm by selecting the alarm entry and clicking on the View Alarm button. Alternatively, you can double-click on the alarm entry.

Note — When sorting alarms, sorting more than 15 000 outstanding or logged alarms may slow GUI performance. Use filters to return a reasonable number of alarms. Creating search filters for network alarms is described in Procedure 34-13.

4 Review the alarm information.

a View the alarm information in each tab and respond according to your alarm-handling policies.

Table 34-3 lists the types of alarm information available to users from the Alarm Info form. For information about troubleshooting using alarm information guidelines see the *5620 SAM Troubleshooting Guide*.

Table 34-3 Alarm Info form fields

Field	Information
Alarm tab on Alarm Info form, Info tab displayed	
Domain	The general area of the 5620 SAM software that is affected by the alarm. This is of specific interest and use to those monitoring alarms using the XML OSS interface. See the *5620 SAM-O OSS Interface Developer Guide* for more information.
Application domain	
Site ID	IP address of the NE that raises the alarm
Site Name	Name of the NE
Object Type	Type of object
Alarmed Object Type	
Object Name	Name of the object
Alarmed Object Name	
Object Id	Unique string identifying the object down to the lowest level, for example, network ID #, chassis #, slot #, daughterCardSlot #
Alarmed Object Id	

(1 of 3)

Field	Information
Alarm	Name of the alarm
Alarm Name	
Time Detected	When the alarm was raised
Type	Vendor-specific and X.733 standards for the event type of the alarm
Alarm Type	
Severity	Vendor-specific, TMN, and X.733 standards for severity of the alarm
Alarm Severity	
OLC State	Configured OLC state
Cause	Vendor-specific and X.733 standards for the probable cause of the alarm
Probable Cause	
Ack	Whether the alarm has been acknowledged by an operator (true) or not (false)
Acknowledged	
Acknowledged By	Name of operator that acknowledged the alarm
Cleared By	Name of operator that last cleared the alarm
Urgency	Urgency setting of the alarm
Additional text	Any extra text included with the alarm
First Time Detected	Time of the first recorded instance of the alarm
Last Time Detected	Time of the last recorded instance of the alarm. This field provides useful information when multiple instances of the same alarm are raised. As each new instance of the alarm is raised, the number of occurrences statistic increases, and Last Time Detected shows the time that the last instance of the alarm was raised.
Number of correlated alarms	Number of correlated alarms
Correlating Alarm ID	Unique string that identifies the correlating alarm object down to the lowest level
Alarm tab on Alarm Info form, Severity tab displayed	
Severity details Cleared details Promoted details Escalated details	Information about alarm severity. You can modify the alarm severity by clicking on the View Policy button. You can delete, clear to the historical database, acknowledge, or view the history of the alarm.
Alarm tab on Alarm Info form, Statistics tab displayed	
Frequency Number of Occurrences Number of Occurrences Since Clear Number of Occurrences Since Acknowledged	You can modify the alarm frequency by clicking on the View Policy button and modifying the individual alarm settings. How often the alarm has been raised, based on the specified scenarios. As each new instance of the alarm is raised, the number of occurrences statistic increases, and the Last Time Detected field shows the time that the last instance of the alarm was raised. You can delete, clear to the historical database, acknowledge, or view the history of the alarm.

(2 of 3)

Field	Information
Acknowledgement tab on Alarm Info form, Acknowledgement Info tab displayed	
Acknowledged Acknowledged by Last Time Acknowledged Previously Acknowledged Assigned Urgency Urgency Assigned By	Information about when the alarm was acknowledged, the user that acknowledged the alarm, and the user that set the urgency. You can modify the acknowledgement and urgency by clicking on the View Policy button and modifying the individual alarm settings. The Previously Acknowledged parameter specifies that the alarm had been previously acknowledged. You can delete, clear to the historical database, acknowledge, or view the history of the alarm.
Acknowledgement tab on Alarm Info form, Notes tab displayed	
View button Properties button New button Note tab button Revision History tab button	Create notes by clicking on the New button and entering the note. You can edit or view notes from the same form. Information about the note, including the time created and the name of the user who created the note, are displayed in rows for each note entered. Click on the Revision History tab button to view all notes created for the alarm. Select a note from the list and click on the View button to view the note.
Alarm tab on Alarm Info form, Details tab displayed	
Description Raising Condition Clearing Condition	A description of the alarm. Raising condition for the alarm. Clearing condition for the alarm.
Affected Objects tab on Alarm Info form	
Show Object(s) button Refresh button	Lists the objects that are affected by the alarm. Choose an affected object from the list and click on the Show Object button to open the properties form for the object.
Affecting Objects tab on Alarm Info form	
Show Object(s) button Refresh button	Lists the objects that directly affect the object in alarm. Choose an affecting object from the list and click on the Show Object button to open the properties form for the object.
Correlated Alarms tab on Alarm Info form	
Show Alarm(s) button Refresh button	Lists the objects that directly affect the object in alarm. Choose a correlated alarm from the list and click on the Show Alarms button to open the Alarm Info form for the correlated alarm.

(3 of 3)

b Click on the Affected Objects tab button to view other network objects that are affected by this alarm. Choose an object and click on the Show Object(s) button to open the properties form for the affected object.

For example, a service tunnel alarm is raised. From the Alarm Info form, click on the View Alarmed Object button to go directly to the properties form for that service tunnel. The properties form opens. Click on the Faults tab button to see the same alarm listed under the Object Alarms tab button.

c Click on the Affecting Objects tab button to view other network objects that affect this object. Choose an object and click on the Show Object(s) button to open the properties form for the affecting object.

d Click on the Correlated Alarms tab button to view correlated alarms. Choose an alarm and click on the Show Alarm(s) button to open the Alarm Info form.

5 Handle the alarm according to your alarm-handling policy.

a Click on the Delete button to delete the alarm, if you have permissions to delete alarms. Click on the Yes button to confirm the action, and then click on the OK button.

Caution — You cannot recover a deleted alarm, unless deleted alarms are configured to be logged in the alarm history database, as described in Procedure 34-2.

b Click on the Clear button to clear the alarm. Click on the Yes button to confirm the action, and then click on the OK button. The alarm is cleared from the list, and is added to the alarm log as an alarm history record, if configured.

Note — Some alarms are self-clearing, which means that they are automatically cleared from the alarm list after the condition that triggered the alarm is no longer present. The dynamic alarm list contains an Implicitly Cleared attribute that identifies the self-clearing alarms.

c Click on the Acknowledge button to acknowledge the alarm.

i From the Notes tab, modify the urgency and assigned severity of the alarm, if required. You need permissions to modify the alarm.

ii From the Notes tab, add a note to the alarm, if required.

You can also choose a note from the list, click on the Properties button, and modify the note by setting the Reason for change and Detailed Text parameters.

iii Click on the Apply button to save the changes and acknowledge the alarm. If you added a note, the note appears in the list of notes.

When you view the alarm again, the acknowledgement information is updated to include:

- the user that acknowledged the alarm
- when the alarm was acknowledged
- whether the alarm had already been previously acknowledged
- any changes to the assigned urgency of the alarm

iv If required, you can click on the Revision History tab button and view a revised note. The revised note information includes:

- date modified
- user that modified the note
- reason for the note change
- an explanation of the note change
- contents of the note before and after the modification

d Click on the View Policy button. The Specific Policy form opens for that alarm type. You can view the policy configured for the alarm type, as described in Procedure 34-3.

e Click on the View Alarm History button to view the alarm history for this type of alarm. An Alarm History form appears with the Alarm Name filter equal to the type of alarm you are viewing.

i Click on the Search button. A list of alarm history records appears based on the filter.

ii Choose the record from the alarm history database log, as described in Procedure 34-17.

Procedure 34-10 9500 MPR Error Recovery Mechanism

This procedure applies to cleaning up inconsistencies created due to MIB population failures which can occur during service creation on 9500 MPR NEs. Inconsistencies on these NEs can be detected during full NE synchronization or on opening the NE properties form. The user will be notified by an implicitly cleared alarm with a Warning severity level on the NE.

1 Right-click on a 9500 MPR NE instance, and select Properties from the drop-down menu. A Network Element (Edit) form opens.

2 If there are NE inconsistencies, a Cleanup Inconsistencies button will appear on the form.

3 Click on the Cleanup Inconsistencies button.

4 Click on the Faults tab button of the Network Element (Edit) form to check for any remaining NE inconsistency alarms.

Note — For failures during 9500 MPR service creation the user should, after clearing the deployer, perform the following:

- A full resynch of the NEs on which service creation failure has occurred in order to restore existing NE entries
- Perform Procedure "9500 MPR Error Recovery Mechanism" to clean up inconsistencies.
- Complete the service by clicking on the Complete Service button.
- It is recommended that the inconsistencies be cleaned up prior to any new service creation.

Procedure 34-11 To copy alarm information to a buffer

The alarm information copied to the buffer of your PC or workstation can be pasted in other applications. This function helps you share the alarm information for troubleshooting purposes.

1 Click on the Faults tab button of an NE properties form to list the alarms.

2 Click on the appropriate fault tab button.

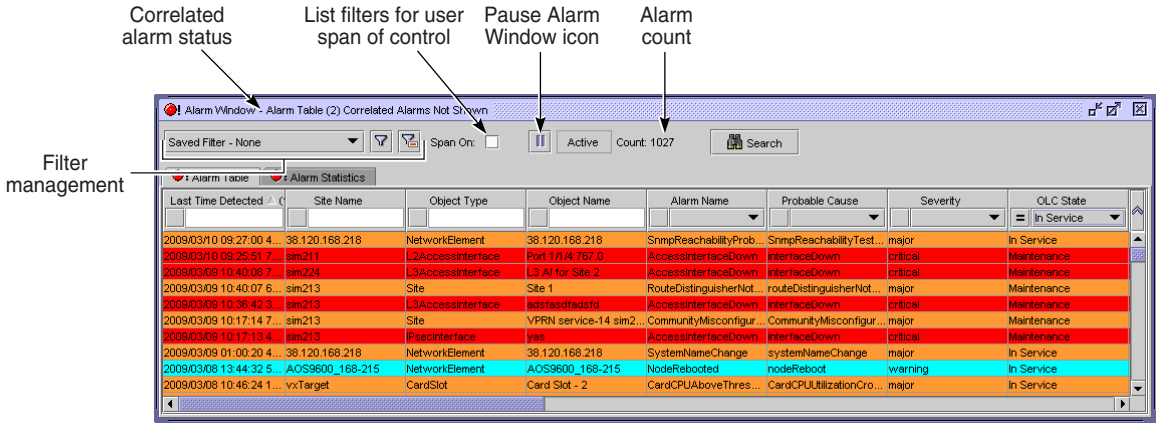
3 Open a listed alarm by selecting the alarm entry and clicking on the View Alarm button. Alternatively, you can double-click on the alarm entry.

4 Click on the Copy to Clipboard button. You can also use the contextual menu in the Alarm Window to copy the alarm information to the clipboard.

Procedure 34-12 To view all network alarms using the dynamic alarm list

The dynamic alarm list Alarm Window allows you to monitor incoming faults from the NEs and 5620 SAM software. This feature is most useful when monitoring the network. Figure 34-11 shows the dynamic alarm list Alarm Window.

Figure 34-11 Dynamic alarm list Alarm Window



19623

1 Click on the Alarm Table tab button in the Alarm Window. The dynamic list of incoming network alarms appears.

Note — You can open and view up to six alarm windows. This is useful when you need to view multiple filtered incoming network alarms.

2 Filter the alarms, if required.

Note — Sorting more than 15 000 outstanding or logged alarms may slow GUI performance. Use filters to return a reasonable number of alarms.

a Choose a filter from the Save Filter drop-down list.

b Create a filter. See Procedure 34-13 for more information.

c Choose an OLC filter from the OLC Filter drop-down menu.

d Choose a severity filter from the Severity Filter drop-down menu.

3 Right-click on one or more alarms in the list. The contextual menu appears.

4 Choose:

a Show Alarm(s) to view the Alarm Info form for each selected alarm. Table 34-3 lists the alarm information displayed.

b Show Affected Object to display the configuration or property form for the object or objects against which the alarm or alarms is raised.

c Acknowledge Alarm(s) to open the alarm acknowledgement form for the alarm or alarms. Enter acknowledgement text, if required, and click on the OK button. Confirm the action. The acknowledgement information is added to the alarm info form, and any acknowledgement text is added to the Notes tab. The Acknowledged By column in the Alarm table indicates the user who acknowledges the alarm.

d Assign Severity to change the severity policy of the alarm using the Assigned Severity parameter. Click on the OK button. Confirm the action.

e Assign the OLC State to the alarm.

f Delete Alarm(s) to delete an alarm or alarms. Confirm the action to delete the alarm or alarms. The alarm or alarms are deleted and added to the alarm history database log as an alarm history record, if configured.

Caution — You cannot recover a deleted alarm, unless the alarm is configured to be logged on deletion, as described in Procedure 34-2.

g Clear Alarm(s) to clear the alarm or alarms. Confirm the action to clear the alarm or alarms. The alarm or alarms are cleared and added to the alarm history database log as an alarm history record, if configured.

h NE Sessions→*option* to start a SSH or Telnet session with the managed equipment that generated the alarm.

i Show Sorting to determine the sort order of how alarm information is displayed:

i Use the left, right, up, and down arrows to resequence the alarm fields as required.

ii Click on the Sort Ascending and Sort Descending buttons to specify the order of displayed alarms.

iii Click on the Close button to return to the dynamic alarm list.

j Copy to Clipboard to copy the alarm information to the buffer of your PC or workstation.

5 Handle the alarm(s) according to your fault management policies. Alarm handling is described in Procedure 34-9. For information about troubleshooting using alarm information guidelines see the *5620 SAM Troubleshooting Guide*.

Procedure 34-13 To create search filters for network alarms

You can create and select filters to view specific network alarms in the dynamic alarm list. You can save multiple filters and view the alarm information by opening up to 6 alarm windows. The name of the filter appears in the alarm window title of each alarm window that is open. Viewing network alarms using the dynamic alarm list is described in Procedure 34-12. Figure 34-11 shows the location of the Manage Filters icon in the alarm window.

Note — The FDN extension of a generic NE alarm is not appended to the Alarm Name field in the 5620 SAM GUI, but is included in the Additional Text field. To create a filter for generic NE alarms that have FDN extensions, you must filter on the Additional Text field.

1 Choose Application→Alarm Window. The Alarm Window opens.

2 Click on the Filter icon beside the filter drop-down list. The Alarm Window filter form opens.

3 Configure the filter criteria.

4 Click on the Add button. The Save Filter form opens.

5 Click on the Save button. The Save Filter form opens.

6 Configure the parameters:

- Filter Name
- Description
- Public

7 Click on the Save button. The Save Filter form closes and the Alarm Window filter form reappears.

8 Close the Alarm Window filter form.

9 Click on the filter drop-down list. The saved filter is shown in the list.

10 Click on the saved filter to load and view the results of the filtered search in the dynamic alarm list. The number of alarms associated with the selected search filter appears in the Count field, as shown in Figure 34-11.

Procedure 34-14 To change the severity filter from the alarm window

1 Click on the Alarm Table tab button in the Alarm Window. The dynamic list of incoming network alarms appears.

2 If required, click on the filter icon to create a filtered list of alarms. See chapter 2 for more information about creating search filters.

3 Right-click on the alarm, a drop down menu appears.

4 Choose Assign Severity. A Severity Assignment window opens.

5 Choose one of the following options. The alarm table panel is refreshed with a filtered list of alarms.

- Severity Filter - None
- cleared
- indeterminate
- info
- condition
- warning
- minor
- major
- critical

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The Severity Assignment window closes.

Procedure 34-15 To pause the dynamic alarm listing

New incoming alarms are added to the dynamic alarm list, with the most recent alarm shown first. If you are viewing an alarm from the dynamic alarm list, new incoming alarms may cause the alarm list to scroll automatically. You can pause the dynamic alarm list to prevent this. Figure 34-11 shows the location of the Pause Alarm Window icon in the Alarm Window.

1 View alarms from the dynamic alarm list, as described in Procedure 34-12.

2 Click on the Pause Alarm Window icon. The icon changes to indicate that the dynamic alarm list Alarm Window is locked for viewing. The icon box changes to red and the text changes to Paused.

Incoming alarms are not added for the duration of the pause.

3 Click on the Pause Alarm Window icon to unlock the dynamic alarm list Alarm Window. The icon changes to indicate the dynamic alarm list Alarm Window is active. The icon box changes to gray and the text changes to Active. Any alarms that occurred during the pause appear in the dynamic alarm list.

Note — You can also scroll lock the dynamic alarm list by highlighting a specific alarm. New incoming alarms appear above the selected alarm, but the selected alarm continues to be selected in the dynamic alarm list. Use the down scroll bar to find the selected alarm.

Procedure 34-16 To view network alarm statistics

1 Click on the Alarm Statistics tab button in the Alarm window. The alarm statistics table appears.

2 View the alarm statistics information.

The Alarm Statistics table lists the number of network alarms sorted in columns by acknowledged and unacknowledged status, and then by the number of critical, major, minor, warning, condition, info, indeterminate, and cleared alarms.

Procedure 34-17 To review historical alarm records

Alarms are logged as historical alarm records in an alarm log database.

1 Choose Tools→Historical Alarms from the 5620 SAM main menu. The Alarm History form opens.

2 If required, specify a filter to narrow the range of historical alarms displayed.

Note — When sorting alarms, sorting more than 50 000 outstanding or logged alarms may slow GUI performance. Use filters to return a reasonable number of alarms. Creating search filters for network alarms is described in Procedure 34-13.

3 Click on the Search button. The list of historical alarm records appears based on the filtering criteria.

4 Select an alarm history record from the list.

5 Click on the Properties button to review the alarm. The alarm history object form appears.

Table 34-3 lists the information displayed for each historical alarm record. Table 34-4 lists the additional historical alarm information available from the alarm history form for logged alarms.

Table 34-4 Alarm information from the Alarm History Object form

Alarm field	Information
Info tab on Alarm History Object form	
Alarm Status	Reason the alarm was logged to the historical alarm database
Last Time Acknowledged	Last time the alarm was acknowledged
Deleted By	Name of operator that deleted the alarm
Time Logged	Timestamp when alarm was moved to the historical alarm database

(1 of 2)

Alarm field	Information
Info tab on Alarm History Object form	
Highest Severity	The most severe status assigned to the alarm. Alarm severity can change due to escalation policies
Number Of Occurrences	How often the alarm was raised
Severity tab on Alarm History Object form	
Detected details Urgency details	Information about the alarm severity

(2 of 2)

6 Manage the logged historical alarm records.

i Click on the Cancel button to close the Alarm History Object form. The Alarm History form reappears.

ii Choose an alarm history record from the list.

iii Click on the Properties button. The AlarmHistoryObject form opens.

iv Click on the View Policy button to view the Specific Policy form. See Procedure 34-3 for more information.

v Click on the Purge Filtered button to purge alarms that meet the purging criteria. Click on the Yes button to confirm the action.

Caution — You cannot recover alarms purged from the historical alarm database log. If you want to save information about those alarms, save a file containing the alarm history database log details, as described in Procedure 34-18.

7 Close the Alarm History form.

When the maximum number of alarms allowed in the alarm log is reached, the oldest alarms are deleted. If you want to save information about those alarms, save a file containing the alarm log details, as described in Procedure 34-18.

Procedure 34-18 To save lists of logged historical alarm records

1 Choose Tools→Historical Alarms from the 5620 SAM main menu. The Alarm History form opens.

2 If required, choose a filter to narrow the range of historical alarms displayed.

3 Click on the Search button. The list of logged historical alarm records appears.

4 Sort the list of logged historical alarm records, as required.

5 Right-click on a list column heading and choose Save To File from the contextual menu. The Save form opens.

6 Save the list according to your company practices. You can:

- choose a directory to save the listed information using the Save In parameter
- create a filename of any length using the File Name parameter
- choose a format for the output file: HTML or comma-delimited CSV

7 Click on the Save button. The information is saved in the appropriate file format.

You can use the saved lists of logged alarm historical records for post-processing on another PC or workstation, or store for record keeping.

Procedure 34-19 To view the object against which an alarm logged to the alarm history database was raised

You can view the object that was the source of the historical alarm.

1 Choose Tools→Historical Alarms from the 5620 SAM main menu. The Alarm History form opens.

2 If required, choose a filter to narrow the range of historical alarms displayed.

3 Click on the Search button. The historical alarm records appear based on the filtering criteria.

4 Double-click on an alarm in the list. The alarm history record opens.

5 Click on the View Alarmed Object button. The configuration form, properties form, or other appropriate form opens. This is the form for the object that was the source of the original alarm.

Procedure 34-20 To reload all alarms

The 5620 SAM uses an alarm service to cache alarm information. To ensure the cache is current with all alarms stored in the database, administrators can reload all alarms from the database.

Caution — After the procedure is complete, client GUI users viewing open alarm forms and windows may have out-of-date information. Operators should close all open windows and forms, then relaunch them. This includes windows and forms displaying alarm status information, for example, the navigation tree.

1 Log in to a 5620 SAM client GUI with a user account that is assigned the administrator scope of command role or a scope of command role with write access permissions to the fm.FaultManager class. Enter and confirm the password and click on the OK button.

2 Choose Administration→Reload Alarm Information from the 5620 SAM main menu.

3 Clicking on the OK button to confirm that you are aware of all of the other users that will be affected by the alarm reload.

Alarm information is reloaded, and all active client GUIs are updated with the confirmation message that the alarms have been reloaded. Client GUI users can close then reopen windows as required, to refresh the alarm information.

4 Click on the OK button to confirm the message.

5 Close then reopen any open windows or forms, if required.

35 — OAM diagnostic tests

35.1 OAM diagnostic tests overview

The proper delivery of services requires that a number of operations must occur correctly at different levels in the service. For example, operations such as the association of packets to a service, VC labels to a service, and each service to a service tunnel, must be performed successfully for the service to pass traffic to subscribers as agreed to according to SLAs.

Even when tunnels are operating correctly and are correctly bound to services, incorrect information may cause connectivity issues.

To verify that a service is operational and that configuration information is correct, a set of configurable in-band or out-of-band, packet-based OAM tools is available.

For in-band, packet-based testing, the OAM packets closely resemble customer packets to effectively test the forwarding path. However, these packets are distinguishable from customer packets, so they are kept within the service provider network and not forwarded to the customer. For out-of-band testing, OAM packets are sent across a portion of the transport network, for example, across LSPs to test reachability.

You can configure and manage OAM tests:

- from the properties forms of network objects, for example, LSP pings from the LSP properties form
- from the Manage Tests form
- from the service and composite service flat topology maps

You can create and schedule the execution of test suites that contain groups of OAM tests using the 5620 SAM Service Test Manager, or STM. See chapter 75 for information about the STM. See chapter 74 for information about scheduled tasks. See chapter 4 for information about managing tests and test results using service flat topology maps.

Table 35-1 lists the supported OAM test types, the objects against which the tests can be performed, the test types, and the network layer being tested.

Table 35-1 OAM test types and test objects

Network level	Test type	Network object or service component for test
Application (level 7)	DNS lookup	DNS
	DHCP lookup (2)	DHCP

(1 of 3)

Network level	Test type	Network object or service component for test
Ethernet	CFM Loopback	Ports
	CFM Link trace	
	CFM Continuity Check	
	CFM One Way Delay	
	CFM Two Way Delay	
	CFM Eth test	
	CFM Single Ended Loss	
Service (level 6)	VPRN ping	VPRN site
	VPRN trace	
	ICMP ping	
	ICMP trace	
	CPE ping	VPLS site Epipe VLL site
	MFIB ping	
	ANCP loopback	Network element
	VCCV ping	VLL
	VCCV trace	VLL
	MAC populate	VPLS site Epipe VLL site VLL MEF MAC Ping is only supported on 7250 SAS-ES and 7250 SAS-ESA, Release 3.0 VPLS sites.
	MAC ping	
	MAC trace	
	MAC purge	
	MEF MAC ping(1)	
Service transport binding (level 5)	Service site ping	Network element
Service transport (level 4)	MTU ping	Service tunnel (SDP)
	SDP ping	
Transport (level 3)	LSP ping	LSP LSP path
	LSP trace	
	P2MP LSP ping	P2MP LSP P2MP path
	P2MP LSP trace	
	LDP ping (2)	MPLS site LDP site
	LDP trace (2)	
	LDP tree trace	

(2 of 3)

Network level	Test type	Network object or service component for test
Routed network (level 2)	ICMP ping	IP unicast traffic
	ICMP traceroute	
	OmniSwitch ping and traceroute(4)	
	Multicast trace	IP multicast traffic
	Multicast stat (3)	
	Multicast router information	
Layer 1 or Layer 2 (level 1)	MAC ping (3)	Ethernet
	MAC traceroute (3)	
	ATM ping	ATM PVC connection

(3 of 3)

Notes

(1) Supported only on 7250 SAS-ES and 7250 SAS-ESA, Release 3.0.

(2) Cannot be performed using the 5620 SAM or using CLI on devices.

(3) Not yet supported using the 5620 SAM but is supported using CLI on devices.

(4) Implemented using user-defined scripts

Ethernet CFM

Ethernet Connectivity Fault Management, or CFM, supports end-to-end service management in an L2 network. CFM tools provide path discovery, and fault detection, isolation, and notification. See chapter 43 for more information about how to configure an IEEE 802.1ag-enabled network for Ethernet CFM.

The following CFM diagnostic tests detect connectivity failure.

CFM continuity check

CFM continuity check, or CC, messages, are multicast messages that a MEP transmits periodically to remote MEPs in the same MEG. CC tests are used to discover a remote end point, check the health of a site, and detect cross-connect misconfigurations. The loss of three consecutive CCM messages, or the receipt of a CCM with incorrect information, indicates a fault.

Note 1 — If a service is modified after you associate it with an MD, for example, a new site is added, you must manually add new MEPs, as required.

Note 2 — If a CFM continuity check test is running on a service when you add a new MEP to the service, you must stop the test and execute it again to make the new MEP active.

Note 3 — When a service is modified after a CFM continuity check is created, for example, a new B-VPLS site is added to the service, you must manually add a virtual MEP to the site.

CFM dual-ended loss

A CFM dual-ended loss test functions as an optional extension of a CC test. It applies only to Y.1731 MEPs. This type of test is used to calculate the rate of frame loss in each direction for Ethernet packets sent between two MEPs. When a CC test is executed with the dual-ended loss option enabled, the option is replicated on all participating MEPs that support the test, along with the accompanying alarm threshold values. If a MEP detects that the local or remote frame loss ratio has exceeded the alarm threshold for a remote MEP, the MEP raises an alarm against the remote MEP.

CFM single-ended loss

The CFM single-ended loss test applies only to Y.1731 MEPs. This one-way test originates on a source MEP and terminates on a destination MEP. The target of a single-ended loss test is a destination MAC address. The test is used to calculate the rate of frame loss in each direction for Ethernet packets sent between the two MEPs.

CFM loopback

CFM loopback messages are sent to a unicast destination MAC address. The MEP at the destination responds to the loopback message with a loopback reply. A MEP or a MIP can reply to a loopback message if the destination MAC address matches the MAC address of the MEP or MIP. CFM loopback tests verify connectivity to a specific MEP or MIP.

CFM link trace

CFM link trace messages that contain a target unicast MAC address are sent to multicast destination MAC addresses. Each MIP at the same MD level replies with a link trace response. Messages are forwarded to the next hop until they reach the destination MAC address. The originating MEP collects the replies to determine the path.

CFM one-way delay

The CFM one-way delay test applies only to Y.1731 MEPs. The test originates on one MEP and terminates on a target MEP. The results are read from the target MEP. In the test, frame delay is defined as the time elapsed since the start of transmission of the first bit of the frame by a source site until the frame is received by the destination site. The frame delay represents the one-way trip time between the source and destination sites.

CFM two-way delay

The CFM two-way delay test applies only to Y.1731 MEPs. In this test, the frame delay is defined as the time elapsed since the start of transmission of the first bit of the frame by the source site until the frame is received by the same site after passing through the destination site. The frame delay represents the round-trip time between the source and destination sites.

CFM Eth

The CFM Eth test applies only to Y.1731 MEPs. This one-way test originates on a source MEP and terminates on a destination MEP. The target of a CFM Eth test is a MAC address. The test is used to perform one-way in-service diagnostics that include verifying bandwidth throughput, frame loss, and bit errors. To perform the test, a MEP inserts frames with Eth-test information that includes specific throughput, frame size, and transmission patterns. A MIP is transparent to Eth-test frames.

MTU ping OAM

The MTU Ping OAM diagnostic tool, which is called sdp-mtu in the CLI, provides a tool for service providers to determine the exact frame (MTU) size that is supported on a service tunnel (also called an SDP), to within one byte. Use the MTU ping OAM to:

- determine the maximum frame size supported between the service ingress and the service termination point
- solve troubleshooting issues that are related to equipment used across the network core that may not be able to handle large frame sizes

In a large network, network devices can support a variety of packet sizes, up to a limit, that are transmitted across its interfaces. This size limit is referred to as the MTU of network interfaces. You must consider the MTU of the entire service tunnel end-to-end when you provision services, especially for VLL services in which the service must support the ability to transmit the largest customer packet.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. In 5620 SAM 8.0 R1 and later, the messages of the MTU Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

Tunnel ping OAM

The Tunnel Ping OAM tool, which is called sdp-ping in the CLI, performs in-band unidirectional or bidirectional connectivity tests on service tunnels (also called an SDP). The OAM packets are sent in-band in the tunnel encapsulation, so they follow the same path as the service traffic. The response can be received out-of-band in the control plane or in-band using the data plane for a bidirectional test.

For a unidirectional test, tunnel ping OAM tests:

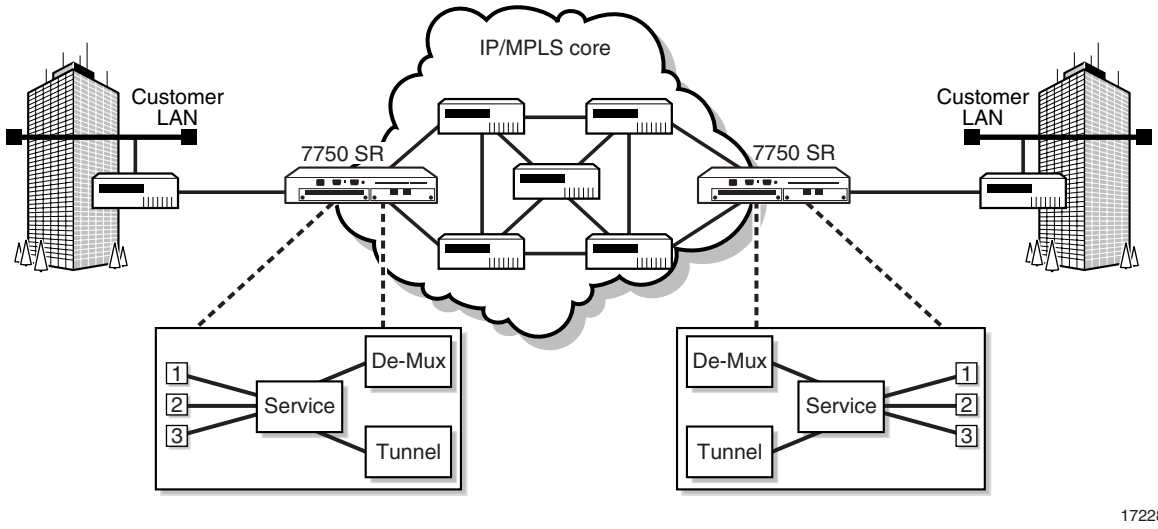
- egress service tunnel ID encapsulation
- whether the packet can reach the far-end IP address destination of the service tunnel ID within its encapsulation
- whether a packet of the specified size goes to the far-end IP address of the service tunnel ID within its encapsulation

- forwarding class mapping to ensure that the test packet is treated the same as the customer traffic
- determine whether SLA delay metrics are met

For a bidirectional test, tunnel OAM uses a local egress service tunnel ID and an expected remote service tunnel ID, so the user can specify where the returned messages should be sent from based on the far-end tunnel ID.

Figure 35-1 shows how a tunnel OAM packet can be inserted to test the connectivity between two customer LANs across the IP/MPLS core.

Figure 35-1 Sample OAM diagnostic



Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. In 5620 SAM 8.0 R1 and later, the messages of the Tunnel Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

Service site ping OAM

The Service Site Ping OAM diagnostic tool, which is called svc-ping in the CLI and was formerly called the circuit ping, provides end-to-end connectivity testing for an individual service. This diagnostic operates at a higher level than the tunnel OAM ping because it verifies connectivity for an individual service rather than connectivity across the service tunnel. This allows you to isolate a problem within the service rather than at the port, which is the endpoint of the service tunnel.

The diagnostic tests a service ID for correct and consistent provisioning between two service endpoints. The following information can be obtained from a service site ping OAM:

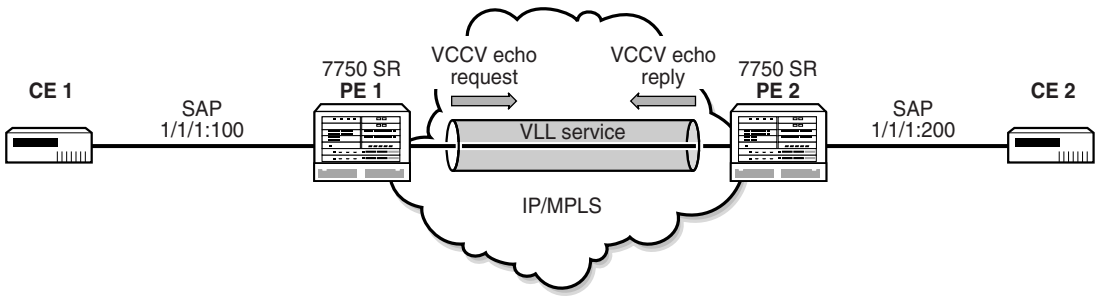
- verification that the local and remote service sites exists
- verification of the current state of the local and remote service sites
- ensuring that the local and remote service types are correlated
- ensuring that the same customer is associated with the local and remote service sites
- ensuring that there is a service-to-circuit association at both the local and remote service sites using the Use Local Tunnel and Use Remote Tunnel options, to check the circuit between service sites
- verification that the local and remote ingress and egress service labels match

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. In 5620 SAM 8.0 R1 and later, the messages of the Service Site Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

VCCV Ping OAM

The VCCV Ping OAM diagnostic tool, which is called vccv-ping in the CLI, performs in-band VLL connectivity tests. It can be used for all types of VLLs and supports cross-circuit tests as long as the circuit types match; for example, an epipe to epipe connector. The purpose of the ping is to determine that the destination PE device is the egress for the L2 FEC. Figure 35-2 shows a VCCV Ping.

Figure 35-2 VCCV Ping OAM diagnostic



In this example, the ping test packet or packets are sent with the destination IP address of PE 2. The request is encapsulated in a VLL packet and is forwarded to PE 2. PE 2 replies to the source device IP address. The packets are sent using the same encapsulation and along the same path as user packets in the VLL. This test provides a check of both the control plane and the data plane.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. In 5620 SAM 8.0 R1 and later, the messages of the VCCV Ping OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

VCCV trace OAM

The VCCV Trace OAM diagnostic tool, which is called vccv-trace in the CLI, displays the hop-by-hop path used by the VLL. VCCV trace can trace the entire path of a PW with a single command issued at the T-PE or at an S-PE. It is an iterative process by which the ingress T-PE or T-PE sends successive VCCV-Ping messages with incrementing the TTL value, starting from TTL=1. The process is terminated when the reply is from the egress T-PE or when a timeout occurs.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. In 5620 SAM 8.0 R1 and later, the messages of the VCCV Trace OAM tool use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

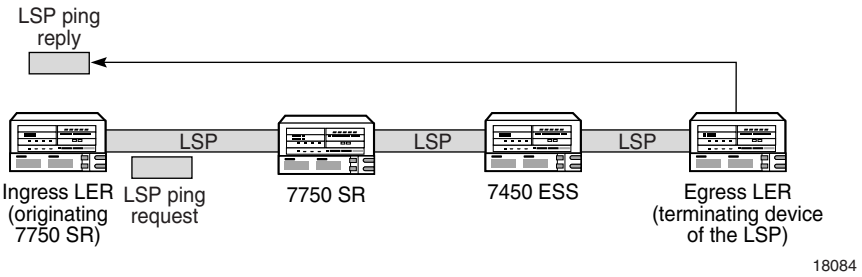
LSP Ping OAM

The LSP Ping OAM diagnostic tool, which is called lsp-ping in CLI, performs in-band LSP connectivity tests. The following information can be determined from the test:

- detect data plane failures in LSPs and with LSP connectivity
- test whether the LSP tunnels are working in both directions

In an LSP ping, the originating router creates an MPLS echo request packet for the LSP and MPLS path to be tested. The MPLS echo request packet is sent and awaits an MPLS echo reply packet from the router that terminates the LSP. The status of the LSP is displayed when the MPLS echo reply packet is received. Figure 35-3 shows an LSP ping.

Figure 35-3 LSP Ping diagnostic



Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. In 5620 SAM 8.0 R1 and later, the messages of the LSP Ping use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

LSP Trace OAM

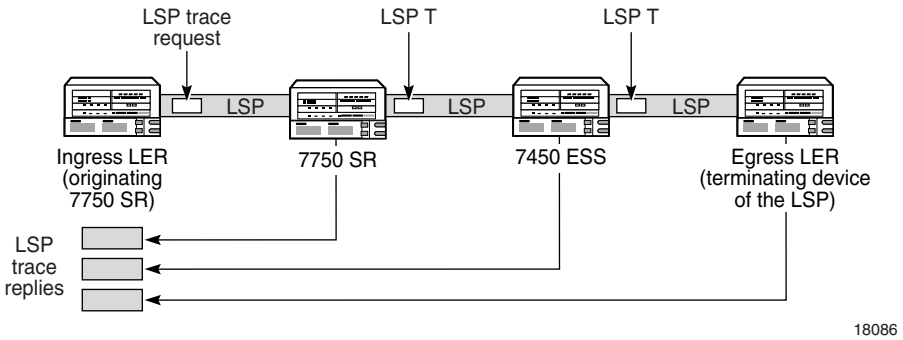
The LSP Trace OAM diagnostic tool, which is called lsp-trace in CLI, displays the hop-by-hop route used by the LSP. The following information can be determined from the test:

- hop-by-hop path for an LSP
- destination path of the packets

In an LSP trace, the originating router creates an MPLS echo request packet for the LSP to be tested. The packet contains increasing TTL values. The MPLS echo request packet is sent and awaits a TTL exceeded response or the MPLS echo reply packet from the router that terminates the LSP. The devices along the hop-by-hop route reply to the MPLS echo request packets with TTL and MPLS echo reply information.

Figure 35-4 shows an LSP trace.

Figure 35-4 LSP Trace diagnostic



Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. In 5620 SAM 8.0 R1 and later, the messages of the LSP Trace use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

P2MP LSP Ping OAM

The PSMP LSP Ping OAM diagnostic tool, which is called p2mp-lsp-ping in CLI, performs in-band LSP connectivity tests.

The echo request message is sent on the active P2MP instance and is replicated in the data path over all branches of the P2MP LSP instance. By default, all egress LER nodes which are leaves of the P2MP LSP instance will reply to the echo request message.

You can reduce the scope of the echo reply messages by explicitly entering a list of addresses for the egress LER nodes that are required to reply. A maximum of 5 addresses can be specified in a single run of the p2mp-lsp-ping command. If all 5 egress LER nodes are 7x50 nodes, they will be able to parse the list of Egress LER addresses and will reply. At 5620 SAM Release 8.0 R1, the p2mp-lsp-ping command specifies that only the top address in the P2MP Egress Identifier TLV must be inspected by an egress LER. When interoperating with other implementations, an 7x50 egress LER will respond if its address is anywhere in the list. Furthermore, if another vendor implementation is the egress LER, only the egress LER matching the top address in the TLV may respond.

If you enter the same Egress LER address more than once in a single p2mp-lsp-ping command, the head-end node displays a response to a single one and displays a single error warning message for the duplicate ones. When queried over SNMP, the head-end node issues a single response trap and issues no trap for the duplicates.

P2MP LSP Trace OAM

The PSMP LSP Ping OAM diagnostic tool, which is called p2mp-lsp-trace in CLI, performs in-band LSP connectivity tests.

The LSP trace capability allows you to trace the path of a single S2L path of a P2MP LSP. Its operation is similar to that of the p2mp-lsp-ping command, but the sender of the echo reply request message includes the Downstream Mapping TLV to request the downstream branch information from a branch LSR or BUD LSR. The branch LSR or BUD LSR will then also include the Downstream Mapping TLV to report the information about the downstream branches of the P2MP LSP. An egress LER must not include this TLV in the echo response message.

The parameter probe-count operates in the same way as in the LSP Trace on a P2P LSP. It represents the maximum number of probes sent per TTL value before giving up on receiving the echo reply message. If a response is received from the traced node before reaching maximum number of probes, then no more probes are sent for the same TTL. The sender of the echo request then increments the TTL and uses the information it received in the Downstream Mapping TLV to start sending probes to the node downstream of the last node which replied. This continues until the egress LER for the traced S2L path replied.

LDP Tree Trace OAM

The LDP Tree Trace OAM diagnostic tool, which is called ldp-treetrace in OAM level of the CLI, is used to detect and discover the ECMP routing paths for a LSP between egress and ingress routers. The following information is determined from the test:

- number of ECMP paths
- number of failed hops

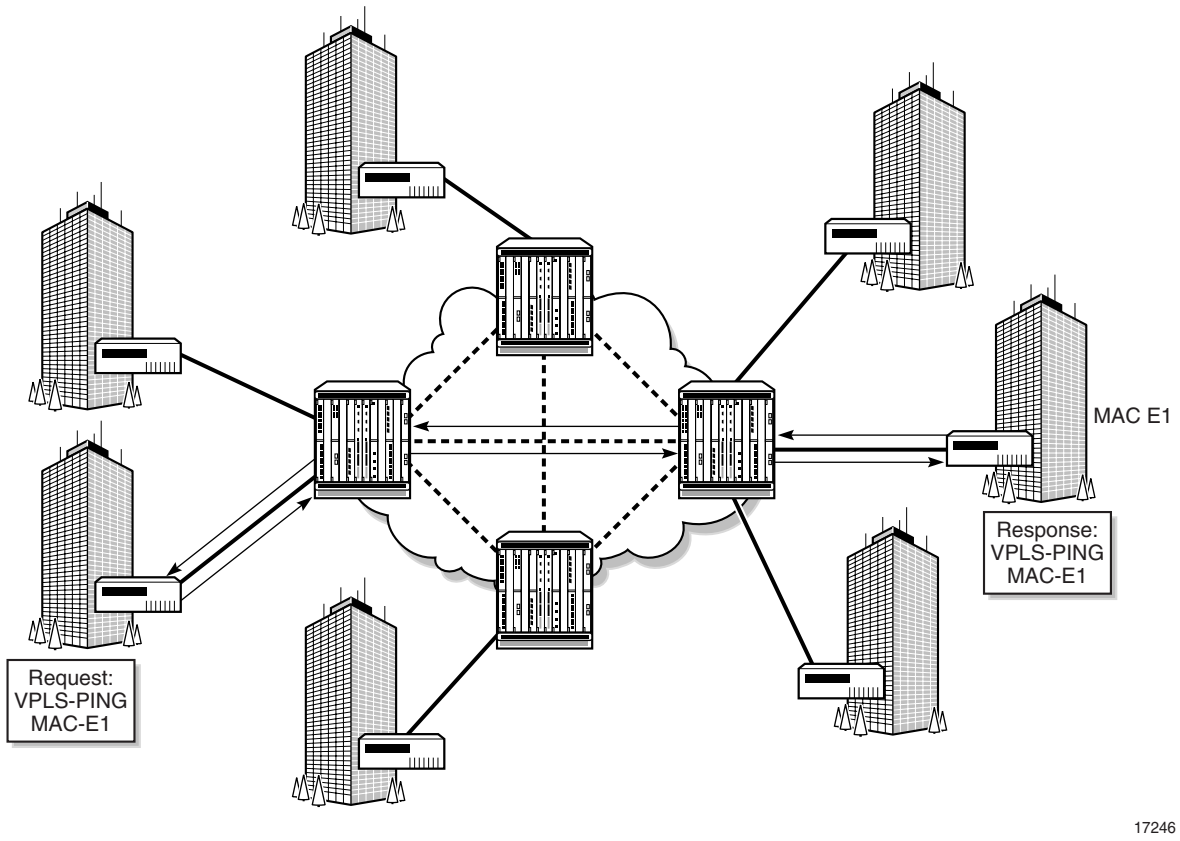
In an LDP tree trace, the originating router creates an MPLS echo request packet. The packet contains a set of IP header destination addresses. Routers along the path reply to the request with information about themselves and neighboring routers in the downstream path. The originating router uses this information to probe the downstream routers until it discovers a bit map setting common to all routers along the path. The result is a tree of available routers that the originating router can use for next hops. After discovery, the paths are tested using LSP ping and LSP trace.

Note — The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. In 5620 SAM 8.0 R1 and later, the messages of the LDP Tree Trace use the T-LDP local LSR ID as the source IP address. Previously the NE's system interface address was used for this purpose.

MAC ping OAM

The MAC ping OAM tool, which is called mac-ping in CLI, is used to test connectivity in a VLL or VPLS by verifying a remote MAC address at the far end of a service. Figure 35-5 shows a sample MAC ping from one end of a service to the far-end MAC address of the service.

Figure 35-5 Sample MAC ping diagnostic



The MAC ping determines the existence of the far-end egress point of the service. MAC pings can be sent in-band or out-of-band. You must specify either:

- the target (far-end) MAC address
- the broadcast address

In a MAC ping that is out-of-band, the ping is forwarded along the flooding domain when no MAC address bindings exist or is sent along the bindings if MAC address bindings exist. A response ping is sent from the far-end device when there is an egress binding for the service.

In a MAC ping that is in-band, the ping is sent with a VC label TTL of 255. The ping packet goes across each hop, and when it reaches the egress router, it is identified by the OAM label and the response is sent back along the management plane.

MEF MAC ping

Use the MEF MAC ping OAM tool to test connectivity in a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0, VPLS site. The MEF MAC ping verifies a remote MAC address at the far end of the service.

MEF MAC ping must run simultaneously in both directions between the VPLS sites being tested.

MAC trace OAM

The MAC trace OAM tool, which is called mac-trace in CLI, displays the hop-by-hop route of MAC addresses used to reach the target MAC address at the far end of a service. MAC traces can be sent in-band or out-of-band.

You must specify either:

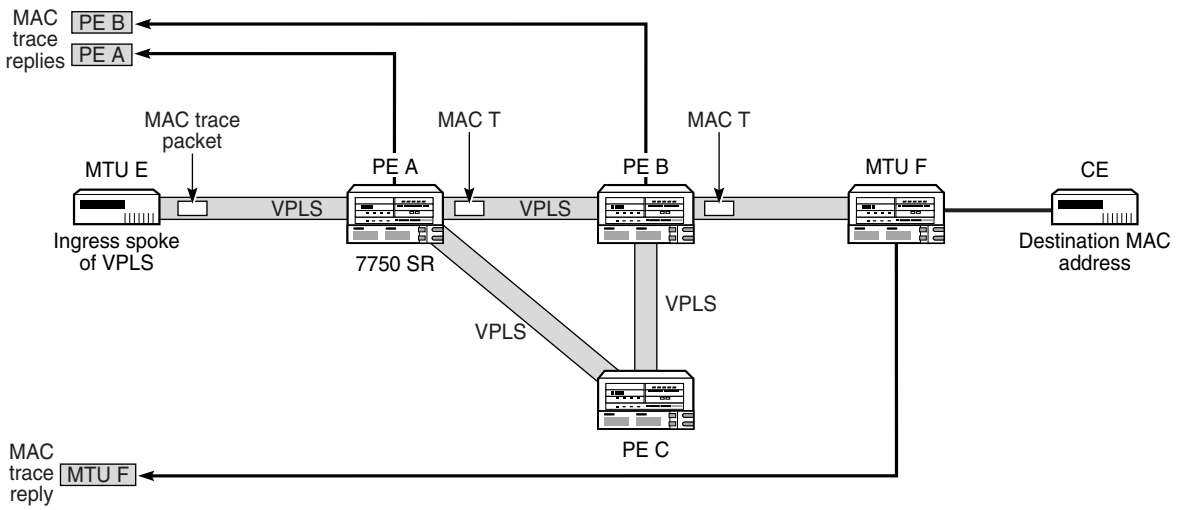
- the target (far-end) MAC address
- the broadcast address

In a MAC trace that is out-of-band, the destination IP address is specified by mapping the destination MAC address. If the destination MAC address is known to be a specific site, the far-end IP address of the service tunnel is used. If the destination MAC address is not known, the packet is sent to all service tunnels in the service.

In a MAC trace that is in-band, the trace request contains tunnel encapsulation, VC label, OAM, and other information. If the destination MAC address is known, the appropriate tunnel encapsulation and VC label is used. If the destination MAC address is not known, the packet is sent to all service tunnels, including all necessary tunnel encapsulation and egress VC labels for each bound service tunnel.

Figure 35-6 shows a MAC trace.

Figure 35-6 MAC trace diagnostic



MAC populate OAM

The MAC populate OAM tool, which is called mac-populate in CLI, is used to:

- Know whether the FIB table is accurate by testing forwarding plan correctness. This is done by populating a service FIB with an OAM-tagged MAC entry. This MAC entry indicates that the node is the egress node for the MAC address of a service. You can then use the FIB manager to see the OAM-tagged MAC entry.
- Send a message through the flooding domain to learn a MAC address, as if a customer packet with that source MAC address had flooded the domain from that ingress point of the service.

You can:

- force an existing MAC address to become OAM-tagged
- distinguish, in the FIB manager, MAC addresses that are OAM-tagged
- age an OAM-tagged MAC address

In a MAC populate, the OAM-tagged MAC address is populated on the egress point of the service. You can specify whether to flood this OAM-tagged MAC address to other devices so that the same OAM-tagged entry is added to the FIB tables of other devices.

MAC purge OAM

The MAC purge OAM tool, which is called mac-purge in CLI, is used to delete an OAM-tagged entry from a FIB, which was generated using the MAC populate OAM tool. This clears the FIB of any learned information for a specific MAC address, allows the FIB to be populated only by a MAC populate request, and can be used to flush all devices in a service domain.

CPE ping

The CPE ping tool, which is called cpe-ping in the CLI, is used to trace the end-to-end switching of specified MAC addresses of customer premises equipment. This ping extends the functionality of the MAC ping beyond the egress (customer-facing) port by allowing a ping to the SAP of a VPLS.

ANCP loopback

The ANCP loopback test, which is called oam ancp in the CLI, is used to send DSL OAM commands to complete an OAM test from a centralized point or when operational boundaries prevent direct access to the DSLAM. The ANCP loopback test raises an alarm that generates a log event displaying both successful and failed results.

VPRN ping and VPRN trace

The VPRN ping and VPRN trace OAM tools are enabled from the VRF site of the subscriber's VPRN service. The VPRN ping determines the existence of the far-end egress point of the service. This allows testing of whether a specific destination can be reached. VPRN pings can be sent in-band or out-of-band.

The VPRN trace displays the hop-by-hop path for a destination IP address within a VPRN service. This allows operators to know the destination path of customer traffic. VPRN traces can be sent in-band or out-of-band.

ATM OAM ping

The ATM OAM ping tool, which is called atmoam-ping in CLI, performs an ATM ping on an existing ATM PVC from the PVC endpoint using ATM OAM loopback cells. An ATM ping tests VC integrity and endpoint connectivity for PVCs using OAM loopback capabilities.

Multicast FIB ping

The multicast FIB ping OAM tool, which is called mfib-ping in CLI, identifies the SAPs that egress an IP multicast stream within a VPLS. This diagnostic can also be used to display the SAPs that are operationally up in the VPLS.

Multicast router information

The multicast router information OAM tool, which is called mrinfo in CLI, identifies VPRN multicast information for the target router. The information includes details that are related to adjacent routers, supported protocols, traffic metrics, and time-to-live thresholds. Administrators can use this information to identify bidirectional adjacency relationships.

Multicast trace

The multicast trace OAM tool, which is called mtrace in CLI, identifies the hop-by-hop route used by VPRN multicast traffic to reach the target router. This diagnostic gathers the hop address, routing error conditions, and packet statistics at each hop. The 5620 SAM attempts to trace the receiver-to-sender route for the traffic. The destination of the diagnostic can be any PIM-enabled interface in the routing instance.

ICMP ping

The ICMP ping OAM tool, which is called icmp-ping in CLI, identifies the reachability of a remote host across the IP network. The tool is used with ICMP trace to detect and localize faults in IP networks.

The ICMP ping OAM tool can also be enabled from the VRF site of the subscriber's VPRN service. An ICMP ping determines the existence of the far-end egress point of the service. This allows testing of whether a specific destination can be reached. ICMP pings can be sent in-band or out-of-band.

ICMP trace

The ICMP trace OAM tool, which is called icmp-trace in CLI, identifies the diagnostic used to trace the ICMP traceroute control table. The tool is used with ICMP ping to detect and localize faults in IP networks.

ICMP trace displays the hop-by-hop path for a destination IP address within a VPRN service. This allows operators to know the destination path of subscriber traffic. ICMP traces can be sent in-band or out-of-band.

OmniSwitch ping and traceroute

The 5620 SAM supports OmniSwitch ping and traceroute by using user-defined CLI scripts. Sample OmniSwitch ping and traceroute scripts are provided in section 35.4. See Procedure 35-34 for information about creating an OmniSwitch OAM script. See Procedures 35-35 and 35-36 for information about configuring and running OmniSwitch OAM scripts.

DNS ping

The DNS ping OAM tool, which is called dns-ping in CLI, identifies the diagnostic used to ping the DNS name, if DNS name resolution is configured.

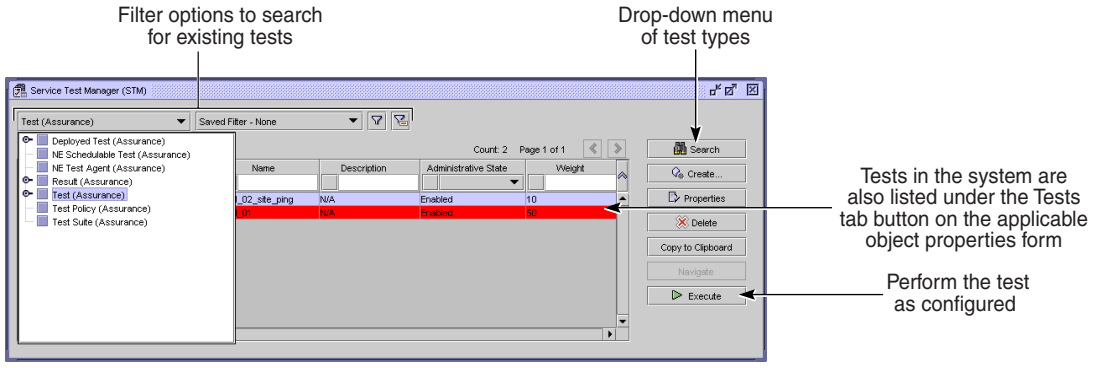
Service assurance test management and configuration

There are two main types of forms for the service assurance test manager.

- Browse and list manager, to generate lists of OAM diagnostics and to run OAM diagnostics
- Configuration form, to create or modify service assurance tests and review the results of service assurance tests

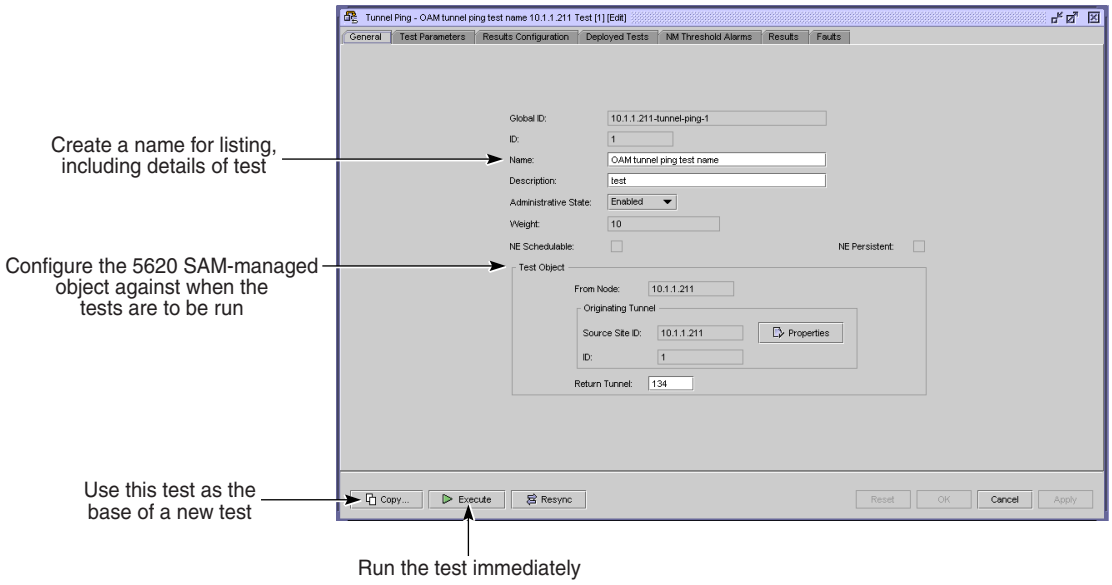
Figure 35-7 shows the browse and list manager form.

Figure 35-7 Service assurance test manager browse and list form



Each service assurance test configuration form contains multiple tabs. Figure 35-8 shows a sample service assurance OAM test with the General tab displayed.

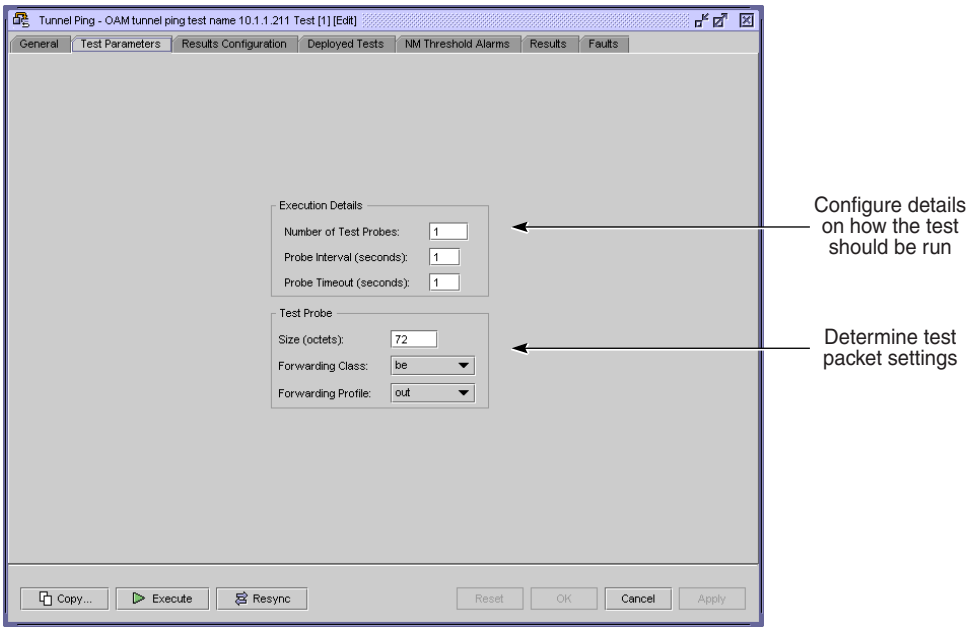
Figure 35-8 Service assurance OAM test configuration form - General



18037

Figure 35-9 shows the same sample service assurance OAM test with the Test Parameters tab displayed.

Figure 35-9 Service assurance OAM test configuration form - Test Parameters tab



18034

Figure 35-10 shows the same sample service assurance OAM test with the Results Configuration tab displayed.

Figure 35-10 Service assurance OAM test configuration form - Results Configuration

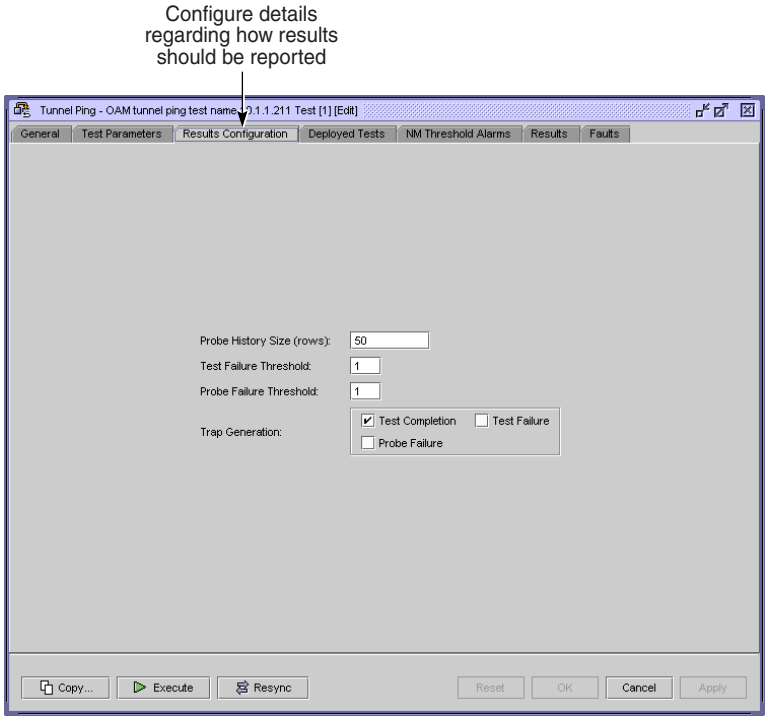


Figure 35-11 shows the same sample service assurance OAM test with the Results tab displayed. Selecting the Results tab button opens an additional form, which provides detailed test results, including OAM test packet details, when the OAM test involves sending test packets.

Figure 35-11 Service assurance OAM test configuration form - Results

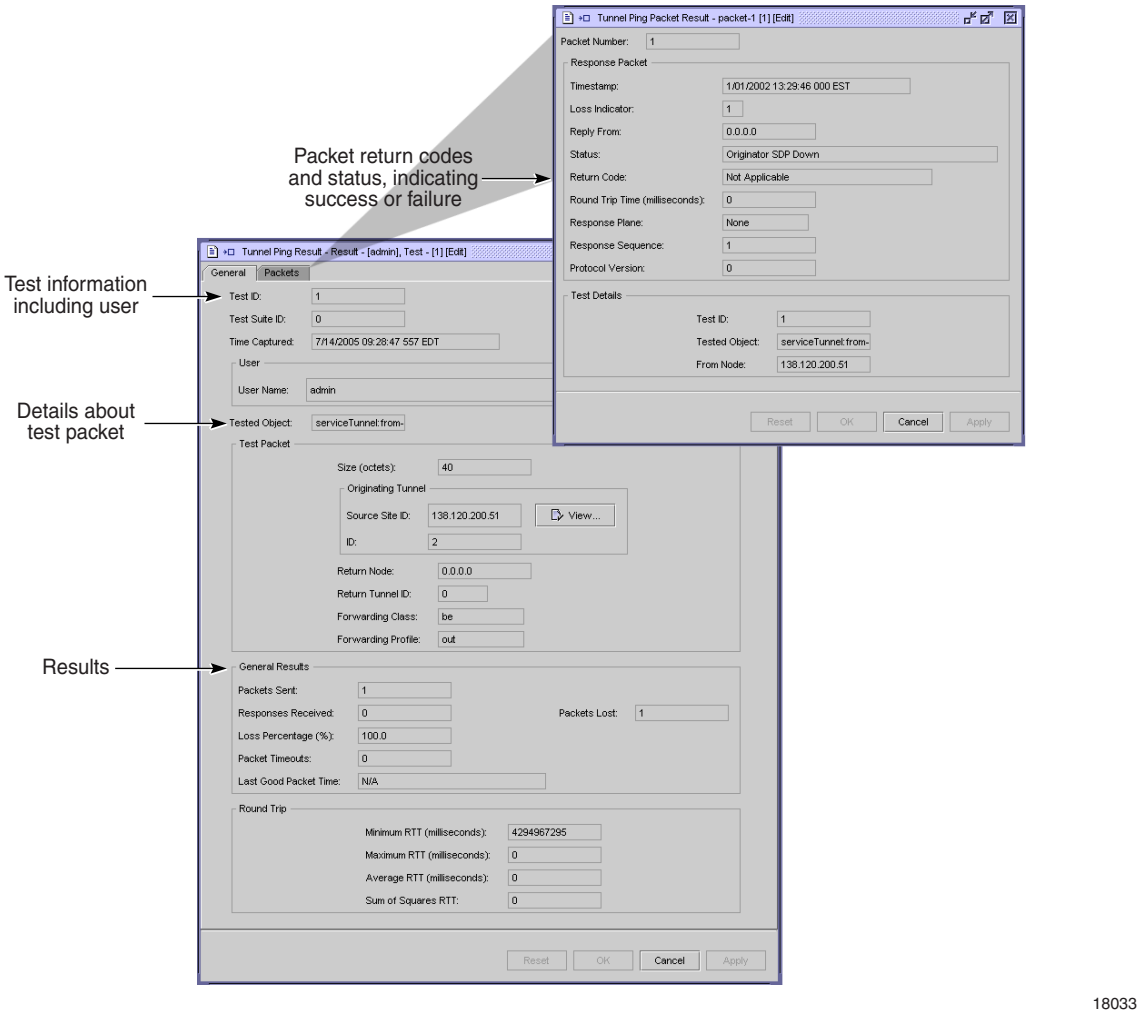
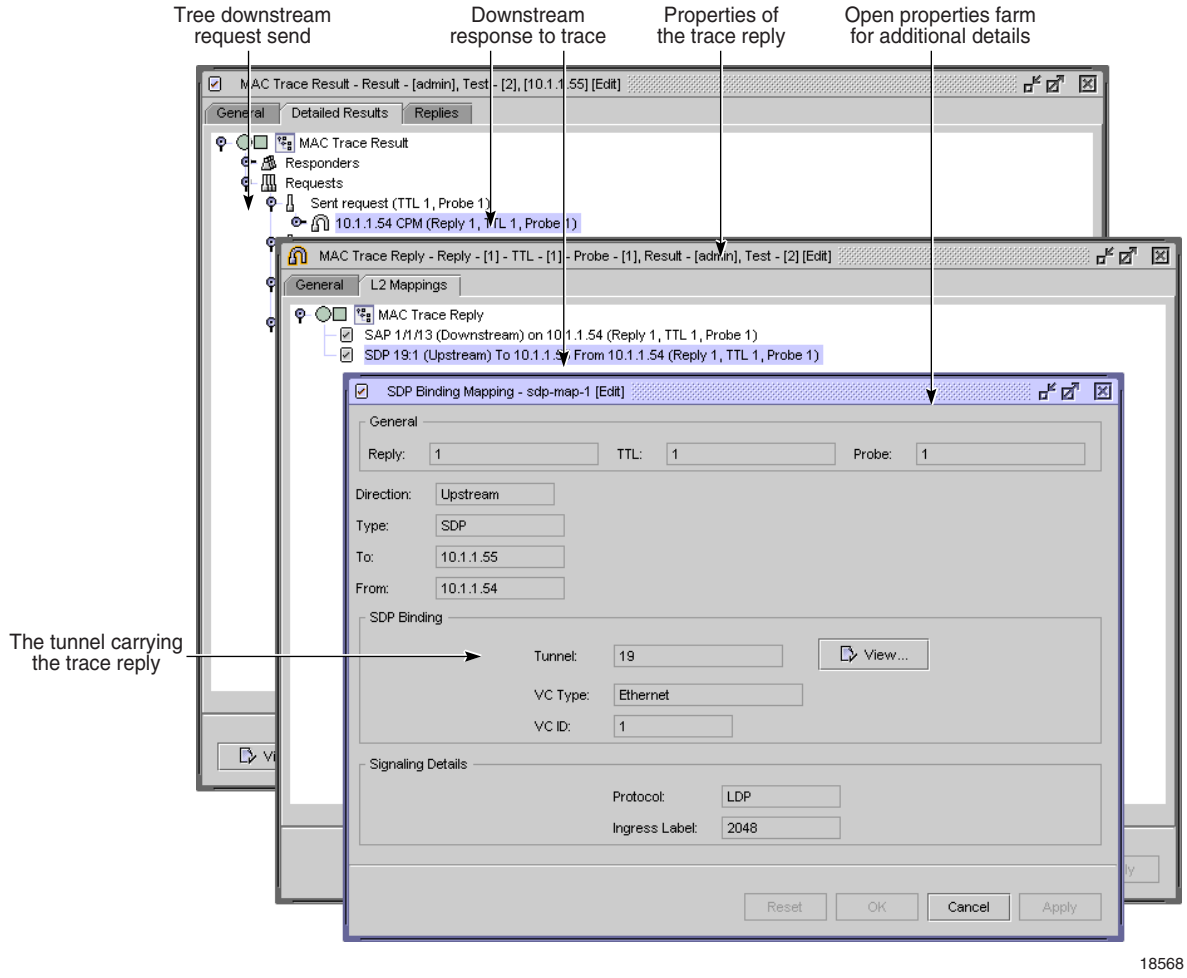


Figure 35-12 shows the information from a sample MAC trace. Trace probe information is available from the Detailed Results tab. Continue to navigate down from the trace requests to view result information.

Figure 35-12 Service assurance OAM test probe and trace results details



35.2 Sample OAM diagnostic test configuration

Figure 35-13 shows a sample OAM diagnostic sequence, illustrating how you can use multiple OAM tests to verify service creation and diagnose service problems. This sample shows a VPLS.

Figure 35-13 Sample OAM diagnostic sequence for a VPLS

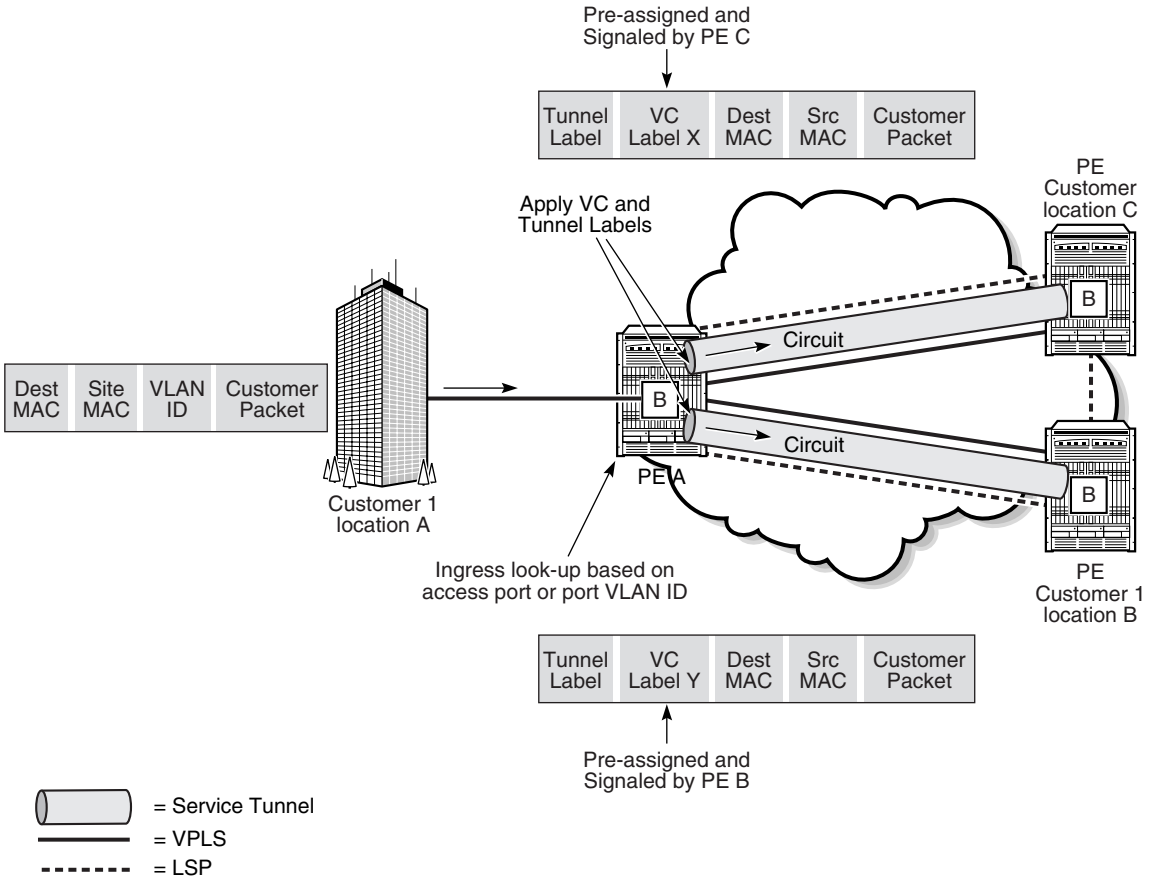


Table 35-2 lists the high-level tasks necessary to configure this sample.

Table 35-2 Sample OAM diagnostic configuration for a service

Task	Description
Service creation and OAM validation	
1. MPLS and LSP creation	Create an MPLS network and LSPs for use by the service tunnels connecting the VPLS sites. Test the validity of the LSPs using LDP tree trace or LSP ping. If the results indicate a problem with the path, use LSP trace to check the specific MPLS path for the device causing the ping failure.
2. Service tunnel creation	Create a service tunnel that uses the MPLS LSP created earlier and perform a tunnel ping on the service tunnel to verify tunnel connectivity. Create all tunnels necessary to interconnect the VPLS sites, and repeat the tunnel ping to ensure tunnel connectivity. After all of the tunnels are created, use the tunnel ping remote tunnel option and specify the return tunnel path. Verify bidirectional tunnel connectivity.

(1 of 2)

Task	Description
3. Service creation	Create a service using the service tunnels to interconnect the VPLS sites, either using mesh or spoke service tunnel bindings. Use a service site ping between each VPLS site device and its neighboring sites to verify service configuration consistency.
4. MAC diagnostics	Connect the CPE devices to the VPLS and verify traffic. Use MAC trace from the edge devices to verify MAC address learning by the VPLS sites and to ensure that the correct associations are made between MAC addresses and the service tunnels or SAPs to which they are bound. Use MAC ping against an unknown MAC address to verify that no response is returned. Use MAC populate to create an OAM-specific MAC address. Use MAC ping and MAC trace against the created MAC address to verify that customer traffic is not affected by the additional MAC address. Use MAC purge to remove the created OAM MAC address.
Service OAM diagnostics	
1. Diagnose traffic flow problems at a specific MAC address	Use MAC ping against the MAC address to which traffic is not flowing. Use the source and destination MAC address to simulate customer traffic routes as closely as possible. Use MAC trace to pinpoint the location of the traffic failure. Check for MAC filter rules or MAC table sizes to identify possible causes of the failure, for example, incorrect configurations.
2. Diagnose the components of the service	Use service site ping to test the potential next hops to ensure consistent configuration. Use tunnel ping to the far end of the tunnel using the remote tunnel option and specify the return tunnel path. Verify bidirectional tunnel connectivity. Use LSP ping to determine if the tunnel is working. Use an LSP trace to determine if an intervening device is down.

(2 of 2)

35.3 Workflow to use OAM diagnostic tests

1. Create the transport network and customer services.
2. Monitor customer services or troubleshoot the transport network before you commission, according to your company's policies.
3. When the creation of a tunnel needs to be tested, or a customer service is compromised, use the service assurance tools to troubleshoot the problem.

Note — Not all service assurance tools are applicable to every NE managed by the 5620 SAM.

   i. Use MTU ping to troubleshoot and resolve tunnel and service problems that are related to frame size across all equipment that is used by the service or tunnel.

   ii. Use tunnel ping to troubleshoot and resolve tunnel and service problems that are related to issues that circuits may have transmitting traffic across the GRE or MPLS network.

   iii. Use service site ping to troubleshoot and resolve service problems that are related to the end-to-end connectivity of a customer service within the provider network.

iv Use VCCV ping and VCCV trace to troubleshoot and resolve issues that are related to VLL services.

v Use LDP tree trace to detect and discover available routers for ECMP routing.

vi Use LSP ping and LSP trace to troubleshoot and resolve problems that are related to MPLS LSPs, LDPs, and MPLS paths.

vii Use MAC ping, MEF MAC Ping, MAC trace, MAC populate, MAC purge, and CPE ping to troubleshoot and resolve problems that are related to FIBs and MAC addressing. The tests are used in combination; for example, MAC populate to inject a MAC address into the network, MAC ping to determine where the address was learned, MAC trace to determine the path, CPE ping to test the VPLS, and MAC purge to remove the injected MAC address.

viii Use ANCP loopback to send OAM messages to the access node.

ix Use VPRN ping, VPRN trace, ICMP ping and ICMP trace to troubleshoot and resolve problems with a VPRN service.

x Use ATM ping to test ATM PVC connections.

xi Use multicast FIB ping to troubleshoot and resolve problems with the multicast component of a VPLS.

xii Use multicast router information and multicast trace to troubleshoot and resolve problems with the multicast component of a VPRN service.

xiii Use ICMP ping, ICMP trace, and DNS ping to troubleshoot and resolve problems with IP reachability.

4 Use the OAM tool diagnostic response messages and results form information to resolve the customer service problem.

35.4 Sample OmniSwitch ping and traceroute CLI scripts

The following ping and traceroute scripts are sample CLI scripts that can be used to run ping and traceroute tests. See the *5620 SAM Scripts and Templates Developer Guide* for information about creating, configuring, and using scripts.

Sample OmniSwitch ping script

The following is sample code for an OmniSwitch OAM ping script.

Code 35-1: Sample OmniSwitch OAM ping script

```
<velocityProperties>
  <tab><name>General</name><tooltip>The general tab</tooltip>
    <group><name>General</name><tooltip>The general group</tooltip>
      <property>
        <name>ip_address</name>
        <uiName>IP Address:</uiName>
        <tooltip>IP address of the system to ping (IPv4
xxx.xxx.xxx.xxx)</tooltip>
        <type>String</type>
        <default>0.0.0.0</default>
```

```
        <uiOrder>1</uiOrder>
        <required>true</required>
      </property>
      <property>
        <name>count</name>
        <uiName>Count:</uiName>
        <tooltip>Number of frames to be transmitted</tooltip>
        <type>Integer</type>
        <default>6</default>
        <uiOrder>2</uiOrder>
        <required>true</required>
      </property>
      <property>
        <name>packed_size</name>
        <uiName>Packet Size:</uiName>
        <tooltip>Size of the data portion of the packet sent for this
ping, in bytes</tooltip>
        <type>Integer</type>
        <default>64</default>
        <required>true</required>
        <uiOrder>3</uiOrder>
        <min>1</min>
        <max>60000</max>
      </property>
      <property>
        <name>interval</name>
        <uiName>Interval (seconds):</uiName>
        <tooltip>Polling interval</tooltip>
        <type>Integer</type>
        <uiOrder>4</uiOrder>
        <default>1</default>
        <min>1</min>
        <max>10000</max>
      </property>
      <property>
        <name>timeout</name>
        <uiName>Timeout (seconds):</uiName>
        <tooltip>Number of seconds the program will wait for a
response before timing out</tooltip>
        <type>Integer</type>
        <uiOrder>5</uiOrder>
        <default>5</default>
        <min>1</min>
        <max>10000</max>
      </property>
    </group>
  </tab>
</velocityProperties>

ping $ip_address count $count size $packed_size interval $interval
timeout $timeout
```

Sample OmniSwitch traceroute script

The following text is sample code for an OmniSwitch OAM traceroute script.

Code 35-2: Sample OmniSwitch traceroute script

```
<velocityProperties>
  <tab><name>General</name><tooltip>The general tab</tooltip>
    <group><name>General</name><tooltip>The general group</tooltip>
      <property>
        <name>ip_address</name>
        <uiName>IP Address:</uiName>
        <tooltip>IP address of the host whose route you want to trace.
(IPv4 xxx.xxx.xxx.xxx)</tooltip>
        <type>String</type>
        <default>0.0.0.0</default>
        <uiOrder>1</uiOrder>
        <required>true</required>
      </property>
      <property>
        <name>maxHopValue</name>
        <uiName>Maximum Hop:</uiName>
        <tooltip>Maximum hop count for the trace</tooltip>
        <type>Integer</type>
        <default>5</default>
        <uiOrder>2</uiOrder>
        <required>true</required>
      </property>
    </group>
  </tab>
</velocityProperties>

traceroute $ip_address max-hop $maxHopValue
```

35.5 OAM diagnostic tests procedures

Use the following procedures to create and execute OAM diagnostic tests.

Procedure 35-1 To create and run an MTU ping OAM diagnostic from a service tunnel

Use the MTU ping diagnostic to find the largest valid frame size.

1. Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.
2. Filter to list only the source and destination routers of the service tunnel and click on the Search button. The list of service tunnels appears.
3. Double-click on a service tunnel from the list. The Tunnel (Edit) form opens.
4. Click on the Tests tab button.
5. Click on the MTU Ping tab button.
6. Click on the Create button. The MTU Ping (Create) form opens with the General tab displayed. The form displays information about the service tunnel being tested and the originating tunnel ID.

7 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent

8 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- MTU Start Size (octets)
- MTU End Size (octets)
- MTU Step Size (octets)

Note — If the step size is small but the end message size is large, the amount of time to complete the MTU ping may be many minutes. Ensure that you have an appropriate step size that reflects the range of MTU packet sizes you want to test.

9 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

10 Click on the Apply button to save the changes.

11 Perform the MTU ping.

i Click on the Execute button in the MTU Ping (Edit) form. The MTU ping diagnostic starts. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results. The diagnostic is complete.

ii Click on the Results tab button. The list of MTU ping OAM probes sent is displayed.

iii Click on the row(s) as appropriate to view diagnostic information.

iv Click on the Properties button. The OAM results form opens. The diagnostic information includes:

- source and destination of the diagnostic
- timestamp of when the test was completed
- time to complete the diagnostic, in milliseconds
- frame size sent
- OAM diagnostic status
- diagnostic code returned

See Procedure 35-44 for more information about the diagnostic status messages. Use the status message to interpret the diagnostic results. For example, the status message Response Received indicates that the MTU OAM diagnostic completed successfully.

- **v** Close the form.

12 Close the Tunnel (Edit) form when the OAM diagnostics are complete.

Procedure 35-2 To create and run a tunnel ping OAM diagnostic from a service tunnel

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

2 Filter to list only the source and destination routers of the service tunnel and click on the Search button. The list of service tunnels opens.

3 Double-click on a service tunnel from the list. The Tunnel (Edit) form opens.

4 Click on the Tests tab button.

5 Click on the Tunnel Ping tab button.

6 Click on the Create button. The Tunnel Ping (Create) form opens with the General tab displayed. The form displays information about the circuit being tested, including the originating tunnel ID.

7 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Return Tunnel

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

8 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Forwarding Class
- Forwarding Profile

The Probe Interval (seconds) parameter has an effect only when multiple probes are to be sent.

Ensure that you configure the Forwarding Class parameter to work with the services that use the tunnel.

9 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

10 Click on the Apply button to save the changes.

11 Confirm the action. The created tunnel ping test appears in the list of tests on the Tunnel Ping tab of the Tunnel (Edit) form.

12 Perform the tunnel ping OAM diagnostic:

i Click on the Execute button in the Tunnel Ping (Edit) form. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results. The diagnostic is complete.

ii Click on the Results tab button. The list of tunnel ping OAM packets sent is displayed.

iii Click on the row(s) as appropriate to view diagnostic information.

iv Click on the Properties button. The OAM results form opens. The diagnostic information includes:

- source and destination of the diagnostic
- timestamp of when the test was completed
- time to complete the diagnostic, in milliseconds
- OAM diagnostic status
- diagnostic code returned

See Procedure 35-44 for more information about the diagnostic status messages. Use the status message to interpret the diagnostic results.

v Close the form.

13 Close the Tunnel (Edit) form when the OAM diagnostics are complete.

Procedure 35-3 To create an MTU ping OAM diagnostic from the test manager

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service Transport→Create MTU Ping from the Create contextual menu. The MTU Ping (Create) form opens.

4 Configure the parameters described in Procedure 35-1. You must additionally configure the source of the service tunnel.

   i Click on the Select button beside the Source Site ID parameter. The Select Originating Tunnel form opens.

   ii Click on the Search button.

   iii Select a tunnel from the list.

   iv Click on the OK button. The MTU Ping (Create) form reappears with the IP address and ID of the selected service tunnel.

5 Click on the Apply button to save the changes.

6 Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

7 Click on the Execute button to start the ping. A deployed test is created and run.

8 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 35-4 To create and execute a CFM CC OAM diagnostic

Perform this procedure to manually create and execute a CFM CC test.

Note — The 5620 SAM automatically creates a CFM CC test when you create an MD and global MEG. You can execute an automatically created test using the STM, or from the Tests tab of a MEG.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button and choose Ethernet CFM→CFM Continuity Check from the menu. The CFM Continuity Check Test (Create) form opens.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Duration

4 If you are configuring the test for a 7705 SAR, configure the parameters in the Initial Dual Ended Loss Test Options panel:

- Enable Test
- Alarm Threshold (%)
- Alarm Clearing Threshold (%)

5 Click on the Select button. The Select Maintenance Entity Group form opens.

6 Specify a search filter, if required, and click on the Search button. A list of MEGs is displayed.

7 Select a MEG in the list and click on the OK button. The Select Maintenance Entity Group form closes, and the MEG is displayed on the CFM Continuity Check Test (Create) form.

8 Click on the Apply button. The form displays additional buttons and tabs.

9 To execute the test, click on the Execute button on the CFM Continuity Check (Edit) form.

10 Click on the Results tab button to view the test results. See Procedure 35-43 for information about test results.

11 Close the CFM Continuity Check Test (Create) form.

Procedure 35-5 To create and execute a CFM loopback diagnostic

Perform this procedure to manually create and execute a CFM loopback test. You can create multiple CFM loopback tests for an originating MEP.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Loopback from the contextual menu. The CFM Loopback Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Loopback form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Loopback form closes, and the CFM Loopback (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Loopback form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Loopback form closes, and the CFM Loopback (Create) form displays the MEP information.

11 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to select the destination MEP. The Select MEP - CFM Loopback form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Loopback form closes, and the CFM Loopback (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to select the destination MIP. The Select MIP - CFM Loopback form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Loopback form closes, and the CFM Loopback (Create) form refreshes.

Note — MIP selection is not supported for OmniSwitch NEs.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM Loopback form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Loopback form closes, and the CFM Loopback (Create) form refreshes.

12 Configure the MEP Transmit LBM Information parameters:

- Data Size
- VLAN Priority
- Number of Loopback Sent

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab button to view the test results. See Procedure 35-43 for information about test results.

Procedure 35-6 To create and execute a CFM link trace diagnostic

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Link Trace from the Create contextual menu. The CFM Link Trace (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Link Trace form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Link Trace form closes, and the CFM Link Trace (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Link Trace form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Link Trace form closes, and the CFM Link Trace (Create) form displays the MEP information.

11 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM Link Trace form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Link Trace form closes, and the CFM Link Trace (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Link Trace form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Link Trace form closes, and the CFM Link Trace (Create) form refreshes.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM Link Trace form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Link Trace form closes, and the CFM Link Trace (Create) form refreshes.

12 Configure the TTL parameter.

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab button to view the test results. See Procedure 35-43 for information about test results.

Procedure 35-7 To create and execute a CFM Eth test diagnostic

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Eth Test from the Create contextual menu. The CFM Eth Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Eth Test form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Eth Test form closes, and the CFM Eth Test (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Eth Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Eth Test form closes, and the CFM Eth Test (Create) form displays the MEP information.

11 Perform one of the following.

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to select the destination MEP. The Select MEP - CFM Eth Test form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Eth Test form closes, and the CFM Eth Test (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Eth Test form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Eth Test form closes, and the CFM Eth Test (Create) form refreshes.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM Eth Test form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Eth Test form closes, and the CFM Eth Test (Create) form refreshes.

12 Configure the MEP Transmit LBM Information parameters:

- Data Size (octets)
- VLAN Priority

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab button to view the test results. See Procedure 35-43 for information about test results.

Procedure 35-8 To create and execute a CFM one-way delay diagnostic

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM One Way Delay Test from the Create contextual menu. The CFM One Way Delay Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM One Way Delay form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM One Way Delay form closes, and the CFM One Way Delay (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM One Way Delay Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM One Way Delay Test form closes, and the CFM One Way Delay Test (Create) form displays the MEP information.

11 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM One Way Delay form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM One Way Delay form closes, and the CFM One Way Delay Test (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM One Way Delay form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM One Way Delay form closes, and the CFM One Way Delay Test (Create) form refreshes.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - CFM One Way Delay form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM One Way Delay form closes, and the CFM One Way Delay (Create) form refreshes.

12 Configure the Priority parameter in the MEP Transmit LBM Information panel.

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab button to view the test results. See Procedure 35-43 for information about test results.

Procedure 35-9 To create and execute a CFM two-way delay diagnostic

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Two Way Delay Test from the Create contextual menu. The CFM Two Way Delay Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Two Way Delay form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Two Way Delay form closes, and the CFM Two Way Delay (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Two Way Delay Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Two Way Delay Test form closes, and the CFM Two Way Delay Test (Create) form displays the MEP information.

11 Perform one of the following:

a Select a MEP as the test destination. Perform the following steps.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM Two Way Delay form opens.

ii Select an entry and click on the OK button. The Select MEP - CFM Two Way Delay form closes, and the CFM Two Way Delay Test (Create) form refreshes.

b Select a MIP as the test destination. Perform the following steps.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Two Way Delay form opens.

ii Select an entry and click on the OK button. The Select MIP - CFM Two Way Delay form closes, and the CFM Two Way Delay Test (Create) form refreshes.

Note — MIP selection is not supported on OmniSwitch NEs.

c Select an unmanaged MEP as the test destination. Perform the following steps.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to select the destination MEP. The Select Unmanaged MEP - Two Way Delay form opens.

ii Select an entry and click on the OK button. The Select Unmanaged MEP - CFM Two Way Delay form closes, and the CFM Two Way Delay (Create) form refreshes.

12 Configure the Priority parameter.

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab button to view the test results. See Procedure 35-43 for information about test results.

Procedure 35-10 To create and execute a CFM single-ended loss diagnostic

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Ethernet CFM→CFM Single Ended Loss Test from the Create contextual menu. The CFM Single Ended Loss Test (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State

5 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Single Ended Loss Test form opens.

6 Specify a search filter, if required, and click on the Search button. A list of global MEGs is displayed.

7 Select an entry and click on the OK button. The Select Global MEG - CFM Single Ended Loss Test form closes, and the CFM Single Ended Loss Test (Create) form displays the global MEG.

8 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Single Ended Loss Test form opens.

9 Specify a search filter, if required, and click on the Search button. A list of MEPs is displayed.

10 Select a MEP in the list and click on the OK button. The Select Originating MEP - CFM Single Ended Loss Test form closes, and the CFM Single Ended Loss Test (Create) form displays the MEP information.

11 Choose a destination MEP:

i Click on the Select MEP button beside the Target MAC Address parameter. The Select MEP - CFM Single Ended Loss Test form opens.

ii Double-click on an entry in the list, or choose an entry and click on the OK button. The Select MEP - CFM Single Ended Loss Test form closes, and the CFM Single Ended Loss Test (Create) form refreshes.

12 Configure the following parameters in the MEP Transmit LMM Information panel:

- Priority
- Count
- Interval

13 Click on the Apply button. The form displays additional buttons and tabs.

14 To execute the test, click on the Execute button.

15 Click on the Results tab button to view the test results. See Procedure 35-43 for information about test results.

Procedure 35-11 To create a tunnel ping OAM diagnostic from the test manager

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service Transport→Create SDP Ping from the Create contextual menu. The Tunnel Ping (Create) form opens.

4 Configure the parameters described in Procedure 35-2. You must additionally configure the source of the service tunnel.

i Click on the Select button beside the Source Site ID parameter. The Select Originating Tunnel form opens.

ii Configure the filter criteria.

iii Click on the Search button.

iv Select a tunnel from the list.

v Click on the OK button. The Tunnel Ping (Create) form reappears with the IP address and ID of the selected service tunnel.

5 Click on the Apply button to save the changes.

6 Click on the Execute button to start the tunnel ping. A deployed test is created and run.

7 Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

8 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 35-12 To configure and run VPRN OAM diagnostics from a service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Service Manager form opens.

2 Filter to list only the services on which you want to perform OAM diagnostics and click on the Search button.

3 Choose a service from the list and click on the Properties button. The Service (Edit) form opens.

4 Click on the Sites tab button.

5 Choose a site or sites from the list and click on the Properties button. The Site (Edit) form opens.

6 Click on the Tests tab button.

7 Configure and run a VPRN ping or VPRN trace OAM diagnostic.

a To configure and run a VPRN ping:

i Click on the VPRN Ping tab. A list of VPRN diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The VPRN ping form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

iv Click on the Select button to select a VPRN site. The Select VPRN Site - VPRN Ping form appears.

v Click on the Search button.

vi Select a VPRN site and click on the OK button. The Select VPRN Site - VPRN Ping form closes.

vii Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Source IP Address
- Target IP Address
- Time To Live
- Reply via Control Plane
- Forwarding Profile
- Forwarding Class

viii Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

ix Click on the Apply button to save the changes.

x Confirm the action.

xi Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

b To configure and run a VPRN trace:

i Click on the VPRN Trace tab. A list of VPRN trace diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The VPRN Trace (Create) form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

iv Click on the Select button to select a VPRN site. The Select VPRN Site - VPRN Trace form appears.

v Click on the Search button.

vi Select a VPRN site and click on the OK button. The Select VPRN Site - VPRN Trace form closes.

vii Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Source IP Address
- Target IP Address
- Initial Time to Live
- Maximum Time to Live
- DiffServ Field
- Reply via Control Plane
- Forwarding Profile
- Forwarding Class

viii Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

ix Click on the Apply button to save the changes.

x Confirm the action.

xi Choose the diagnostic from the list.

xii Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

8 Configure and run an ICMP ping or ICMP trace OAM diagnostic.

a To configure and run ICMP ping:

i Click on the ICMP Ping tab. A list of ICMP diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The ICMP Ping form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- From IP Address
- Target IP Address
- Next Hop Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

iv Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Rapid
- Time To Live
- Data Pattern
- Positional Data Pattern
- DiffServ Field
- Egress Interface Index
- Bypass Routing
- Do Not Fragment

v Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

vi Click on the Apply button to save the changes.

vii Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

b To configure and run ICMP trace:

i Click on the ICMP Trace tab. A list of ICMP trace diagnostics appears.

ii Double-click on a row in the list to edit an existing test, or click on the Create button to create a new test. The ICMP Trace form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- From IP Address
- Target IP Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

iv Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Maximum Time To Live
- DiffServ Field
- Time To Wait (milliseconds)

v Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

vi Click on the Apply button to save the changes.

vii Choose the diagnostic from the list.

viii Click on the Execute button. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Note — Results of individually run ICMP Trace tests are viewed on the Results tab. The Results tab displays only the result of the last individually run ICMP Trace test, any previous individually run test results are overwritten.

Results from ICMP Trace tests that are scheduled or part of a test suite are also stored on the Results tab. The number of scheduled test results stored corresponds to the value configured in the Probe History Size (rows) parameter. Scheduled ICMP Trace test results do not overwrite individually run test results or previously run scheduled test results.

Procedure 35-13 To configure and run MAC populate OAM diagnostics

You can also perform the diagnostic from the Tests tab of a VPLS or Epipe VLL service form.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create MAC Populate from the Create contextual menu. The MAC Populate (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Target Type
- Target MAC Address
- Send via Control Plane
- Flood
- Force OAM
- Age (seconds)
- Service Name
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

6 Click on the OK button to save the changes.

7 Choose the created test from the list of OAM diagnostics.

8 Click on the Execute button to start the MAC populate diagnostic. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 35-14 To configure and run MAC purge OAM diagnostics

You can also perform the diagnostic from the Test tab of a VPLS or an Epipe VLL.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create MAC Purge from the Create contextual menu. The MAC Purge (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Target Type
- Target MAC Address
- Send via Control Plane
- Inhibit Learning
- Flood
- Service Name
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

6 Click on the OK button to save the changes.

7 Choose the created test from the list of OAM diagnostics.

8 Click on the Properties button.

9 Click on the Execute button to start the MAC purge diagnostic. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 35-15 To configure and run MAC ping OAM diagnostics

You can also perform the diagnostic from the Test tab of a VPLS or an Epipe VLL.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→ MAC Ping from the Create contextual menu. The MAC Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- Target MAC Address
- Source MAC Address
- Service Name
- Name

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile
- Reply Control
- Control Plane

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Properties button.

10 Click on the Execute button to start the MAC ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 35-16 To configure and run MEF MAC ping OAM diagnostics

You can also perform the diagnostic from the Test tab of a VPLS.

Note — MEF MAC Ping must run simultaneously in both directions between the source and destination VPLS sites. Configure a test from the source VPLS site to the destination VPLS site and from the destination VPLS site to the source VPLS site.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create MEF MAC Ping from the Create contextual menu. The MEF MAC Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent
- Target Type
- Target MAC Address

5 Choose a VPLS service.

i Click on the Select button in the Service panel. The Select Service - MEF MAC Ping form opens.

ii Configure the filter criteria and click on the Search button. A list of VPLSs appears.

iii Choose a VPLS and click on the OK button. The Select Service - MEF MAC Ping form closes.

6 When you choose a VPLS, the Site panel appears on the form. Choose a VPLS site that belongs to the selected VPLS.

i Click on the Site panel Select button. The Select Site - MEF MAC Ping form opens.

ii Configure the filter criteria and click on the Search button. A list of VPLS sites appears.

iii Choose a VPLS site and click on the OK button. The Select Site - MEF MAC Ping form closes.

7 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)

8 Click on the Results Configuration tab button and configure the parameters:

- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

9 Click on the OK button to save the changes.

10 Choose the created test from the list of OAM diagnostics.

11 Click on the Execute button to start the MEF MAC ping. A deployed test is created and run. Click on the Deployed Tests tab button to open the deployed test and view the current state of the test. When the test is complete, the deployed test is removed and you can view the results.

12 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- round trip jitter
- round trip latency
- round trip frame loss

Procedure 35-17 To configure and run MAC trace OAM diagnostics

You can also perform the diagnostic from the Test tab of a VPLS or an Epipe VLL.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create MAC Trace from the Create contextual menu. The MAC Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- Target MAC Address
- Source MAC Address
- Initial Time to Live
- Maximum Time to Live
- Service Name
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Forwarding Profile
- Forwarding Class

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the Apply button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Execute button to start the MAC trace. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 35-18 To configure and run CPE ping OAM diagnostics

You can also perform this diagnostic from the Test tab of a VPLS.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create CPE Ping from the Create contextual menu. The CPE Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Service Name
- Name
- Destination IP Address
- Source IP Address
- Source MAC Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- VC's Label Time Live
- Send via Control Plane
- Reply via Control Plane
- Forwarding Profile
- Forwarding Class

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes.

8 Click on the Search button to display the list of OAM diagnostics.

9 Double-click on the created test from the list of OAM diagnostics.

10 Click on the Execute button to start the CPE ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab.

12 To display the test results, select the test from the CPE Ping Result list and click on the Properties button. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 35-19 To configure and run ANCP loopback diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L2 Service→Create ANCP Loopback from the Create contextual menu. The ANCP Loopback (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent

5 Click on the Select button beside the System ID (Loopback IP Address) parameter. The Select Originating Node - ANCP Loopback form opens.

6 Configure the filter criteria.

7 Click on the Search button.

8 Double-click on an entry in the list, or select an entry and click on the OK button. The Select Originating Node - ANCP Loopback form closes, and the ANCP Loopback (Create) form refreshes.

9 Click on the Test Parameters tab button and perform one of the following steps.

a Configure the ANCP loopback diagnostic for a subscriber ID.

i Set the Target Type parameter to Subscriber Ident String.

ii Configure the Subscriber Ident String parameter.

b Configure the ANCP loopback diagnostic for an ANCP string.

i Set the Target Type parameter to ANCP String.

ii Configure the ANCP String parameter.

10 Configure the parameters:

- Count
- Timeout (seconds)

11 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

12 Click on the Apply button to save changes.

13 Click on the Execute button to start the ANCP loopback diagnostic. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete you can view the results.

14 Click on the Results tab to view the test results.

15 Select the test from the ANCP Loopback Result list and click on the Properties button. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 35-20 To configure and run service site ping OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service→ Service Site Ping from the Create contextual menu. The Service Site Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- System ID (Loopback Ip Address)

5 Click on the Test Parameters tab button and configure the parameters:

- Target IP Address
- Service ID
- Use Local Tunnel
- Use Remote Tunnel

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available. When you set the Use Local Tunnel and Use Remote Tunnel parameters, the test becomes a ping that tests the service tunnel bindings between the service sites.

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes.

8 Choose the created test from the list of OAM diagnostics and click on the Properties button.

9 Click on the Execute button to start the service site ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 35-21 To configure and run VCCV ping OAM diagnostics

You can also perform a VCCV ping from a VLL service form.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service→Create VCCV Ping from the Create contextual menu. The VCCV Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

5 Click on the Select button in the First Spoke SDP Binding panel. The Select First Spoke SDP Binding - VCCV ping form appears.

6 Click on the Search button.

7 Select the first spoke SDP binding and click on the OK button. The Select First Spoke SDP Binding - VCCV ping form closes.

8 Click on the Select button in the Downstream SDP Binding panel. The Select downstream spoke SDP Binding - VCCV ping form appears.

9 Click on the Search button.

10 Select the downstream spoke SDP binding and click on the OK button. The Select downstream spoke SDP Binding - VCCV ping form closes.

11 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type

12 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

13 Click on the OK button to save the changes.

14 Choose the created test from the list of OAM diagnostics.

15 Click on the Execute button to start the VCCV ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

16 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- IP address of the destination and far-end device
- Time Last Response
- Number of Responses Received
- Response Time
- Loss indicator, a value of 0 indicates that the test packet was received and a value of 1 indicates that the test packet was lost

Procedure 35-22 To configure and run VCCV Trace OAM diagnostics

You can also perform a VCCV Trace test from a VLL service form.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Service→Create VCCV Trace from the Create contextual menu. The VCCV Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

5 Click on the Select button in the First Spoke SDP Binding panel. The Select First Spoke SDP Binding - VCCV Trace form appears.

6 Click on the Search button.

7 Select the first spoke SDP binding and click on the OK button. The Select First Spoke SDP Binding - VCCV Trace form closes. The parameters in the First Spoke SDP Binding block are populated.

8 Configure the parameters:

- Initial Time to Live
- Maximum Time to Live

9 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type

10 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

11 Click on the OK button to save the changes. The VCCV Trace (Create) form closes.

12 Click on the Test (Assurance) item in the Service Test Manager form and then click the Search button.

13 Choose the created test from the list of tests in the Test (Assurance) block.

14 Click on the Execute button to start the VCCV Trace test. A deployed test is created and run.

15 Click on the Properties button. The VCCV Trace (Edit) form opens with the General tab displayed.

16 Click on the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

17 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- information about the configuration test, including the configured parameter values
- number of probes to be issued
- time of last response
- source and response IP addresses
- number of hops
- probe responses from nodes in path

Procedure 35-23 To configure and run LSP Ping OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create LSP Ping from the Create contextual menu. The LSP Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- Site ID
- IP Address
- LDP Prefix
- LDP Prefix Length
- Destination Path Address
- Next Hop Interface Name
- Next Hop Interface Address
- Return LSP

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

The parameters in the Source IP Address, LDP, and Details panels can only be configured when the Target Type parameter is set to Any LSP and when the LDP Site ID is configured.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes. The Service Test Manager form opens.

8 Double-click on the created test from the list of OAM diagnostics.

9 Click on the Execute button to start the LSP ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 35-24 To configure and run LSP Trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create LSP Trace from the Create contextual menu. The LSP Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- Site ID
- IP Address
- LDP Prefix
- LDP Prefix Length
- Destination Path Address
- Probe Failure Threshold
- Next Hop Interface Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

The parameters in the Source IP Address, LDP, and Details panels can only be configured when the Target Type parameter is set to Any LSP and when the LDP Site ID is configured.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Initial Time to Live
- Maximum Time To Live
- Forwarding Class
- Forwarding Profile

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the OK button to save the changes. The Service Test Manager form opens.

8 Choose the created test from the list of OAM diagnostics and click on the Properties button.

9 Click on the Execute button to start the LSP trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

Procedure 35-25 To configure and run P2MP LSP Ping OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create P2MP LSP Ping from the Create contextual menu. The P2MP LSP Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State

5 Click the Select button in the P2MP Dynamic Lsp panel to choose the P2MP Dynamic LSP you want to test.

6 Click the Select button in the P2MP Instance panel to choose the P2MP Instance you want to test.

7 Configure the Select All S2L Paths parameter.

If you enabled the parameter, go to step 10.

8 Click on the S2L Paths tab.

9 Select the S2L paths that you want to test. A maximum of five can be selected.

10 Click on the Test Parameters tab and configure the parameters:

- Probe Timeout (seconds)
- Probe Interval (seconds)
- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

11 Click on the Results Configuration tab and configure the parameters:

- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

12 Click on the NM Thresholds tab to configure threshold-crossing alarms, as required.

Refer to Procedure 35-39 for details.

13 Click on the OK button to save the changes. The Service Test Manager form opens.

14 Choose the created test from the list of OAM diagnostics and click on the Properties button.

The P2MP LSP Ping (Edit) form opens, with the General tab displayed.

15 Click on the Execute button to start the P2MP LSP ping. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

Note — When this test is performed on an existing Point-to-Multipoint LSP, up to five S2L paths can be selected. If none are selected, all available paths up to the limit of five will be pinged.

16 Click on the Results tab in the P2MP LSP Ping (Edit) form.

If you enabled the Select All S2L Paths parameter in step 7, the Results tab will show an entry for each path tested.

17 Select the test from the list and click on Properties. The P2MP LSP Ping Result form opens, with the General tab displayed.

The General tab displays the test parameters you configured, along with time the test was executed, its status, and the following test information:

- Number of Probes Sent
- Probe Timeouts
- Number of Responses Received
- Probes Lost

Note — The test results depend on the type of test you run. Refer to Procedure 35-43 for more information.

18 Click on the Details tab.

19 View the test results for the:

- Round Trip Time
- Outbound One Way Time
- Inbound One Way Time

20 Click on the Response Probes tab.

21 Select a response probe from the list and click on Properties. The P2MP LSP Ping Probe Result form opens.

Note — The test results depend on the type of test you run. Refer to Procedure 35-43 for more information.

22 View details on the response probe, including:

- Status
- Round-Trip Time
- Response sequence

23 Repeat steps 17 to 22 for all tested S2L paths.

Note — Refer to the Service assurance test management and configuration in Section 35.1 and to Chapter 75 for more information on viewing test results.

Procedure 35-26 To configure and run P2MP LSP Trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose MPLS→Create P2MP LSP Trace from the Create contextual menu. The P2MP LSP Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent

5 Click the Select button in the P2MP Dynamic Lsp panel to choose the P2MP Dynamic LSP you want to test.

6 Click the Select button in the P2MP Instance panel to choose the P2MP Instance you want to test.

7 Click the Select button in the S2L Destination Address panel to choose the S2L Destination Address you want to test.

8 Click on the Test Parameters tab and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Initial Time to Live
- Maximum Time To Live
- Forwarding Class
- Forwarding Profile

9 Click on the Results Configuration tab and configure the parameters:

- Maximum Failures
- Trap Generation

10 Click on the NM Thresholds tab to configure threshold-crossing alarms, as required.

Refer to Procedure 35-39 for details.

11 Click on the OK button to save the changes. The Service Test Manager form opens.

12 Choose the created test from the list of OAM diagnostics and click on the Properties button.

The P2MP LSP Trace (Edit) form opens, with the General tab displayed.

13 Click on the Execute button to start the P2MP LSP trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

14 Click on the Results tab.

15 Select the test from the list and click on Properties. The P2MP LSP Trace Result form opens, with the General tab displayed.

The General tab displays the test parameters you configured, along with time the test was executed and its status.

Note — The test results depend on the type of test you run. Refer to Procedure 35-43 for more information.

16 Click on the Hops and Probes tab.

A tree view of the Hops and Probes associated with this test is provided.

17 Right-click on a Hop from the tree view and click on Properties.

The P2MP LSP Trace Hop (Edit) form is displayed, showing the General tab.

18 View the test results for the:

- Response Probe
- Round Trip Details
- Outbound One Way Trip Details
- Inbound One Way Trip Details

19 Right-click on a Probe from the tree view and click on Properties.

The P2MP LSP Trace Probe (Edit) form is displayed, showing the General tab.

20 View details on the probe, including:

- Response Probe
- LSP Details

21 Repeat this test for all required S2L paths. The test only evaluates one S2L path per execution.

Note — Refer to the Service assurance test management and configuration in Section 35.1 and to Chapter 75 for more information on viewing test results.

Procedure 35-27 To configure and run LDP Tree Trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button. The test options are displayed in a drop-down menu.

3 Choose MPLS→Create LDP Tree Trace from the Create contextual menu. The LDP Tree Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Site ID
- LDP Prefix
- LDP Prefix Length

5 Click on the Test Parameters tab button and configure the parameters:

- Maximum Time To Live
- Timeout (seconds)
- Retry Counter
- Forwarding Class
- Profile
- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the OK button to save the changes. The Service Test Manager form opens.

8 Choose the created test from the list of OAM diagnostics and click on the Properties button.

9 Click on the Execute button to start the LDP tree trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 Click on the Results tab. A list of LDP tree trace tests appears.

11 Choose a LDP tree trace from the list and click on the Properties button.

12 View the test results. The results depend on the type of test. See Procedure 35-43.

Procedure 35-28 To configure and run multicast router information OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Multicast→Create Mrinfo from the Create contextual menu. The mrinfo (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent
- Target Type
- Site ID

5 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

6 Click on the Select button to choose a PIM interface. The Select PIM Interface form opens.

7 Select a PIM interface in the list and click on the OK button. The Select PIM Interface form closes, and the interface information is displayed on the mrinfo (Create) form.

8 Click on the OK button to save the changes.

9 Choose the created test from the list of OAM diagnostics.

10 Click on the Execute button to start the diagnostic request for multicast router information. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43.

Procedure 35-29 To configure and run multicast trace OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Multicast→Create Mtrace from the Create contextual menu. The mtrace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent
- Target Type
- Site ID
- Source Address
- Destination Address
- Response Address

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Initial Time to Live
- Maximum Number of Hops

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the OK button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Execute button to start the multicast trace. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43.

Procedure 35-30 To configure and run multicast FIB ping OAM diagnostics

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Multicast→Create Mfib Ping from the Create contextual menu. The MFIB Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent
- Service Name
- Multicast Source
- Multicast Group
- Name

When the Service Name parameter is configured, you can configure the Name parameter for the site.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Time To Live
- Timeout (seconds)
- Reply via Control Plane

When you set the target IP address, then choose a service ID, only service IDs from the selected site are available.

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the OK button to save the changes.

8 Choose the created test from the list of OAM diagnostics.

9 Click on the Execute button to start the multicast FIB ping. A deployed test is created and run. Open the deployed test to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

10 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43.

Procedure 35-31 To configure and run an ATM OAM ping

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose L1/L2→Create ATM Ping from the Create contextual menu. The ATM Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent
- ATM Interface ID

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Loopback Location (hex)
- Destination Type

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the Apply button to save the settings. A confirmation window opens.

8 Click on the Yes button.

9 Choose the created test from the list of OAM diagnostics.

10 Click on the Execute button to start the ATM ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

11 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

12 To configure another ATM OAM ping, click on the Clear button and repeat steps 5 to 11. Otherwise, go to step 13.

13 Click on the Cancel button to close the form.

Procedure 35-32 To configure and run an ICMP ping

You can also perform an ICMP ping from the Test tab of a VPRN or EIS service configuration form.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose ICMP→ ICMP Ping from the Create contextual menu. The ICMP Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- System ID (Loopback IP Address)
- From IP Address
- Source IP Address
- Target IP Address
- Next Hop Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

Note — The NE Persistent test is not supported on OmniSwitch NEs.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Rapid
- Time To Live
- Data Pattern
- Positional Data Pattern
- DiffServ Field
- Egress Interface Index
- Bypass Routing
- Do Not Fragment
- Forwarding Class
- Forwarding Profile

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the Apply button to save the settings.

8 Click on the Execute button to start the ICMP ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Average Round-Trip Time
- Maximum Round-Trip Time
- Minimum Round-Trip Time
- Round-Trip Jitter

10 To configure another ICMP ping, click on the Clear button and repeat steps 5 to 9. Otherwise, go to step 11.

11 Click on the Cancel button to close the form.

Procedure 35-33 To configure and run an ICMP trace

You can also perform an ICMP trace from the Test tab of a VPRN or EIS.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose ICMP→Create ICMP Trace from the Create contextual menu. The ICMP Trace (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- System ID (Loopback IP Address)
- From IP Address
- Source IP Address
- Target IP Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Maximum Time To Live
- DiffServ Field
- Time to Wait (milliseconds)

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Maximum Failures
- Trap Generation

7 Click on the Apply button to save the settings.

8 Click on the Execute button to start the ICMP trace. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Current Hop Count
- Current Probe Count
- Minimum Round-Trip Time
- Round-Trip Jitter

Note — Results of individually run ICMP Trace tests are viewed on the Results tab. The Results tab displays only the result of the last individually run ICMP Trace test, any previous individually run test results are overwritten.

Results from ICMP Trace tests that are scheduled or part of a test suite are also stored on the Results tab. The number of scheduled test results stored corresponds to the value configured in the Probe History Size (rows) parameter. Scheduled ICMP Trace test results do not overwrite individually run test results or previously run scheduled test results.

10 To configure another ICMP trace, click on the Clear button and repeat steps 5 to 9. Otherwise, go to step 11.

11 Click on the Cancel button to close the form.

Procedure 35-34 To create an OmniSwitch OAM CLI script

Warning — Scripts that are not correctly created or applied can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define user responsibilities for CLI script usage, and ensure that scripts are verified and validated before they are executed on devices in a live network.

Perform this procedure to create an OmniSwitch OAM CLI script using the sample scripts provided in section 35.4.

1 Choose Tools→Scripts from the 5620 SAM main menu. The Script Manager form opens.

2 Choose CLI Script (script) from the object drop-down list and click on the Create button. The CLI Script (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Script ID
- Name
- Description
- Type
- Use Latest Version
- State
- Continue On Command Failure
- Content Type

Enable the Use Latest Version parameter to associate all of the targets of the script with the latest version of the CLI script.

You must set the Content Type parameter to Velocity.

4 Perform the following steps to specify the script target types.

i Click on the Add button in the NE Types panel. The Select Property - CLI Script form opens.

ii Select one or more OmniSwitch NE types in the list and click on the OK button. The Select Property - CLI Script form closes, and the NE types are listed on the CLI Script (Create) form.

5 Click on the Apply button to apply the configuration.

6 Click on the Versions tab button.

7 Create the script by clicking on the Add button. The Script Editor *script_name* form opens.

8 Create the CLI script text by performing one of the following steps.

a Import an existing text file with a CLI script. You can create a text file by copying and pasting the text from the sample OmniSwitch ping or traceroute script into a text editor. The sample scripts are in section 35.4.

i Choose File→Import from the Editor menu. The Import dialog box appears.

ii Choose the file to be imported and click on the Import button. The script appears in the script manager editor workspace.

iii Modify the script as required.

b Enter or copy and paste the CLI script text from the sample OmniSwitch ping script or traceroute script into the script manager editor workspace. The sample OAM scripts are found in section 35.4.

9 Perform one of the following.

a Save the script to the script manager.

i Choose File→Save from the Editor menu or click on the Save button. The Comment form opens.

ii Configure the parameters:

- NE Version Information
- Comment

iii Click on the OK button.

b Export the script to a local or network text file.

i Choose File→Export from the Editor menu, or click on the Export button. A dialog box appears and prompts you to choose a file storage location in the network.

ii Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field.

iii Click on the Export button. The script version text file is saved in the specified location.

10 Choose File→Close from the Editor menu. The Script Editor form closes, and the CLI Script (Edit) form reappears with the Version tab displayed. The new version of the script appears in the list.

11 Close the CLI Script (Edit) form.

12 Close the Script Manager list form.

See procedures 35-35 and 35-36 for information about configuring and running OmniSwitch ping and traceroute OAM scripts.

Procedure 35-35 To configure and run an OmniSwitch OAM ping

Warning — Scripts that are not correctly created or applied can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define user responsibilities for CLI script usage, and ensure that scripts are verified and validated before they are executed on devices in a live network.

The following procedure describes how to configure and run an OmniSwitch ping test using the script created using Procedure 35-34.

1 Ensure that the mediation policy for each OmniSwitch target is configured with the correct user name and password for CLI communication. See Procedure 13-4.

2 Choose Tools→Scripts from the 5620 SAM main menu. The Script Manager form opens.

3 Choose CLI Script (script) from the object drop-down list.

4 Configure the filter criteria. A list of scripts appears at the bottom of the Script Manager form.

5 Double-click on the OmniSwitch ping script that you created using Procedure 35-34. The CLI Script (Edit) form opens with the General tab displayed.

6 Click on the Targets tab button.

7 Click on the Add button. The Target Configuration form opens.

8 Click on the Add button. The Select Network Elements form opens.

9 Choose one or more OmniSwitch devices and click on the OK button. The Select Network Elements form closes, and the OmniSwitch nodes are listed on the Target Configuration form.

10 Configure the test parameters.

i Choose a target from the Target List panel.

ii Configure the parameters, as shown in Figure 35-14.

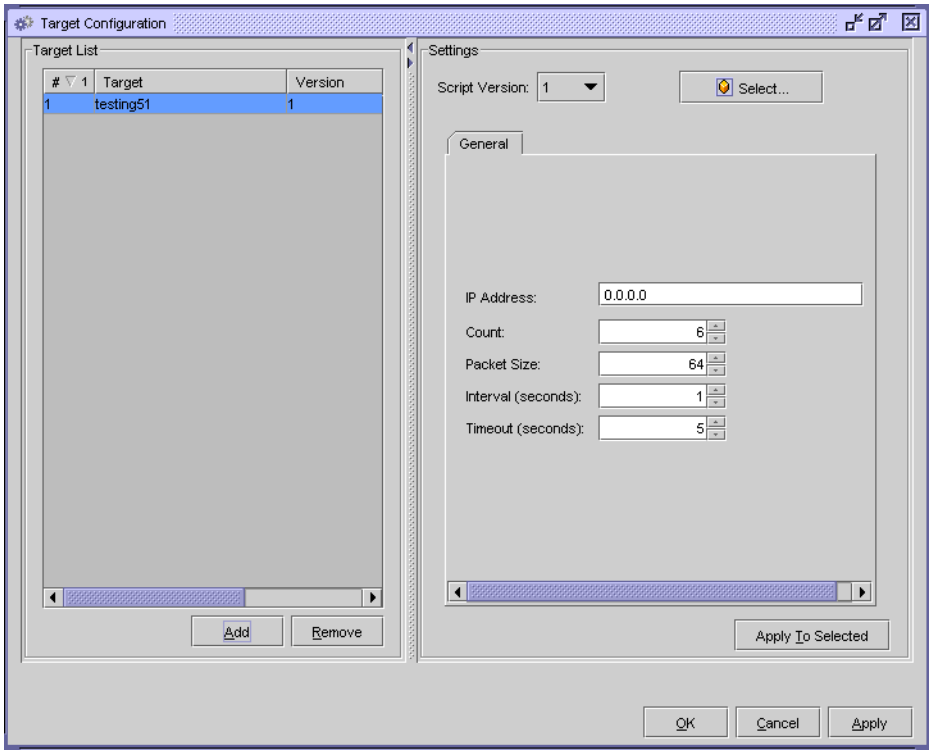
- IP Address
- Count
- Packet Size (octets)
- Interval (seconds)
- Timeout (seconds)

iii Click on the Apply To Selected button.

iv Repeat steps 10i to 10iii to configure additional targets, if required.

v Click on the OK button to close the Target Configuration form. The CLI Script (Edit) form opens with the Targets tab displayed.

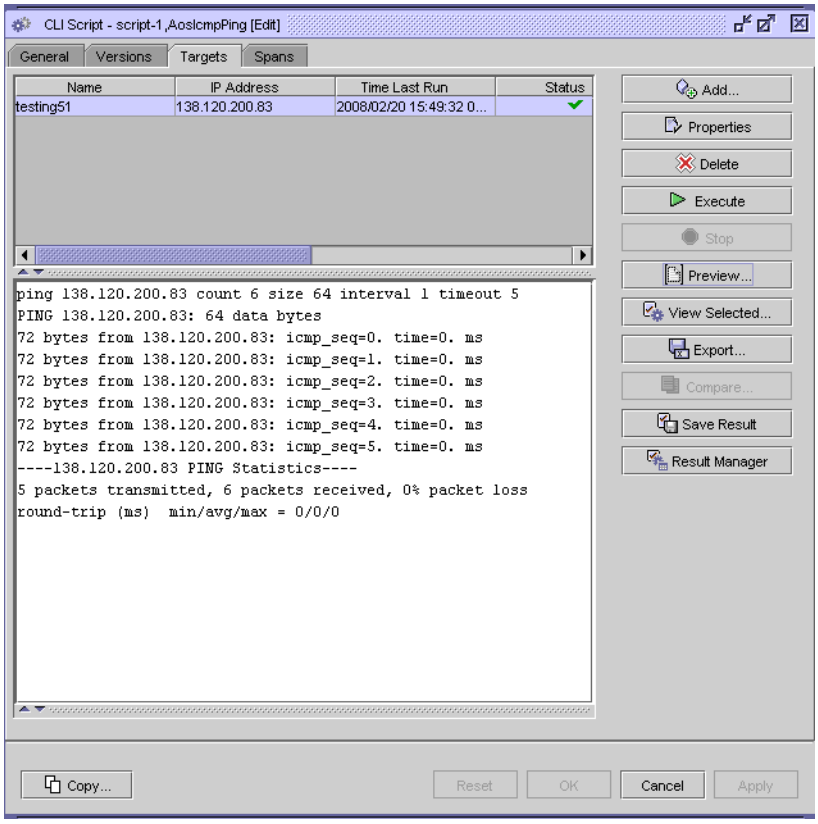
Figure 35-14 OmniSwitch ping target parameters form



11 To run the script on specified targets, choose one or more entries from the list.

12 Click on the Execute button. The results of the test appear, as shown in Figure 35-15.

Figure 35-15 OmniSwitch ping test results example



13 Perform one of the following to view the results of the scripts:

a Choose a target from the list. The results of the script that was run on the specified target appears in the panel below the list.

i Click on the Save Result button to save the results to the result manager. A dialog box appears. Click on the OK button.

Note — You can save the results of multiple scripts to the result manager simultaneously; choose the entries in the list and click on the Save Result button.

ii Export the results to a local or network text file.

iii Click on the Export button. A dialog box appears and prompts you to choose a file storage location on the network.

iv Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field.

v Click on the Export button. The results text file is saved in the specified location.

b Choose one or more entries from the list and click on the View Selected button. The View Selected form opens and displays the results of the script. The results for each target are separated by a comment that indicates the script version, associated target, script status, run time and date, and script parameters.

i Export the results of the script to a local or network text file. Choose File→Export from the Editor menu, or click on the Export button. A dialog box appears and prompts you to choose a file storage location in the network. Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field. Click on the Export button. The results text file is saved in the specified location.

ii Choose File→Close from the View Selected form to close the View Selected form.

14 Click on the OK button or Cancel button to close the CLI Script (Edit) form.

15 Close the Script Manager form.

Procedure 35-36 To configure and run an OmniSwitch OAM traceroute

Warning — Scripts that are not correctly created or applied can cause serious damage to the network. Alcatel-Lucent recommends that system administrators clearly define user responsibilities for CLI script usage, and ensure that scripts are verified and validated before they are executed on devices in a live network.

The following procedure describes how to configure and run an OmniSwitch traceroute using the script created using Procedure 35-34.

1 Ensure that the mediation policy for each OmniSwitch target is configured with the correct user name and password for CLI communication. See Procedure 13-4.

2 Choose Tools→Scripts from the 5620 SAM main menu. The Script Manager list form opens.

3 Choose CLI Script (script) from the object drop-down list.

4 Configure the filter criteria. A list of scripts appears at the bottom of the Script Manager form.

5 Double-click on the OmniSwitch traceroute script that you created using Procedure 35-34. The CLI Script (Edit) form opens with the General tab displayed.

6 Click on the Targets tab button.

7 Click on the Add button. The Target Configuration form opens.

8 Click on the Add button in the target list to add an OmniSwitch to the list. The Select Network Elements form opens with a list of OmniSwitch nodes.

9 Choose one or more OmniSwitch nodes and click on the OK button. The Select Network Elements form closes, and the OmniSwitch nodes appear in the target list panel of the Target Configuration form.

10 Configure the test parameters.

i Choose a target from the Target List panel.

ii Configure the parameters, as shown in Figure 35-16.

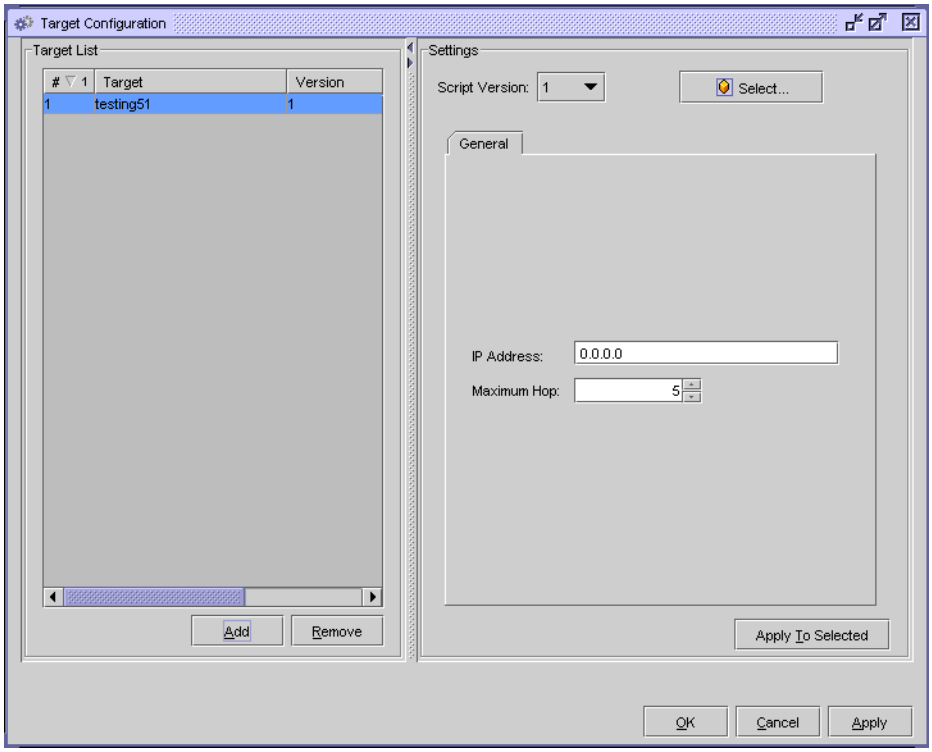
- IP Address
- Maximum Hop

iii Click on the Apply To Selected button.

iv Repeat steps 10i to 10iii to configure additional targets.

v Click on the OK button to close the Target Configuration form. The CLI Script (Edit) appears with the Targets tab displayed.

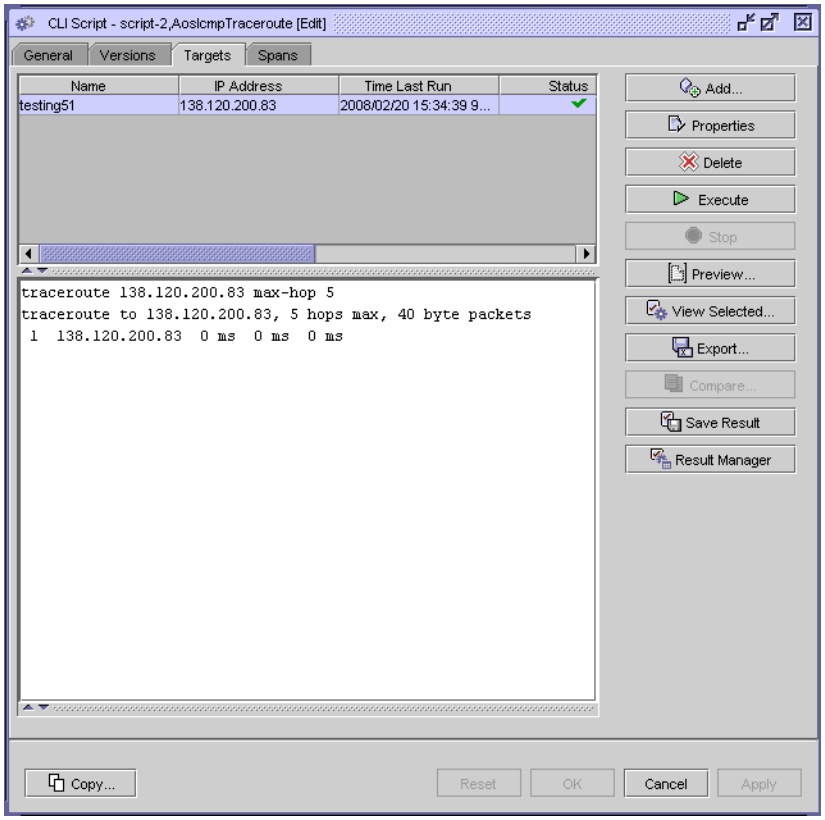
Figure 35-16 OmniSwitch traceroute target parameters form



11 To run the script on the specified targets, choose one or more entries from the list.

12 Click on the Execute button. The test results appear, as shown in Figure 35-17.

Figure 35-17 OmniSwitch traceroute test results example



13 Perform one of the following to view the results of the scripts:

a Choose a target from the list. The results of the script that was run on the specified target appears in the panel below the list.

i Click on the Save Result button to save the results to the result manager. A dialog box appears. Click on the OK button.

Note — You can save the results of multiple scripts to the result manager simultaneously; choose the entries in the list and click on the Save Result button.

ii Export the results to a local or network text file.

iii Click on the Export button. A dialog box appears and prompts you to choose a file storage location on the network.

iv Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field.

v Click on the Export button. The results text file is saved in the specified location.

b Choose one or more entries from the list and click on the View Selected button. The View Selected form opens and displays the results of the script. The results for each target are separated by a comment that indicates the script version, associated target, script status, run time and date, and script parameters.

i Export the results of the script to a local or network text file. Choose File→Export from the Editor menu, or click on the Export button. A dialog box appears and prompts you to choose a file storage location in the network. Scroll to the location in which you want to save the text file, and enter a filename in the appropriate field. Click on the Export button. The results text file is saved in the specified location.

ii Choose File→Close from the View Selected form to close the View Selected form.

14 Click on the OK button or Cancel button to close the CLI Script (Edit) form.

15 Close the Script Manager form.

Procedure 35-37 To configure and run a DNS ping

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose ICMP→Create DNS Ping from the Create contextual menu. The DNS Ping (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable
- NE Persistent
- Target Type
- System ID (Loopback IP Address)
- From IP Address
- Source IP Address
- DNS Server Type
- DNS Name
- DNS Server Address

The NE Schedulable parameter is configurable only if the NE Persistent parameter is not enabled.

The NE Persistent parameter is configurable only if the NE Schedulable parameter is not enabled.

5 Click on the Test Parameters tab button and configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)

6 Click on the Results Configuration tab button and configure the parameters:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Trap Generation

7 Click on the Apply button to save the settings.

8 Click on the Execute button to start the DNS ping. A deployed test is created and run. Open the deployed test from the Deployed Tests tab button to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

9 View the test results on the Results tab. The results depend on the type of test. See Procedure 35-43. Result information includes:

- Average Round-Trip Time
- Maximum Round-Trip Time
- Minimum Round-Trip Time
- Round-Trip Jitter
- Sum of Squares Round-Trip Time

10 To configure another DNS ping, click on the Clear button and repeat steps 5 to 9. Otherwise, go to step 11.

11 Click on the Cancel button to close the form.

Procedure 35-38 To configure threshold-crossing alarms on NE-schedulable OAM tests

You can configure threshold-crossing alarms for OAM tests that are NE-schedulable. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level.

You can also configure threshold-crossing alarms on test definitions within a test policy. See Procedure 75-10 for additional information.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Test (Assurance) icon from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of tests is displayed.

5 Choose an NE-schedulable test from the list and click on the Properties button. The Test (Edit) form opens with the General tab displayed.

6 Click on the Threshold Alarms tab.

7 Click on the Add button. The NE Threshold Event (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

9 Click on the Rising Threshold tab.

10 Configure the Threshold Value parameter.

11 Click on the Falling Threshold tab.

Note — The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the NM Threshold Event (Create) form.

12 Configure the Threshold Value parameter.

13 Click on the OK button. The NE Threshold Event (Create) form closes.

14 Repeat steps 7 to 13 to configure threshold events on additional tests.

15 Select a test from the list and click on the Execute button. A threshold-crossing alarm appears on the dynamic alarm list if the threshold rises above or falls below the configured level.

16 Close the Test (Edit) form. The Service Test Manager form reappears.

17 Close the Service Test Manager form.

Procedure 35-39 To configure NM threshold-crossing alarms on non-NE-schedulable OAM tests

You can configure NM threshold-crossing alarms for OAM tests that are non-NE-schedulable. NM threshold-crossing alarms are not configurable for service site ping, VPRN trace, MTU ping, Mrinfo and Mtrace tests. An alarm is raised when an NM threshold is crossed, either because the value rose above or fell below the configured level. The type of NM threshold-crossing event available for selection depends on the test type.

Non-NE-schedulable OAM tests can be configured as NE persistent. NE persistent tests are deployed to the network node after the first execution and remain on the node each time the test is executed.

You can also configure NM threshold-crossing alarms on test definitions within a test policy. See Procedure 75-11 for additional information.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Test (Assurance) icon from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of tests is displayed.

5 Choose a non-NE-schedulable test from the list and click on the Properties button. The Test (Edit) form opens with the General tab displayed.

6 Click on the NM Threshold Alarms tab.

7 Click on the Add button. The NM Threshold Event (Create) form opens with the General tab displayed.

8 Configure the parameters.

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

Note — If you are configuring an NM threshold-crossing alarm for an NE persistent test, the type of NM threshold-crossing event available for configuration depends on the test type.

9 Click on the NM Rising Threshold tab.

10 Configure the Threshold Value parameter.

11 Click on the NM Falling Threshold tab.

Note — The NM Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the NM Threshold Event (Create) form.

12 Configure the Threshold Value parameter.

13 Click on the OK button. The NM Threshold Event (Create) form closes, and a dialog box appears.

14 Click on the OK button.

15 Click on the Apply button on the Test (Edit) form. A dialog box appears.

16 Confirm the action. The test appears on the list.

17 Repeat steps 7 to 16 to configure NM threshold events on additional tests.

18 Select a test from the list and click on the Execute button. A threshold-crossing alarm appears on the dynamic alarm list if the threshold rises above or falls below the configured level.

19 Close the Test (Edit) form. The Service Test Manager form reappears.

20 Close the Service Test Manager form.

Procedure 35-40 To edit an OAM diagnostic test

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Test (Assurance) icon from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of tests is displayed.

5 Choose one or more OAM diagnostic tests from the results list and click on the Properties button. The appropriate edit form opens.

6 Change any configurable parameter for the test.

7 Click on the OK button to save the changes. A dialog box appears.

8 Confirm the action. The modified test or tests are shown in the list.

Procedure 35-41 To delete an OAM diagnostic test

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test (Assurance) icon from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of tests is displayed.

5 Choose one or more OAM diagnostic tests from the results list and click on the Properties button. The appropriate edit form opens.

6 Choose one or more OAM diagnostic tests from the results list and click on the Delete button. A dialog box appears.

7 Confirm the action. The test or tests are deleted from the list of available OAM diagnostic tests.

Procedure 35-42 To set STM managed device test limits

You can configure the maximum number of pings and traces allowed to be performed from the 5620 SAM by the managed devices, or you can limit the number of tests performed. The default is to allow an unlimited number of tests.

Note — Limiting the number of tests does not raise an alarm on 5620 SAM or an SNMP trap on the managed device. The indication that the limit has been reached is no returned test results.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose NE Test Agent (Assurance) from the object drop-down list.

3 Click on the Search button. A list of NE Test Agent policies appears, one for each managed device.

4 Choose on one or more policies from the list and click on the Properties button. The configuration form opens.

5 You can set the number of tests allowed for individual managed devices, or for all managed devices, using the following parameters:

- Unlimited Concurrent Pings
- Unlimited Concurrent Traces
- Maximum Concurrent Pings
- Maximum Concurrent Traces

6 Click on the Apply button to save the changes. A dialog box appears.

7 Click on the Yes button to confirm the action.

Procedure 35-43 To view OAM diagnostic test results

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Navigate to the test results.

The navigation path is Result (Assurance)→Test Result (Assurance). The ActionResult (Assurance), Ping Result (Assurance), and Trace Result (Assurance) objects contain the test results.

3 Select a filter option. Use the configurable filters choices and properties options on the Service Test Manager form and click on the Search button. The list of test results that meet the filter criteria are displayed.

4 Choose a test result from the list and click on the Properties button. The appropriate OAM diagnostic test results form opens with the General tab displayed.

5 Click on the form tabs to view the test results for the OAM diagnostic. You can click on the View button beside an object and open the properties form for the object.microseconds

a CFM Continuity Check OAM diagnostic information includes:

- identifies the MD and MEG involved in the test
- MEP creation on a SAP
- MEP creation on a SDP
- intervals (seconds) between continuity checks
- MHF creation

b CFM loopback OAM diagnostic information includes:

- originating node
- originating MEP
- destination MAC addresses
- data size
- VLAN priority
- number of messages sent

c CFM link trace OAM diagnostic information includes:

- originating node
- originating MEP
- target MAC addresses
- TTL

d CFM One Way OAM diagnostic information includes:

- originating node
- originating MEP
- destination MAC addresses
- priority

e CFM Two Way OAM diagnostic information includes:

- originating node
- originating MEP
- destination MAC addresses
- VLAN priority

f CFM Single Ended Loss OAM diagnostic information includes:

- originating node
- originating MEP
- destination MAC addresses
- test duration, in seconds
- number of LMR frames received
- number of frames transmitted by the far end
- number of frames received by the near end
- number of frames lost at the near end
- percentage of frames lost at the near end
- number of frames transmitted by the near end
- number of frames received by the far end
- number of frames lost at the far end
- percentage of frames lost at the far end

g CFM Eth Test OAM diagnostic information includes:

- originating node
- originating MEP
- destination MAC addresses
- data size
- VLAN priority

h MTU ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and destination site IP addresses
- originating tunnel ID
- administrative and operational states
- information about previous diagnostics, including the start and finish sizes of the MTU datagram (packet)
- ID of the service being diagnosed
- name of the service being diagnosed
- MTU response size, indicating the largest packet size that the tunnel can transport

i Tunnel ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and destination site IP addresses
- originating and return tunnel IDs
- administrative state
- operational state
- probes to be issued information
- message size
- forwarding class used by the service
- ID of the service being diagnosed
- name of the service being diagnosed
- average, minimum, and maximum one-way time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way time for all ping responses received, used to enable a standard deviation calculation
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available

j VPRN ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- inner and outer encapsulation value of the SAP supporting the requested ping response, when the address type is a SAP and in the case that the inner encapsulation value is from a 5620 SAM-managed device

k VPRN trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses

l VPRN ICMP ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available

m VPRN ICMP trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target IP addresses
- operational size
- number of responses
- initial and maximum time to live
- time to wait (microseconds)

n MAC ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source MAC addresses
- service ID and name
- number of probes to be issued
- administrative and operational states
- information about previous diagnostics
- average, minimum, and maximum round-trip time values, in microseconds, with a value of 0 indicating no round-trip measurement is available
- sum-of-squares round-trip time for all ping responses received, used to enable a standard deviation calculation

o MEF MAC Ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target MAC address
- service ID and name
- number of probes to be issued
- round trip jitter
- round trip latency
- round trip frame Loss

p MAC trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source MAC addresses
- service ID and name
- number of probes to be issued
- administrative and operational states
- information about previous diagnostics

q Service site ping OAM diagnostic information includes:

- target and source IP addresses
- service ID and name
- probes to be issued information
- check mark buttons to specify whether a local tunnel, remote tunnel, or local and remote tunnel is performed
- information about previous service site OAM diagnostics, including probes sent and responses received, loss percentage, packet timeouts, and last good packet time
- ID of the service being diagnosed

r VCCV ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- IP address of the destination and far-end devices
- time of last response
- number of responses received
- response time
- loss indicator, with a value of 0 indicating that the test packet was received and a value of 1 indicating that the test packet was lost
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

s VCCV trace OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- number of probes to be issued
- time of last response
- source and response IP addresses
- number of hops
- probe responses from nodes in path

t LSP ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

u P2MP LSP ping diagnostic information includes:

- information about the configuration test, including the configured parameter values
- test probe: size, Time to Live, Forwarding Class, Forwarding Profile
- results: probes sent, responses received, probe timeouts, probes lost
- probe result status
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum outbound and inbound one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

v P2MP LSP trace diagnostic information includes:

- information about the configuration test, including the configured parameter values
- trace attempt: size, Initial Time to Live, Forwarding Class, Forwarding Profile
- probe result status
- number of probes sent
- responses received
- timeouts
- failures
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum outbound and inbound one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

w LDP Tree Trace Result diagnostic information includes:

- information about the configuration test, including the configured parameter values
- number and IP address of hops included in the test
- destination IP address of the path associated with the hop
- next hop IP address
- a display of available hops in a tree format

x Multicast router OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- status of diagnostic
- number of sent, received, and lost packets
- packet loss percentage
- number of packet timeouts
- time for last successful contact with the target IP address

y Multicast trace OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and group multicast addresses
- destination and response IP addresses
- virtual router ID
- number of hops in path
- response from nodes in path
- number of trace attempts
- number of successful traces
- time for last successful trace
- identifier if multicast path changed from last successful trace

z Multicast FIB ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- service ID and name
- number of probes to be issued
- operational size
- number of responses
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum one-way trip time values, in microseconds, with a value of 0 indicating that no one-way trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

aa ICMP ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- target and source IP addresses
- virtual router ID
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- average, minimum, and maximum round-trip time values, in microseconds, with a value of 0 indicating that no round-trip measurement is available
- sum-of-squares one-way trip time for all ping responses received, used to enable a standard deviation calculation

ab ICMP trace OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and target IP addresses
- virtual router ID
- number of hops
- probe responses from managed devices
- number of trace probe attempts
- number of successful traces
- time for last successful trace
- initial and maximum time to live values

ac DNS ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- average, minimum, and maximum round-trip time values, in microseconds, with a value of 0 indicating that no round-trip measurement is available
- sum-of-squares round-trip time for all ping responses received, used to enable a standard deviation calculation
- round-trip jitter, in microseconds, for a ping probe, with a value of 0 indicating that no measurement is available
- the IP Address for the requested DNS name, as reachable by the DNS server, shown for IPv4 addresses in dotted-decimal format
- status, including response received to indicate a successfully completed diagnostic

ad ANCP ping OAM diagnostic information includes:

- information about the configuration test, including the configured parameter values
- source and destination site IP addresses
- administrative and operational states
- ID of the circuit being diagnosed
- information about previous ANCP OAM diagnostics, including packet history size, probes sent and responses received, and packet failure

Procedure 35-44 To interpret OAM diagnostic results

1 Perform the OAM diagnostic, as described in Procedure 35-1 to Procedure 35-31.

2 Perform Procedure 35-43 to view OAM diagnostic test results.

3 The General and Response Packets tabs display the key information about OAM diagnostic results. When there is no packet information required, as for an OAM ping, the information appears on the Packets Results form without any tab buttons. For example, status and return code information appears directly on the Packets Results form. You can view test packet information by performing the following actions:

i Click on the Response Packets tab button. A list of test objects appears.

ii Choose an object from the display and click on the Properties button. The Packets Results form opens.

4 Interpret the results, based on the status and return code information.

a For MTU OAM diagnostics, the key information is how many frames were sent and incrementally increased in size before the frames could not be sent. When the frame cannot be sent because it is too large, that results in a request timeout message. The largest frame that was sent is the last frame size with an associated success response.

b For tunnel OAM diagnostics, the key information is the result of the diagnostic, displayed in the status message. Table 35-3 lists the displayed messages and descriptions.

Table 35-3 Tunnel OAM diagnostics results

Displayed message	Description
Request Timeout	The request timed out with a reply.
Orig-SDP Non-Existent	The request was not sent because the originating SDP does not exist.
Orig-SDP Admin-Down	The request was not sent because the originating SDP administrative state is operationally down.
Orig-SDP Oper-Down	The request was not sent because the originating SDP operational state is down.
Request Terminated	The operator terminated the request before a reply could be received or before the timeout of the request could occur.
Far End: Originator-ID Invalid	The request was received by the far end, but the far end indicates that the originating SDP ID is invalid.
Far End: Responder-ID Invalid	The request was received by the far end, but the responder ID is not the same destination SDP ID that was specified.
Far End:Resp-SDP Non-Existent	The reply was received, but the return SDP ID used to respond to the request does not exist
Far End:Resp-SDP Invalid	The reply was received, but the return SDP ID used to respond to the request is invalid.
Far End:Resp-SDP Down	The reply was received, but the return SDP ID indicates that the administrative or operational state of the SDP is down.
Success	The tunnel is in service and working as expected. A reply was received without any errors.

c For service site OAM diagnostics, the key information is the result of the diagnostic, which is displayed in the status message and with the other records from the General tab.

As the diagnostic traverses the service across the originating and destination IP addresses, the service tunnels, and the used VCs, the status of each portion of the service is displayed. Table 35-4 lists the displayed messages and descriptions.

Table 35-4 Service site OAM diagnostics results

Displayed message	Description
Sent - Request Timeout	The request timed out with a reply.
Sent - Request Terminated	The request was not sent because the diagnostic was terminated by the operator.
Sent - Reply Received	The request was sent and a successful reply message was received.
Not Sent - Non-Existent Service-ID	The configured service ID does not exist.
Not Sent - Non-Existent SDP for Service	There is no SDP for the service being tested.
Not Sent - SDP For Service Down	The SDP for the service is down.
Not Sent - Non-Existent Service Egress Label	There is a service label mismatch between the originator and responder.

d For MAC, VPRN, and multicast FIB ping OAM diagnostics, the key information is the result of the diagnostic. Table 35-5 lists the displayed messages, the return code, and descriptions.

Table 35-5 MAC, VPRN, multicast FIB ping OAM diagnostics results

Displayed message (return code)	Description
notApplicable (0)	The OAM diagnostic message does not apply to the OAM diagnostic performed.
fecEgress (1)	The replying router is an egress for the FEC.
fecNoMap (2)	The replying router has no mapping for the FEC.
notDownstream (3)	The replying router is not a downstream router.
downstream (4)	The replying router is a downstream router, and the mapping for this FEC on the router interface is the specified label.
downstreamNotLabel (5)	The replying router is a downstream router, and the mapping for this FEC on the router interface is not the specified label.
downstreamNotMac (6)	The replying router is a downstream router, but it does not have the specified MAC address.
downstreamNotMacFlood (7)	The replying router is a downstream router, but it does not have the specified MAC address and cannot flood the request to other routers.
malformedEchoRequest (8)	The received echo request is malformed.

(1 of 2)

Displayed message (return code)	Description
tlvNotUnderstood (9)	One or more TLVs were not understood.
downstreamNotInMFib (10)	The replaying router is a downstream router, but it is not part of the MFIB.
Downstream mapping mismatched (11)	The downstream mapping is mismatched.
Upstream interface index unknown (12)	The upstream interface index is unknown.
Label switched but no MPLS forwarding at stack-depth (13)	The label switched successfully but MPLS forwarding did not occur at stack-depth.
No label entry at stack-depth (14)	The label entry at stack-depth did not occur.
Protocol not associated with interface at FEC stack-depth (15)	The protocol is not associated with the interface at FEC stack-depth.
Premature termination of ping due to label stack shrinking to a single label (16)	The ping was terminated prematurely due to the label stack shrinking to a single label.

(2 of 2)

e For multicast router OAM diagnostics, the key information includes information that is related to adjacent routers, supported protocols, traffic metrics, and time-to-live thresholds. Administrators can use this information to identify bidirectional adjacency relationships.

f For multicast trace OAM diagnostics, the key information is the result of the diagnostic, displayed in the status message. Table 35-6 lists the displayed messages and descriptions.

Table 35-6 Multicast trace OAM diagnostics results

Displayed message	Description
No Error	No error.
Wrong Interface	The router not forwarding the multicast source or group traffic because the router is not part of the multicast path.
Prune Sent	The router sent a prune request upstream that impacts the multicast source and group in the trace request.
Prune Received	The router stopped forwarding traffic for the multicast source and group in response to a request from the next hop router.
Scoped	The multicast group is subject to administrative scoping.
No Route	The router has no route for the multicast source or group and no way to determine a potential route.
Wrong Last Hop	The router is not the correct last-hop router.
Not Forwarding	The router is not forwarding the multicast source or group traffic for an unspecified reason.
Reached RP or Core	Request arrived on the rendezvous point or core.
Request on RPF	The request arrived on the expected RPF interface.
No Multicast	The request arrived on an interface that is not enabled for multicast traffic.
Hops Hidden	One or more hops are hidden from the trace.
Fatal Error	Fatal error.
No Space	There is insufficient room to insert another response data block in the packet.
Old Router	The previous router hop cannot process the multicast trace request.
Admin. Prohibited	The multicast trace was administratively prohibited.
Unknown	—

g For most diagnostics, some common return codes are used. The return codes indicate the status of OAM tests, usually when there was a problem performing the test. Table 35-7 lists the messages, return codes, and descriptions.

Table 35-7 OAM diagnostics return codes

Displayed message (return code)	Description
responseReceived (1)	A response was received on the device to the OAM diagnostic performed.
unknown (2)	The OAM diagnostic failed for an unknown reason.
internalError (3)	An internal error on the device caused the diagnostic to not be performed.
maxConcurrentLimit Reached (4)	The device cannot perform the OAM diagnostics because there are too many OAM diagnostic operations already running.
requestTimedOut (5)	The OAM diagnostic could not be completed because no reply was received within the allocated timeout period.
unknownSDPOrigin (6)	Indicates an invalid or non-existent originating service tunnel.
downOrigSdpId (7)	The originating service tunnel is operationally down.
requestTerminated (8)	The OAM diagnostic was cancelled before the timeout or reply period was reached.
invalidOriginatorId (9)	The far-end device replied indicating that the originating ID was invalid.
invalidResponderId (10)	The far-end device replied with an invalid responding ID.
unknownRespSdpId (11)	The far-end device replied with an invalid response service tunnel ID.
downRespSdpId (12)	The responding service tunnel with the given ID is operationally or administratively down.
invalidServiceId (13)	An invalid or non-existent service ID.
invalidSdp (14)	An invalid or non-existent service tunnel for the service.
downServiceSdp (15)	The service tunnel bound to the service is down.
noServiceEgressLabel (16)	The egress label for the service does not exist.
invalidHostAddress (17)	The IP address for the host is invalid, for example, in the case of a broadcast or multicast IP address.
invalidMacAddress (18)	The MAC address specified in the OAM diagnostic is invalid.
invalidLspName (19)	The LSP name specified in the OAM diagnostic is invalid.
macIsLocal (20)	The MAC address is the local SAP or device MAC address, not the MAC address of the downstream SAP or device, therefore the MAC ping or trace cannot be sent.
farEndUnreachable (21)	No route is available to the far-end GRE service tunnel.
downOriginatorId (22)	The originating ping device is operationally down.
downResponderId (23)	The device responding to the ping is operationally down.
changedResponderId (24)	The ID of the device responding to the ping has changed.
downOrigSvcId (25)	The originating service identified by the ID is operationally down.
downRespSvcId (26)	The service responding to the ping identified by the ID is operationally down.
noServiceIngressLabel (27)	The ingress label for the service does not exist.
mismatchCustId (28)	The subscriber ID identified with the service differs from the originating device compared to the responding device.
mismatchSvcType (29)	The service type identified with the service differs from one device to another.
mismatchSvcMtu (30)	The service MTU size associated with the service differs from the originating device compared to the responding device.
mismatchSvcLabel (31)	The service label identified with the service differs from the originating device compared to the responding device.

(1 of 4)

Displayed message (return code)	Description
noSdpBoundToSvc (32)	There is no service tunnel bound to the service.
downOrigSdpBinding (33)	The service tunnel associated with the originating device's service is operationally down.
invalidLspPathName (34)	The LSP path name specified in the OAM diagnostic is invalid.
noLspEndpointAddr (35)	There is no LSP endpoint address specified in the OAM diagnostic.
noActiveLspPath (36)	There is no active LSP path.
downLspPath (37)	The far end of the LSP is operationally down.
invalidLspProtocol (38)	The LSP protocol is not valid or is not supported.
invalidLspLabel (39)	The LSP label is invalid.
routeIsLocal (40)	For a VPRN ping, the route is a local route.
noRouteToDest (41)	For a VPRN ping, there is no route available to the destination of the OAM diagnostic.
localExtranetRoute (42)	For a VPRN ping, the route is a local extranet route.
srcIpInBgpVpnRoute (43)	For a VPRN ping, the source IP address belongs to a BGP VPN route.
srcIpInvalid (44)	For a VPRN ping, the source IP address is invalid or no route is available to the source IP address.
bgpDaemonBusy (45)	For a VPRN trace, the BGP routing process is busy on the device, and VPRN route target information cannot be retrieved.
mcastNotEnabled (46)	Multicast is not enabled on the device, so the diagnostic cannot be performed.
mTraceNoSGFlow (47)	—
mTraceSysIpNotCfg (48)	The system IP address is not configured. The address is required for a response to a multicast trace.
noFwdEntryInMfib (49)	No forwarding entry could be found for the specified source and destination addresses in the MFIB.
dnsNameNotFound (50)	The domain name specified in the dns query does not exist
noSocket (51)	For icmp-ping, unable to get socket.
socketOptVprnIdFail (52)	For icmp-ping, unable to set SO_VPRNID for socket.
socketOptIfIndexFail (53)	For icmp-ping, unable to set IP_IFINDEX for socket.
socketOptNextHopFail (54)	For icmp-ping, unable to set IP_NEXT_HOP for socket.
socketOptMtuDiscFail (55)	For icmp-ping, unable to set IP_MTU_DISC for socket.
socketOptSndbufFail (56)	For icmp-ping, unable to set SO_SNDBUF for socket.
socketOptHdrincFail (57)	For icmp-ping, unable to set IP_HDRINCL for socket.
socketOptTosFail (58)	For icmp-ping, unable to set IP_TOS for socket.
socketOptTtlFail (59)	For icmp-ping, unable to set IP_TTL for socket.
bindSocketFail (60)	For icmp-ping, unable to bind socket.
noRouteByIntf (61)	For icmp-ping, no route to destination via the specified interface.
noIntf (62)	For icmp-ping, no interface specified.
noLocalIp (63)	For icmp-ping, unable to find local ip address.
sendtoFail (64)	For icmp-ping, sendto function failed.

(2 of 4)

Displayed message (return code)	Description
rcvdWrongType (65)	For icmp-ping, received packet of wrong icmp type.
noDirectInterface (66)	For icmp-ping, no direct interface to reach destination.
nexthopUnreachable (67)	For icmp-ping, unable to reach the next-hop.
socketOptHwTimeStampFail (68)	For icmp-ping, unable to set IP_TIM_TIME for socket.
noSpokeSdpInVll (69)	For vccv-ping, unable to find spoke-sdp given SdpId:vc-id
farEndVccvNotSupported (70)	For vccv-ping, far end does not support the VCCV options.
noVcEgressLabel (71)	For vccv-ping, no Vc egress label to send vccv-ping
socketOptIpSessionFail (72)	For icmp-ping, unable to set IP_SESSION for socket.
rcvdWrongSize (73)	For icmp-ping, received packet of wrong size.
dnsLookupFail (74)	For icmp-ping, dns lookup failed.
noIpv6SrcAddrOnIntf (75)	For icmp-ping, no ipv6 source on the interface.
multipathNotSupported (76)	For lsp-trace, downstream node does not support multipath.
nhIntfNameNotFound (77)	For lsp-ping/trace, Given next-hop interface name not found.
msPwInvalidReplyMode (78)	For vccv-ping, MS-PW switching node supports ip-routed reply mode only.
ancpNoAncpString (79)	ANCP string unknown to the system.
ancpNoSubscriber (80)	Subscriber unknown to the system.
ancpNoAncpStringForSubscriber (81)	Subscriber has no associated ANCP string.
ancpNoAccessNodeforAncpString (82)	No access node is found for the given ANCP string.
ancpNoAncpCapabilityNegotiated (83)	ANCP capability not negotiated with the involved DSLAM.
ancpOtherTestInProgress (84)	Another ANCP test is running for this ANCP string.
ancpMaxNbrAncpTestsInProgress (85)	Maximum number of concurrent ANCP tests reached.
spokeSdpOperDown (86)	For vccv-ping, spoke-sdp is operationally down.
noMsPwVccvInReplyDir (87)	Switching node in MS-PW with no vccv support in echo reply direction.
p2mpLspNameOrInstInvalid (88)	P2MP LSP name or instance provided is not valid.
p2mpLspS2LPathDown (89)	LSP path to S2L is down.
p2mpLspS2LAddressInvalid (90)	One or more S2L address is not valid.
p2mpLspNotOperational (91)	P2MP LSP is operationally down.
p2mpLspTrMultipleReplies (92)	Probe returned multiple responses. Result may be inconsistent.
invalidMepId (93)	The user-configured MEP identifier is not valid.
multipleReplies (94)	More than one reply received, when one was expected.
packetSizeTooBig (95)	Packet size is too big.
gtpPingError (96)	General GTP Ping Error.
gtpPingRsrcUnavailable (97)	GTP Path management resource unavailable.
gtpPingDupRequest (98)	Duplicate request for the same peer.

(3 of 4)

Displayed message (return code)	Description
gtpPingCleanUpInProg (99)	GTP Path management clean up in progress.
invalidInterface (100)	The egress interface specified does not exist.

(4 of 4)

36 — VRRP

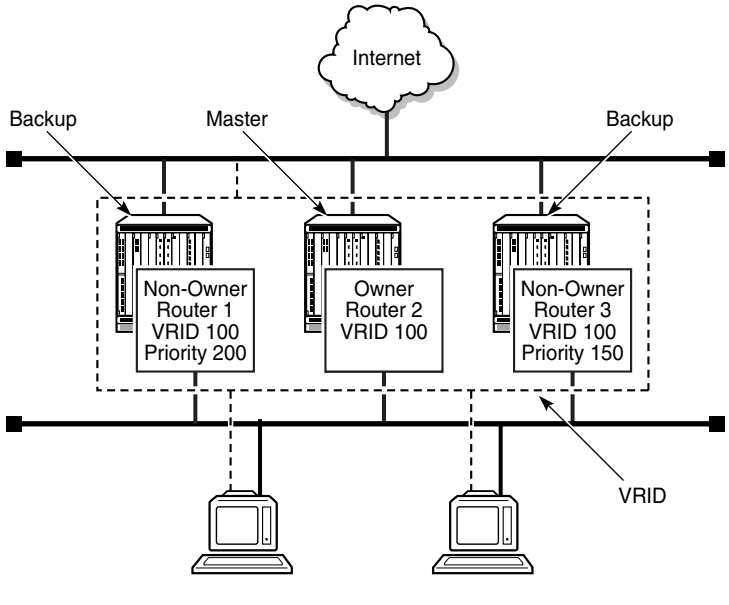
36.1 VRRP overview

The 5620 SAM supports VRRP management. VRRP creates a redundant routing system that takes over packet transmission on a common LAN segment when a router fails. VRRP designates alternative routing paths in the form of virtual routers, or VRs, without changing the IP or MAC address of a protected router.

A VRRP protected router owns the IP address of the VR. The VRRP owner forwards packets using the default gateway. When the owner router fails, packet-forwarding responsibilities are transferred to a designated backup router. This router becomes the master and forwards packets using the VR IP address.

Figure 36-1 shows a basic VR that acts in parallel with the real network. Router 2 is the owner with the address from which packets are forwarded. If Router 2 fails, Router 3, which has been configured to route using the master address in a backup role, begins to forward packets using this IP address. Router 1 is also a backup router, but because its priority number is higher, it ranks below Router 3.

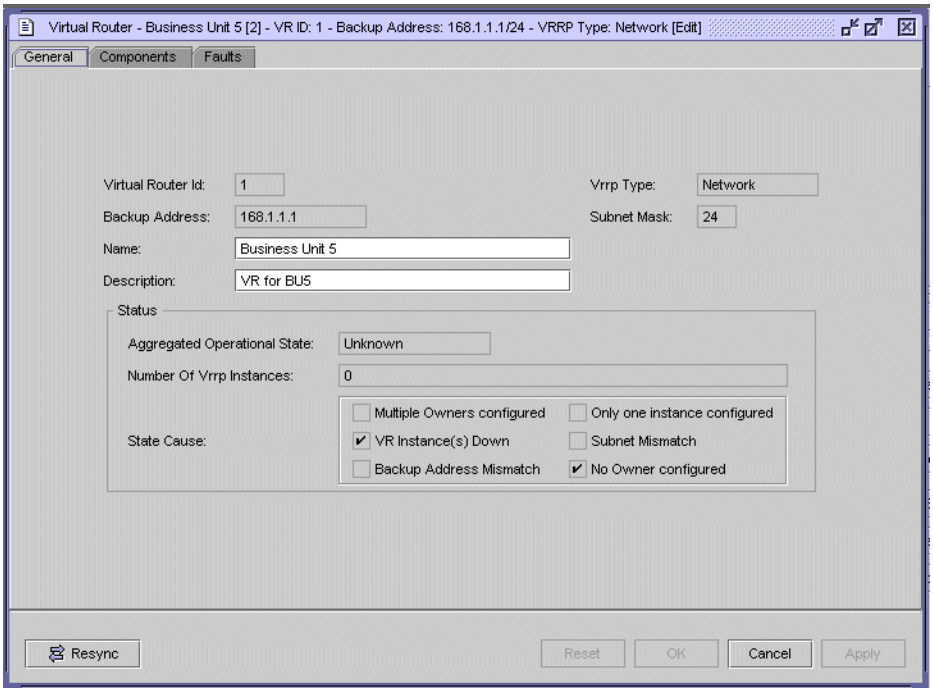
Figure 36-1 VR concepts



The 5620 SAM supports the configuration of VRs for network interfaces and for L3 access interfaces using the tabbed configuration form shown in Figure 36-2.

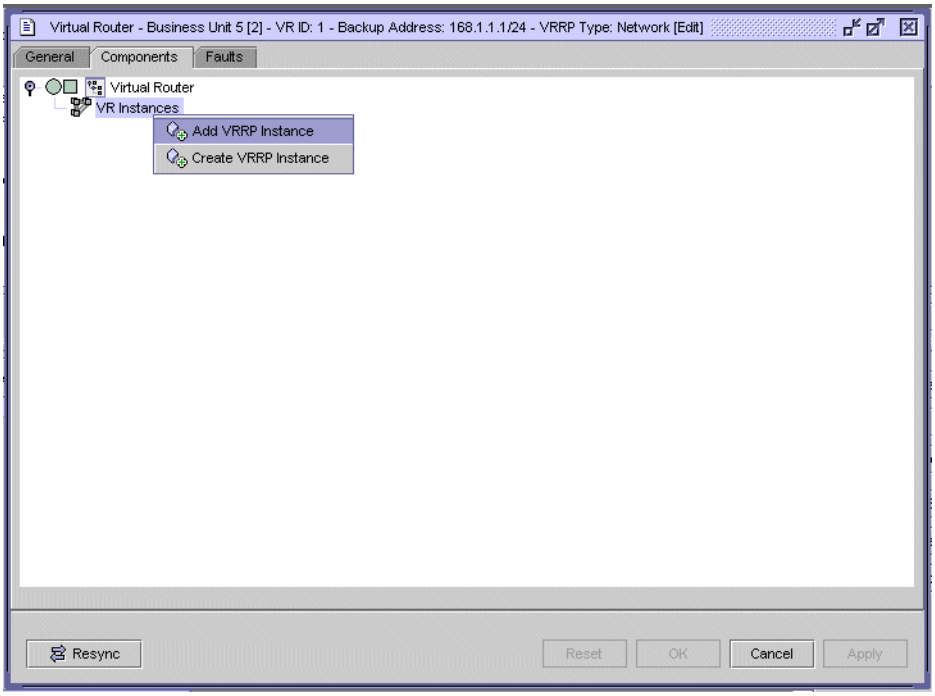
VRRP in an IES involves interfaces from separate IESs. VRRP in a VPRN requires interfaces that are in the same VPRN service. The 5620 SAM supports on-demand, but not scheduled, statistics collection for VRRP in a VPRN. Certain VRRP SNMP traps do not apply to VPRN; see the appropriate NE documentation for information.

Figure 36-2 VRRP management - General



You can configure the VR through another set of tabbed forms and a navigation tree, which allows you to add VRRP instances IP owner and non-owner router interfaces, as shown in Figure 36-3.

Figure 36-3 Adding or creating a VRRP instance

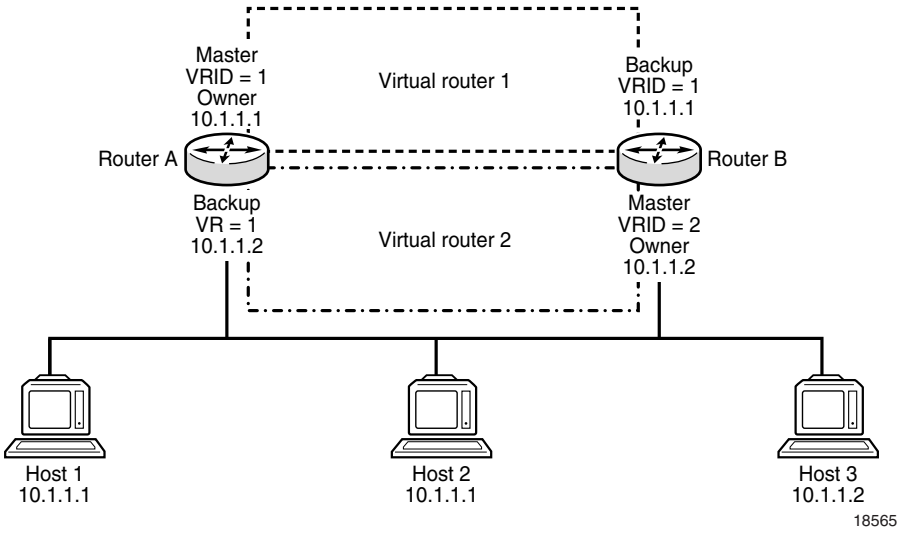


VR

A VR is a logical entity, managed by VRRP, that acts as a default router for hosts on a shared LAN. The VR consists of a VRID and a subnet (that is, ip_address/mask). A VRRP router can back up one or more VRs. The purpose of supporting multiple IP addresses in a single VR is for multi-netting. This common mechanism allows multiple local subnet attachments on a single routing interface. Up to four VRs are allowed on a single Alcatel-Lucent IP interface. The VRs must be in the same subnet.

Figure 36-4 shows a common VR setup in which associated routers provide mutual backup using VRRP. Router A forwards packets on IP address 10.1.1.1 to Hosts 1 and 2 on its default gateway. Router B forwards packets on IP address 10.1.1.2 to Host 3 on its default gateway. If Router A fails, VRID 1 uses IP address 10.1.1.1 to forward packets from Router B to Hosts 1 and 2. At the same time, the Router B interface is still configured to deliver packets on IP address 10.1.1.2 to Host 3. If Router B fails, VRID 2 forwards these packets through backup Router A.

Figure 36-4 Sample VRs



Master router

The VRRP master router, in either a normal or a failover situation, routes all IP packets into the LAN using the physical MAC address for the IP interface as the Layer 2 source MAC address. ARP packets also use the parent IP interface MAC address as the Layer 2 source MAC address.

Owner and non-owner VRRP instances

A VRRP instance is configured in either an owner or non-owner mode.

The owner instance controls the IP address of the VR and is responsible for forwarding packets sent to this IP address. The IP address of the owner VRRP instance is the same as the real interface IP address of the router. The owner assumes the role of the master VR when it is functioning normally in the network. Only one VRRP instance in the domain is configured as the owner. All other instances participating in the domain are non-owners and must have the same VRID.

A backup router becomes the master router after a failover and continues to use the IP address of the original master. As a result, the new master router is the IP address non-owner.

The most important parameter to define for a non-owner VRRP instance is the priority. The priority defines for a VR the selection order. The priority value and the preempt mode combine to determine which VR has the highest priority and becomes the master.

The base priority is used to derive the in-use priority of the VRRP instance as modified by an optional VRRP priority-control policy. VRRP priority-control policies are used to either override or adjust the base priority value depending on events or conditions in the node. See chapter 51 for more information.

VRRP types

When you create a VR, you specify the VRRP type, for example, network or L3 service, and the VR instance is restricted to the specified VRRP type. Configuring a VR using a mix of network and service interfaces through CLI raises a configuration mismatch alarm.

Primary addresses

A primary IP address is an address that is selected from the set of real interface addresses on the VR. VRRP advertisements between master and backup VRRP instances are sent using the primary IP address as the source of the IP packet.

The 7450 ESS or 7750 SR IP interface must always have an assigned primary IP address for VRRP to operate on the interface. The primary IP address of the VR and the primary address on the IP interface are always the same.

Backup addresses

A maximum of 16 IP addresses (for either IPv4 or IPv6) in different subnets can be configured for a VRRP instance. One backup address is permitted for a subnet. The number of backup addresses is limited to the number of primary and secondary addresses configured on the IP interface.

The backup IP addresses for the owner VRRP instance must match the primary address or one of the secondary addresses on the IP interface. If the VRRP instance is not the owner, the backup addresses must be in the subnets of the primary and secondary addresses of the IP interface.

The 5620 SAM includes only eligible IP addresses in the search list.

VRRP message authentication

The type of authentication used by the VR in VRRP advertisement is specified during VRRP instance creation. The current master router uses the configured authentication type when sending VRRP advertisements to backup routers, which authenticate the messages.

36.2 Workflow to configure VRRP

1. Before you create a VR, ensure that a primary IP address is configured for the network or L3 service interface. Each interface must have a primary IP address.
2. Configure the VRRP priority-control policy for a non-owner VRRP instance. See chapter 51 for more information about VRRP priority-control policy events.
3. Create the VR.
   - i. Specify the VRID.
   - ii. Specify the backup IP address.
   - iii. Define the VRRP type.
   - iv. Specify the subnet mask.
4. Create VRRP instances in the VR, as required:
   - Configure the L3 service or network interface ID.
   - Define the owner status.
   - Configure the base priority.
   - Configure the MAC address.
   - Configure message intervals.
   - Configure non-owner parameters, if required.
   - Configure authentication.

36.3 VRRP management procedures

Use the following procedures to perform VR creation and VRRP management tasks.

Procedure 36-1 To create a VR

1. Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.
2. Click on the Create button. The Virtual Router (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Virtual Router ID
- Backup Address
- Name
- Description
- VRRP Type
- Subnet Mask

If you are creating an IPv6 VR, the Backup Address parameter value that you specify must be an IPv6 address.

4 Click on the OK button. The Virtual Router (Create) form closes.

Procedure 36-2 To create and configure a VRRP instance

Before you create a VRRP instance on an interface, ensure that the L3 service or network interface is configured with a primary IP address. The backup IP address that is configured in Procedure 36-1 must belong to the same subnet as the primary IP address of the owner VRRP instance created in this procedure. The 5620 SAM automatically configures a backup address using the IP address of the VR. A search of interface IDs in step 7 of this procedure displays the interface IDs that are eligible for the creation of a VRRP instance for the VR.

You can configure up to a total of four VRRP instances (IPv4 plus IPv6) on one IP interface. However, only one IPv6 instance can be included in this total. On a Release 7.0 or later NE, the global limit for the number of either one or mixed IPv4-IPv6 VRRP instances is 1024. For earlier NE releases, only IPv4 VRRP instances are supported, and the limit is 255.

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Select and right-click on VR Instances and choose Create VRRP Instance from the contextual menu. The VRRP Instance (Create) form opens with the General tab displayed.

Note — If the Backup Address parameter value that you specified in step 3 of Procedure 36-1 is an IPv6 address, then the contextual menu item is Create VRRP IPv6 Instance, and the VRRP IPv6 Instance (Create) form opens.

6 Click on the Select button in the Interface panel. The Select Interface - VRRP Instance or Select Interface - VRRP IPv6 Instance form opens, depending on whether you are creating an IPv4 or IPv6 VRRP Instance respectively.

7 Use the configurable filter and Search button to choose an interface, and click on the OK button. The Select Interface - VRRP Instance (or Select Interface - VRRP IPv6 Instance) form closes and the VRRP Instance (Create) (or VRRP IPv6 Instance (Create)) form reappears with the interface information displayed.

8 Configure the parameters:

- Owner
- Administrative State
- Base Priority

9 If the Owner parameter in step 8 is set to true, you cannot configure the Administrative State and Base Priority parameters and you cannot associate a policy with this VRRP instance. Go to step 11.

10 Assign a VRRP policy to the instance, if required.

Note — The same VRRP policy can be applied to both IPv4 VRRP instances and IPv6 VRRP instances.

- Click on the Select button in the Policy panel. The Select VRRP Policy form opens.
- Choose a VRRP policy and click on the OK button. The Select VRRP Policy form closes and the VRRP Instance (Create) form reappears with the VRRP policy information displayed.

11 Click on the Behavior tab button.

12 Configure the parameters:

- MAC Address
- Message Interval (seconds)
- Message Interval (milliseconds)
- Init Delay (seconds)
- Master Inherit Interval
- Ping Reply
- Telnet Reply
- Standby Forwarding
- Preempt Mode
- SSH Reply
- Traceroute Reply

13 Click on the Authentication tab button.

Note — The Authentication Key is not supported for Release 7.0 R1 VRRP IPv6 Instances. If you are creating an VRRP IPv6 Instance on a Release 7.0 R1 NE, the Authentication tab does not appear.

14 Configure the parameters:

- Type
- Key

15 Click on the Backup Addresses tab button.

16 Click on the Add button. The Backup Address (Create) form opens.

17 Perform one of the following to configure backup addresses:

a Enter an IPv4 address (for an IPv4 VR) or IPv6 address (for an IPv6 VR) manually in the IP Address field in the Backup Address section.

b Select the IP address from a list:

i Click the Choose IP Address button adjacent to the IP Address field. The Select IP Address form opens.

ii Click on the Search button.

iii Choose the desired entry from the list.

iv Click on OK.

The Select IP Address form closes and the IP Address parameter is populated with your selection.

v Click on the Add Link Local Address button. The Admin Link Local Address defined for the network L3 access interface appears in the IP Address field.

Note — If you need to add the Link Local Address as a backup address, then the Admin Link Local Address must be configured and the Admin Link Local Address Preferred parameter must be enabled for the network L3 access interface that you are using. See Procedure 27-4 for more information.

18 Click on OK to save your changes and close the Backup Address (Create) form.

19 Click on the OK button. The Virtual Router (Edit) form reappears with the VRRP instances displayed in the VR instances tree.

Procedure 36-3 To add a VRRP instance

A VRRP instance that you add to the VR must have an IP address with the same VRID and subnet as those of the VR.

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on VR Instances and choose Add VRRP Instance.

Note — If you chose an IPv6 VR in step 3, the contextual menu item is Add VRRP IPv6 Instance, and the Select VRRP IPv6 Instance form opens.

The Select VRRP Instance form opens with a list of eligible instances.

6 Select an instance and click on the OK button. The Select VRRP Instance (or Select VRRP IPv6 Instance) form closes and the Virtual Router (Edit) form reappears with the interface information displayed.

Procedure 36-4 To modify a VR or VRRP instance

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Configure the VR parameters.

To configure parameters for a VRRP instance, click on the Components tab, select and right-click on the VRRP instance, and choose Properties from the contextual menu. Using the contextual menu, you can also:

- Configure the NE associated with the VRRP instance
- Configure the interface associated with the VRRP instance

5 Click on the Properties button in the Instance panel. The VRRP Instance (Edit) form opens with the General tab displayed.

6 The following tabs list the VRRP instance properties that you can select and configure:

- General—associations between the VRRP instance and NEs, network interfaces, and policies (non-owner VRRP instances only).
- Behavior—a virtual MAC address that must be the same for all participating VRRP instances
- Authentication—enables authentication of VRRP advertisements among participating VRRP instances in the VR. For more information, see "VRRP message authentication" in section 36.1.

Note — Authentication is not supported for Release 7.0 R1 VRRP IPv6 Instances. When you modify a Release 7.0 R1 VRRP IPv6 Instance, the Authentication tab is not displayed.

- Backup Addresses—lists backup addresses, whose configuration options you can access by selecting a site and clicking on the Properties button. For more information, see "Backup addresses" in section 36.1.
- VR Instances—lists VRs, whose configuration options you can access by selecting a VR and clicking on the Properties button. For more information, see "Owner and non-owner VRRP instances" in section 36.1.

7 Modify the parameters for the VRRP instance as required.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button to confirm the action. The VRRP Instance (Edit) form closes and the VR Instance (Edit) form reappears.

10 Click on the Close button to close the VR Instance (Edit) form.

Procedure 36-5 To view the status of a VR

The status of a VR informs you of potential problems, such as problems involving VR preconditions and operational states. You can view the following virtual status information:

- Aggregated Operational State—indicates the collective operational states of the VRRP instances in the VR, such as whether all instances are up, all instances are down, or one or more is down
- Number Of VRRP Instances—the number of owner and non-owner VRRP instances in the current VR
- Multiple Owners configured—one owner for each VR
- VR Instance(s) Down—one or more VRs are not working
- Backup Address Mismatch—the backup address for a VRRP instance does not match the primary IP address of the owner, and so does not match the VR IP address
- Only one instance configured—only one VR instance exists, either a master or backup; both are required

- Subnet Mismatch—the IP addresses of the owner and non-owner routers do not belong to the same subnet
- No Owner configured—an IP address owner is not assigned to the current VR

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed. Status information is in the Status panel.

4 Click on the Close button to close the Virtual Router (Edit) form.

Procedure 36-6 To delete a VRRP instance

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR and click on the Properties button. The Virtual Router (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Select and right-click on a VR instance and choose Delete from the contextual menu. A dialog box appears.

6 Click on the Yes button to confirm the action. The VR is deleted and removed from the VR instances tree.

7 Click on the Close button to close the Virtual Router (Edit) form.

Procedure 36-7 To delete a VR

1 Choose Manage→Networking→VRRP Virtual Routers from the 5620 SAM main menu. The Manage VRRP Virtual Routers form opens.

2 Configure the filter criteria. A list of VRs is displayed at the bottom of the Manage VRRP Virtual Routers form.

3 Choose a VR from the list.

4 Click on the Delete button. A dialog box appears.

5 Click on the Yes button to confirm the action. The VR is removed from the list.

6 Click on the Close button to close the Manage VRRP Virtual Routers form.

37 — APS

37.1 APS overview

APS protects SONET/SDH lines from linear bidirectional failures. The NEs in a SONET/SDH network constantly monitor the health of the network. When a failure is detected, the network proceeds to transfer, or switch over, live traffic from the active, or working line, to the standby, or protection line. The transfer occurs quickly to minimize traffic loss. The traffic remains on the protection line until the fault on the working line clears, at which time the traffic can optionally revert to the working line.

In a 1+1 APS architecture, the active OC-*n* signal is transmitted to both the working and protection ports, so the same payloads are transmitted identically to the working and protection ports in the egress direction. The working and protection signals are selected independently in the ingress direction.

Caution — An NE transmits data only on the working line. For a single failure, this configuration can cause a delay of up to 100 ms during an APS switch.

In the 5620 SAM, the main APS elements are the following:

- APS groups

  An APS group is an aggregation of one or two SONET/SDH ports and the associated logical ports, known as APS channels. The first port is known as the working channel and must be configured in the APS group. The second port is the protection channel, which is optionally configurable.
- APS channels

  APS channels are logical and model the physical ports. The set of associated data for an APS channel includes the corresponding physical port identifier, the role, which is working or protection, and the name of the APS group to which the port belongs. If a protection channel is configured, it carries the traffic of the failed working channel. If the protection channel fails, the working channel carries the traffic.
- APS bundles

  APS bundles protect multilink PPP and IMA bundles on channelized ASAP MDAs. All the members of a working or protection APS bundle must belong to the same working or protection line of the APS group.
- APS common port configurations

  All SONET/SDH port parameters on the working and protection channels in an APS group must be identical except for the following:
  - Clock Source
  - Loopback
  - Report Alarms
  - BER Signal Degradation Threshold
  - BER Signal Failure Threshold
  - SONET Section Trace Mode

- APS commands
  Each APS channel has one APS operational command associated with it. The APS operational command is determined by the last command that is issued to both APS channels and the signal condition of the working and protection ports. APS commands affect the APS operational states but do not affect the configuration. The operational state does not persist through an NE restart.

Table 37-1 describes the events that affect 1+1 protection and their relative priority.

Table 37-1 Events affecting 1+1 protection

Priority	Event	Event type
1	Lockout of protection	User initiated
2	Signal failure on protection line	Automatically initiated
3	Forced switch	User initiated
4	Signal failure on working line	Automatically initiated
5	Signal degradation	Automatically initiated
6	Manual switch	User initiated
7	WTR time (revertive switching only)	User initiated (state request)
8	No reversion (non-revertive switching only)	User initiated (state request)

Consider the following when configuring APS.

- A port can belong to only one APS group.
- Two ports that belong to the same APS group must be of the same port type and have the same traffic speed.
- An APS group has one set of APS channels. The set can contain one or two APS channels.
- An APS channel can belong to only one APS group.
- A SONET/SDH port can either belong to only one APS channel.

Bidirectional mode

In 1+1 system bidirectional mode, a signal failure in either direction causes both the near-end and far-end NEs to switch to the protection channels. The highest-priority local request is compared with a remote request; the request that has the greater priority is selected. See Table 37-1 for the list of events that affect 1+1 protection.

Unidirectional mode

In a 1+1 system unidirectional mode, the working interface switches to the protection interface only for the direction in which a signal failure occurs. For example, if there is a signal failure in the transmit direction, the working interface switches to the protection interface for transmission but not for the receipt of data.

Switching modes

The following 1+1 system switching modes are available:

- non-revertive (default)
- revertive

In non-revertive switching, a switch to the protection channel is maintained even after the working line has recovered from a failure or a manual switch is cleared.

In revertive switching, the traffic is switched back to the working channel after the working line has recovered from a failure or a manual switch is cleared.

For revertive switching, you can define a period of time that the system must wait before it can restore traffic from the protection line to the working line. This delay, or WTR time, prevents frequent automatic switches from occurring as a result of intermittent failures.

In case of failure on both the working and protection lines, the line that has the less severe error remains active. If there is a signal degradation on both lines, the active line that failed last remains active. If there is a signal failure on both lines, the working line always remains active because a signal failure on the protection line is a higher priority than a signal failure on the working line.

MLPPP

MLPPP provides a way to distribute data across multiple links within an MLPPP APS bundle to achieve high bandwidth. MLPPP allows for a single frame to be fragmented and transmitted across multiple links. This reduces latency and allows for a higher maximum received recovery unit, or MRU.

MLPPP is supported in MC APS groups. See section "MC APS" for more information about MC APS.

Multiclass MLPPP

Multiclass MLPPP is an extension of the MLPPP standard which allows multiple classes of service to be transmitted over an MLPPP bundle.

Multiclass MLPPP changes the MLPPP header to include either two or four class bits to allow for up to either four or 16 classes of service. This allows multiple classes of services over a single MLPPP connection. The highest priority traffic is transmitted over the MLPPP bundle with minimal delay, regardless of the order in which packets are received.

Multiclass MLPPP is useful in mobile network deployments where multiple types of traffic, each with its own priority level, travel across a single MLPPP link bundle between the base station router and the aggregation router in the point of presence (POP) mobile operator.

Note — Multiclass MLPPP allows for several classes of services to be transmitted over an MLPPP bundle. Link fragmentation and interleaving, however, allows for only two classes of service to be transmitted. Multiclass MLPPP and link fragmentation and interleaving are mutually exclusive.

APS port configurations

A 7710 SR or 7750 SR network or access port can be connected to another 7710 SR or 7750 SR with both the working and protection channels on different IOMs in a single NE, or with the working channel on one NE and the protection channel on another.

Note — Mirroring parameters configured on a specific port or service are maintained during an APS failover.

All SONET/SDH MDAs support APS functionality. Table 37-2 lists the possible port pairings to provide APS protection. Both ports must be of the same type and have the same traffic speed.

Table 37-2 APS port configurations

MDA type—Working channel	MDA type—Protection channel
16 × OC12/OC3 SFP	8 × OC12/OC3 SFP or 16 × OC12/OC3 SFP
8 × OC12/OC3 SFP	8 × OC12/OC3 SFP or 16 × OC12/OC3 SFP
16 × OC3 SFP	8 × OC3 SFP or 16 × OC3 SFP
8 × OC3 SFP	8 × OC3 SFP or 16 × OC3 SFP
4 × OC48 SFP	2 × OC48 SFP or 4 × OC48 SFP
2 × OC48 SFP	2 × OC48 SFP or 4 × OC48 SFP
1 × OC192	1 × OC192
16 × ATM OC3 SFP	16 × ATM OC3 SFP
4 × ATM OC12/OC3 SFP	4 × ATM OC12/OC3 SFP
4 × Channelized OC3 ASAP	4 × Channelized OC3 ASAP
1 × Channelized OC12 ASAP	1 × Channelized OC12 ASAP
1 × Channelized OC3 CES	4 × Channelized OC3 CES
4 × Channelized OC3 CES	1 × Channelized OC3 CES
1 × Channelized OC12 CES	1 × Channelized OC12 CES

Note — The working and protection channels for the following MDA port pairs are set to the same traffic speed based on the APS group speed configuration:

- 16 × OC12/OC3 SFP and 16 × OC12/OC3 SFP
- 16 × OC12/OC3 SFP and 8 × OC12/OC3 SFP
- 8 × OC12/OC3 SFP and 16 × OC12/OC3 SFP
- 8 × OC12/OC3 SFP and 8 × OC12/OC3 SFP
- 4 × ATM OC12/OC3 SFP and 4 × ATM OC12/OC3 SFP

SC APS

1+1 APS can be implemented on a port-by-port basis. If all ports on an MDA or IOM need to be protected, the ports must be individually configured.

The working and protection lines are capable of being connected to:

- two ports on the same MDA
- two ports on different MDAs, and the MDAs are on the same IOM
- two ports on different MDAs on different IOMs

If the working channel and protection channel are on the same MDA, protection is limited to the physical port and the media that connect the two NEs. If different IOMs are used, protection extends to failure of each IOM.

Working and protection lines can be connected to a 7450 ESS, 7710 SR, or 7750 SR, and serve as an access port that provides one or more services to the NE. The access port can be a single channel or multiple channels; each channel must support PPP. In the case of the ATM MDA, each channel must support ATM.

The end NE transmits a valid data signal to both the working and protection lines. The signal on the protection line is ignored until the working channel fails or degrades to the degree that requires a switchover to the protection channel. When the switchover occurs, all services, including all service QoS and filter policies, are activated on the protection channel.

The working channel on a 7750 SR, 7450 ESS, or 7710 SR must connect to the working channel on a peer NE, and the protection channel on a 7750 SR, 7450 ESS, or 7710 SR must connect to the protection channel on a peer NE.

MC APS

You can use APS to protect against NE failure by configuring the working channel of an APS group on one 7750 SR or 7710 SR, and configuring the protection channel of the same APS group on a different 7750 SR or 7710 SR. The two NEs connect using an IP link that is used to establish a signaling path between them.

The working channel on the near-end NE must connect to the working channel on a peer NE, and the protection channel on the far-end NE must connect to the protection channel on a peer NE.

When an MC APS group is configured, the 5620 SAM automatically creates a container which aggregates the MC APS group configurations of each NE.

Multi-chassis APS configuration is supported for ATM clear channel interfaces.

APS on channelized ASAP MDAs

You can protect a channelized SONET/SDH port on a channelized ASAP MDA with a protection port of the same speed on a different channelized ASAP MDA in the same NE. The APS configuration on a channelized ASAP MDA provides protection against a port, MDA, or IOM failure. All SONET/SDH paths and TDM channels in a SONET/SDH port are protected.

Consider the following when you configure APS protection on a deep channel on a channelized ASAP MDA:

- Both SONET and SDH channels are supported.
- Up to three common configuration SONET channels can be created in an APS configuration.

APS on channelized CES MDAs

You can protect a channelized SONET/SDH port on a channelized CES MDA with a protection port of the same speed on a different channelized CES MDA in the same NE. The APS configuration on a channelized CES MDA provides protection against a port, MDA, or IOM failure. All SONET/SDH paths and TDM channels in a SONET/SDH port are protected.

Consider the following when you configure APS protection on a deep channel on a channelized CES MDA:

- Both SONET and SDH channels are supported.
- Up to three common configuration SONET channels can be created in an APS configuration.

APS on multilink bundles

APS on multilink bundles consists of a working and protection bundle which provide bidirectional APS protection to each other. The members of a working or protection multilink bundle must belong to the same working or protection line of the APS group. User traffic is not sent on the protection line.

The 5620 SAM supports APS on MLPPP and IMA bundles. In IMA bundles, IMA cells are sent on the protection line as a keep-alive signal during an APS switchover.

APS 1+1 configuration on the channelized MDA provides protection to all the channels on the protected SONET/SDH port and to all of the multilink bundles with member that links reside on the protected SONET/ SDH port.

APS bundles on multiple NEs

You can configure APS bundles to provide bidirectional APS protection across multiple NEs. MC APS bundles are supported on the 7750 SR and 7710 SR, Release 6.0 or later.

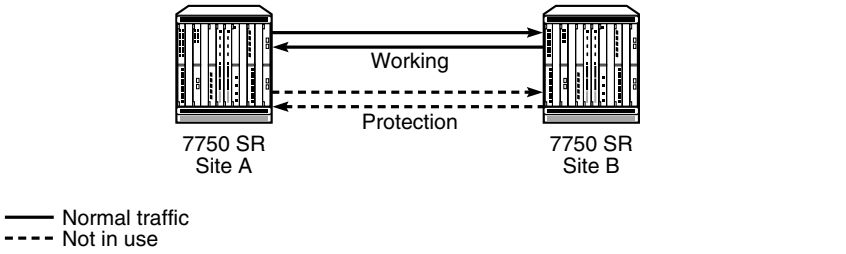
You can use APS to protect against failure by configuring the working bundle on one NE, and configuring the protection bundle of the same APS bundle group on a different NE. The two NEs connect to each other with an IP link that is used to establish a signaling path between them.

1+1 APS configuration example

Figures 37-1 and 37-4 show an example of 1+1 APS for two 7750 SRs that are configured for 1+1 APS in bidirectional and non-revertive modes.

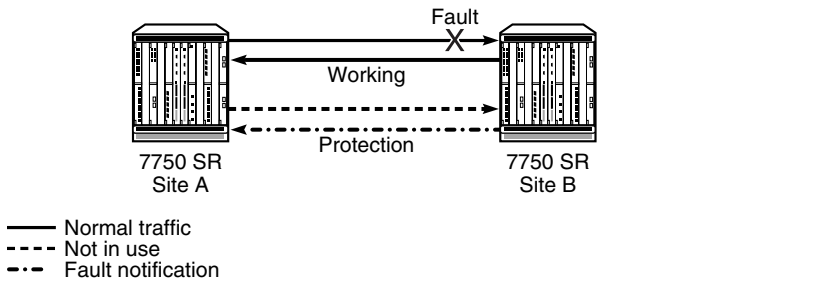
Figure 37-1 shows normal operations between two 7750 SRs. There are no faults on the working line, and the protection line is not in use.

Figure 37-1 Normal operations between two 7750 SRs



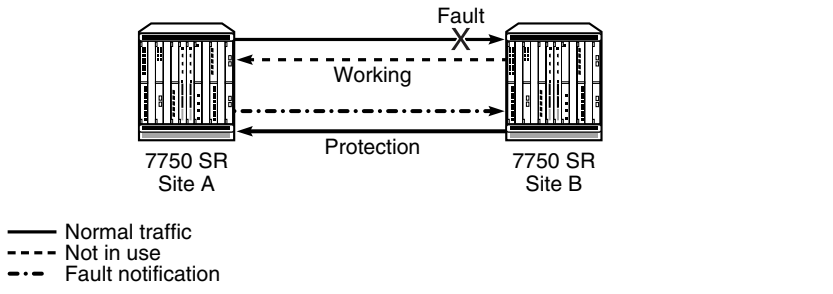
The working line degrades in the direction from site A to site B. Site B detects the fault and notifies site A of the fault using the protection line. Figure 37-2 shows the fault on the working line and site B notifying site A of the fault.

Figure 37-2 Site B detects the fault and notifies site A



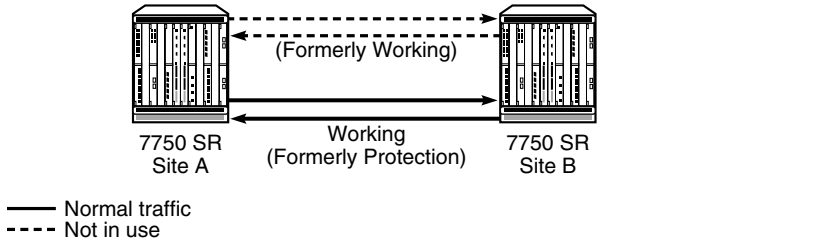
Site B automatically switches to the protection line. Site A receives the fault notification from site B and detects the fault on the working line. Site A acknowledges the fault and notifies site B that it is switching to the protection line. Figure 37-3 shows site B switching to the protection line and site A acknowledging the fault.

Figure 37-3 Site B switches to the protection line and site A acknowledges the fault



Site B receives the notification from site A and site A automatically switches to the protection line. Figure 37-4 shows normal operations resuming on the protection line between site A and site B. The protection line becomes and remains the working line since 1+1 APS is configured for non-revertive switching in this example.

Figure 37-4 Normal operations resume on the protection line



Configuring SAPs on APS-protected ports

You can use APS-protected ports to create SAPs for 5620 SAM services. The SAP list of a service creation form displays the APS-group SONET channels with all other SONET channels, but uses a different port ID format. An example of an APS group port ID is Channel aps-1.sts3-1. To create a SAP that uses an APS group, you must first configure the SONET channels in the APS group.

37.2 Workflow to manage APS

1 Create APS.

- **a** Create a 1+1 APS configuration on SONET/SDH ports as required.
- **b** Perform one of the following APS commands for each APS channel as required.
  - **i** Use the Lockout of Protection command to prevent any working channels from switching to the protection line.
  - **ii** Use the Forced Switch of Working to Protection command to force a high-priority switch of the specified working channel to the protection line.
  - **iii** Use the Forced Switch of Protection to Working command to force a high-priority switch of the specified working channel back from the protection line to the working line.
  - **iv** Use the Manual Switch of Working to Protection command to manually switch the specified working channel to the protection line.
  - **v** Use the Manual Switch of Protection to Working command to manually switch the specified working channel back from the protection line to the working line.

vi Use the Exercise command in the bidirectional mode to exercise the protocol for a protection switch of the specified working channel by issuing a request for that channel and checking the response on the APS channel.

vii Use the Clear command to clear the switch commands for the specified channel.

2 Remove a 1+1 APS configuration as required.

37.3 APS management procedures

Use the following procedures to perform APS management tasks.

Procedure 37-1 To create an SC APS group using SONET/SDH ports

Note — When a multiservice site is configured on an IOM, the working and protection ports must be configured on the same IOM.

1 Locate and expand the shelf object for which you want to configure APS in the Equipment view of the 5620 SAM navigation tree. The APS Groups object is displayed below the shelf object.

2 Right-click on the APS Groups object and choose Create APS Group from the contextual menu. The SC APS Group (Create) form opens with the General tab displayed.

3 Configure the Description parameter.

4 Click on the APS Group tab button.

5 Configure the parameters:

- Auto-Assign ID
- Group Number
- Direction
- Revertion Mode
- Wait To Restore (seconds)

6 Click on the States tab button.

7 Configure the Administrative State parameter.

Note — When a working channel or protection channel is added to an APS group, the channel inherits the current administrative state of the APS group. After the channel is added to the APS group, the administrative state of the physical port can be changed independently.

8 Click on the Apply button. An SC APS Group icon appears under the APS Groups object in the navigation tree.

9 Click on the APS Group tab button.

10 Configure the parameters:

- Direction
- Revertion Mode
- Wait To Restore (seconds)
- Hold Time for Line Signal Degradation
- Hold Time for Line Signal Failure
- RDI Alarm Generation

11 Perform the following steps to configure the working and protection channels.

i Click on the APS Channels tab button.

ii Click on the Add button. The APS Channel (Create) form opens.

iii Set the Channel Role parameter to Working.

Note — You must create the working channel before you create the protection channel.

iv Click on the Select button. The Select Port - APS Channel form opens.

v Click on the Search button. A list of available ports is displayed.

vi Select a port in the list and click on the OK button. The Select Port - APS Channel form closes.

vii Click on the OK button. The APS Channel (Create) form closes and a dialog box appears.

viii Click on the OK button. The channel is listed on the SC APS Group (Edit) form.

ix Click on the Add button. The APS Channel (Create) form opens.

x Set the Channel Role parameter to Protection.

xi Repeat steps iv to viii to add the protection channel.

xii Click on the Apply button.

12 Configure the operational state of the working and protection channels. Perform the following steps:

i Choose a channel from the list and click on the Properties button. The APS Channel - *Type* (Edit) form opens with the APS Channel tab displayed.

ii Configure the Command Switch parameter.

iii Click on the OK button. The APS Channel - *Type* (Edit) form closes.

13 Configure the APS common configuration parameters for the working and protection channels. Perform the following steps:

i Right-click on the SC APS Group icon in the navigation tree and choose Create APS SONET Channel from the contextual menu. The Sts*n* SONET Channel (Create) form opens with the General tab displayed.

ii Configure the channel as described in chapter 17.

Procedure 37-2 To create an MC APS group using SONET/SDH ports

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC APS Group (APS) from the object drop-down list.

3 Click on the Create button. The MC APS Group (Create) form opens.

4 Configure the Group Number parameter.

5 Click on the Select button to configure the Site Id parameter in the First Element panel. The Select a Network Element list form opens.

6 Select an NE and click on the OK button. The Select a Network Element list form closes and the MC APS Group (Edit) form displays the system ID of the first NE in the MC APS group.

7 Click on the Select button to configure the Network Interface parameter in the First Element panel, if required. The Select a Network Element list form opens.

Note 1 — Only numbered IPv4 interfaces are listed.

Note 2 — The default interface is the NE system interface.

8 Click on the Select button to configure the Site Id parameter in the Second Element panel. The Select a Network Element list form opens.

9 Select an NE and click on the OK button. The Select a Network Element list form closes and the MC APS Group (Edit) form displays the system ID of the second NE in the MC APS group.

10 Click on the Select button to configure the Network Interface parameter in the Second Element panel, if required. The Select a Network Element list form opens.

Note 1 — Only numbered IPv4 interfaces are listed.

Note 2 — The default interface is the NE system interface.

11 Click on the Apply button. An MC APS Group Member icon appears under the APS Groups object in the navigation tree of the selected First Element and Second Element NEs.

12 Click on the Members tab button to configure each MC APS group member.

13 Select a group member in the list and click on the Properties button. The MC APS Group Member (Edit) form opens with the General tab displayed.

14 Configure the Description parameter.

15 Click on the APS Group tab button.

16 Configure the parameters:

- Revertion Mode
- Wait To Restore (seconds)

Note — The Wait To Restore (seconds) parameter is configurable when the Revertion Mode parameter is set to revertive.

17 Click on the States tab button.

18 Configure the Administrative State parameter.

Note — When a working channel or protection channel is added to the APS group, the channel inherits the current administrative state of the APS group. After the channel is added to the APS group, the administrative state of the physical port can be changed independently.

19 Click on the Multi Chassis tab button.

20 Configure the parameters:

- Advertise Interval (100s of milliseconds)
- Hold Time (100s of milliseconds)

21 Perform the following steps to configure an APS channel on the NE.

i Click on the APS Channels tab button.

ii Click on the Add button. The APS Channel (Create) form opens.

iii Configure the Channel Role parameter. If you have already created a working channel on the other MC APS group member, set this parameter to Protection. Otherwise, set this parameter to Working.

iv Click on the Select button. The Select Port - APS Channel form opens.

v Click on the Search button.

vi Select a port in the list and click on the OK button. The Select Port - APS Channel form closes.

vii Click on the OK button. The APS Channel (Create) form closes and a dialog box appears.

viii Click on the OK button. The channel is listed on the form.

ix Click on the Apply button.

x Select the channel and click on the Properties button. The APS Channel - *Role* (Edit) form opens with the APS Channel tab displayed.

xi Configure the Command Switch parameter.

xii Click on the OK button. The APS Channel - *Role* (Edit) form closes.

xiii Click on the OK button. A dialog box appears.

xiv Click on the Yes button. The MC APS Group Member (Edit) form closes.

22 Repeat steps 13 to 21 to configure an APS channel on the other NE in the MC APS group.

23 Click on the OK button. The MC APS Group (Edit) form closes.

24 Close the Manage Node Redundancy form.

25 Perform the following steps to configure the MC APS parameters that are common to the working and protection channels.

i Right-click on the MC APS Group Member icon in the navigation tree and choose Create APS SONET Channel from the right-click contextual menu. The Sts*n* SONET Channel (Create) form opens with the General tab displayed.

ii Configure the SONET or SDH channels, as described in chapter 17.

Procedure 37-3 To create an SC APS IMA or MLPPP bundle

Perform this procedure to create an APS bundle using IMA or MLPPP links on one NE. Consider the following when you add a DS0 channel that is a member of an APS group to an APS bundle:

- An APS channel can be a member of an APS bundle only, not of an IMA or multilink PPP bundle.
- All members of a working bundle must belong to a working channel of the same APS group.
- All members of a protection bundle must belong to a protection channel of the same APS group.

- You must create the working bundle before you can add an APS member to the APS bundle. If the member has a protection port, you must create the protection bundle before you can add the member to the APS bundle.
- You cannot delete the working port member of an APS bundle until you remove the member from the APS bundle.

The rules for adding a member to a bundle that is part of an APS bundle also apply to adding a member to a non-APS protected multilink bundle. See Procedures 17-98 and 17-99 for more information.

The following restrictions apply when adding a DS0 channel to an IMA bundle:

- The Clock Source parameter must be set to Node Timed.
- The encapsulation type of the DS0 channel must be ATM.

The following restrictions apply when adding a DS0 channel to a PPP bundle:

- All time slots on the DS0 channel must be selected.
- The encapsulation type of the DS0 channel must be IPCP.

1 Locate and expand the shelf object for which you want to configure an APS bundle in the Equipment view of the 5620 SAM navigation tree. The APS Bundles object is displayed below the shelf object.

2 Right-click on the APS Bundles object and choose Create Bundle from the contextual menu. The APS Bundle Display form opens.

3 Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description

4 Click on the Next button.

5 Configure the parameters:

- Bundle Type

a If you set the Bundle Type parameter to IMA Group, configure the following parameters:

- Red Diff Delay (milliseconds)
- Minimum Links
- IMA Version
- ATM Interface Cell Format
- ATM Minimum VPI Value
- Test Pattern
- Link Activation Timer
- Link Deactivation Timer
- Maximum Links

b If you set the Bundle Type parameter to PPP, configure the following parameters:

- Fragment Threshold (bytes)
- Red Diff Delay (milliseconds)
- Red Diff Delay Action
- Minimum Links
- Yellow Diff Delay (milliseconds)
- Bundle MRRU (bytes)
- Short Sequence
- Link Fragmentation and Interleaving

6 Click on the Finish button.

7 Click on the Close button. The APS Bundle Display form closes.

8 If the Bundle Type parameter is set to PPP in step 5, perform the following steps to configure the MLPPP bundle for multiclass service transmission.

Note — Consider the following when you configure MC MLPPP.

- MC MLPPP is supported only on channelized ASAP MDAs on the 7750 SR and 7710 SR, Release 6.0 or later.
- You must configure MC MLPPP before you add bundle members.
- MC MLPPP is configured on the main APS bundle and the parameters are propagated to the working and protection bundles.

i Right-click on the SC APS Bundle object in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the MLPPP tab button.

iii Configure the parameters:

- End Point ID
- End Point Class ID
- Class Count
- Magic Number

iv Click on the Select button in the MLPPP Ingress QoS Profile or MLPPP Egress QoS Profile panel to choose a QoS profile, if required. If a profile is already selected, click on the Clear button to clear the selection and enable the Select button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form opens.

Note — You can only apply QoS profiles to an MC MLPPP bundle when the Class Count parameter is set to 4.

v Select a profile and click on the OK button. The Select MLPPP Ingress QoS Profile or Select MLPPP Egress QoS Profile form closes.

9 Click on the States tab button.

10 Configure the Administrative State parameter.

Note — You must configure the End Point ID parameter on the APS PPP group before you set the Administrative State parameter to Up on the working and protection bundles.

11 Click on the OK button. A dialog box appears.

12 Click on the Yes button. The APS Bundles (Edit) form closes.

13 To configure the APS working and protection bundles, perform the following steps.

Note — You must create the working bundle before you create the protection bundle.

i Right-click on the SC APS Bundle icon in the navigation tree and choose Create APS Working Bundle from the contextual menu. The Create APS Working/Protecting Bundle form opens.

ii Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description
- Daughter Card CLI Name
- Administrative State

iii Click on the Next button to view the configured bundle parameters.

iv Click on the Finish button.

v Click on the Close button. The Create APS Working/Protecting Bundle form closes.

vi Right-click on the SC APS Bundle icon in the navigation tree and choose Create APS Protection Bundle from the contextual menu. The Create Working/Protecting Bundle form opens.

vii Repeat steps ii to v to create the APS protection bundle.

14 To configure the administrative state of the APS working and protection bundles, perform the following steps.

Note — You must configure the End Point ID parameter on the APS PPP group before you change the working or protection bundle state.

i Right-click on the working bundle object below the SC APS Bundle object in the navigation tree and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

ii Click on the States tab button.

iii Configure the Administrative State parameter.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button. The Multilink Bundle (Edit) form closes.

vi Right-click on the protection bundle object below the SC APS Bundle object in the navigation tree. and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

vii Repeat steps ii to v.

15 To add members to the APS bundle, perform the following steps.

i Right-click on the SC APS Bundle icon in the navigation tree and choose Create Bundle Members from the contextual menu. The Add Bundle Member form opens.

ii Click on the Next button to add DS0 channel groups to the bundle. The Select Channels form opens.

iii Select a compatible channel from the list.

Note 1 — When initially adding bundle members, you must first add one channel group and then repeat the procedure to select up to seven additional channel groups.

Note 2 — Only compatible channels are listed. If you want to configure and use a channel that is currently incompatible, you can click on the Back button, deselect the Show Only Compatible Channels parameter, click on the Next button, select the channel, click on the Properties button.

Note 3 — The channel group with the lowest Port ID is the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member Encap Type for the member to be compatible.

iv Click on the Finish button and confirm the action. The Add Bundle Member form closes.

v Click on the Apply button.

vi Click on the Add button. The Add Bundle Member form opens.

vii Configure the Show Only Compatible Channels parameter.

viii Click on the Next button. The Select Channels form opens.

ix Select up to seven additional channels from the list.

x Click on the Finish button. A dialog box appears.

xi Click on the Yes button. The Add Bundle Members form closes.

xii Click on the Finish button.

xiii Click on the Close button. The Add Bundle Member form closes.

Procedure 37-4 To create an MC APS MLPPP bundle

Perform this procedure to create an APS bundle using IMA or MLPPP links on two NEs.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC APS Bundles (Bundle) from the object drop-down list.

3 Click on the Create button. The MC APS Bundles (Create) form opens.

4 Configure the Bundle Number parameter.

5 Click on the Select button beside the First Network Element parameter. The Select a Network Element list form opens.

6 Select an NE in the list and click on the OK button. The Select a Network Element list form closes.

7 Click on the Select button beside the Second Network Element parameter. The Select a Network Element list form opens.

8 Select an NE in the list and click on the OK button. The Select a Network Element form closes.

9 Click on the OK button. An MC APS Bundle object appears in the navigation tree under the APS Bundles object of each specified NE.

10 Close the Manage Node Redundancy form.

11 Configure the MLPPP bundle for multiclass service transmission. Perform the following steps.

Note — Consider the following when you configure MC MLPPP.

- You must configure MC MLPPP before you add bundle members.
- MC MLPPP is configured on the main APS bundle and the parameters are propagated to the working and protection bundles.

i Right-click on the new MC APS Bundle object in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the MLPPP tab button.

iii Configure the parameters:

- End Point ID
- End Point Class ID
- Class Count
- Magic Number

iv Click on the Apply button. A dialog box appears.

v Click on the Yes button.

12 Click on the States tab button.

13 Configure the Administrative State parameter.

Note — You must configure the End Point ID parameter on the APS PPP group before you set the Administrative State parameter to Up on the working and protection bundles.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The APS Bundles (Edit) form closes.

16 Perform the following steps to configure the MC APS working and protection bundles.

i Right-click on the MC APS Bundle object created in step 6 in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the Protection and Working Bundles tab button.

iii Click on the Add button. The Create APS Working/Protecting Bundle form opens.

iv Configure the parameters:

- Bundle ID
- Auto-Assign ID
- Description
- Administrative State

v Click on the Select button beside the Daughter Card CLI Name parameter. The Select Daughter Card - Multilink Bundle list form opens.

vi Select a daughter card in the list and click on the OK button. The Select Daughter Card - Multilink Bundle list form closes.

vii Click on the Next button.

viii Configure the parameters.

- Bundle Type
- Protection Type

  The working bundle must be on the same NE as the APS working channel and the protection bundle must but on the same NE as the APS protection channel.

ix Click on the Finish button.

x Click on the Close button. The Create APS Working/Protecting Bundle form closes.

xi Close the APS Bundles (Edit) form.

xii Repeat steps i to xi to configure the MC APS protection bundle created in step 8.

17 Perform the following steps to configure the administrative state of the MC APS working and protection bundles.

i Right-click on the working bundle object in the navigation tree and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

ii Click on the States tab button.

iii Configure the Administrative State parameter.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button. The Multilink Bundle (Edit) form closes.

vi Right-click on the protection bundle object in the navigation tree and choose Properties from the contextual menu. The Multilink Bundle (Edit) form opens.

vii Repeat steps ii to v.

18 To add multilink bundle members, perform the following steps.

i Right-click on the MC APS Bundle object on either NE in the navigation tree and choose Properties from the contextual menu. The APS Bundles (Edit) form opens.

ii Click on the Bundle Members tab button.

iii Click on the Add button. The Add Bundle Member form opens.

iv Configure the Show Only Compatible Channels parameter.

v Click on the Next button. The Select Channels form opens.

vi Select a channel in the list.

Note 1 — When initially adding bundle members, you must first add one channel group and then repeat the procedure to select up to seven additional channel groups.

Note 2 — Only compatible channels are listed. If you want to configure and use a channel that is currently incompatible, you can click on the Back button, deselect the Show Only Compatible Channels parameter, click on the Next button, select the channel, click on the Properties button.

Note 3 — The channel group with the lowest Port ID is the primary member for the bundle. The Encap Type of the primary member is used for all other members. When adding members to a bundle at a later time, the Encap Type must be the same as the primary member Encap Type for the member to be compatible.

vii Click on the Finish button. A dialog box appears.

viii Click on the Yes button. The Add Bundle Members form closes.

ix Click on the Apply button.

x Click on the Add button. The Add Bundle Member form opens.

xi Configure the Show Only Compatible Channels parameter.

xii Click on the Next button. The Select Channels form opens.

xiii Select up to seven additional channels from the list.

xiv Click on the Finish button A dialog box appears.

xv Click on the Yes button. The Add Bundle Members form closes.

xvi Click on the OK button. The APS Bundles (Edit) form closes.

Procedure 37-5 To change the operational state of an SC APS channel

1 Right-click on the APS Channel object in the Equipment view of the 5620 SAM navigation tree and choose Properties from the contextual menu. The APS Channel (Edit) form opens.

2 Configure the Command Switch parameter.

3 Click on the OK button. A dialog box appears.

4 Click on the Yes button. The operational state of the APS channel changes and the APS Channel (Edit) form closes.

Procedure 37-6 To delete an SC APS group

1 Right-click on the APS Group object in the Equipment view of the navigation tree and choose Delete from the contextual menu. A dialog box appears.

Caution — Removing an APS group removes the working and protection channels and associated ports from the APS group, and deletes the APS group ID. Ensure that you select the correct APS group.

2 Click on the View Dependencies button. A dialog box appears.

3 Click on the OK button.

4 Select the I understand the implications of this action check box.

5 Click on the Yes button. The 5620 SAM deletes the SC APS group.

Procedure 37-7 To delete an SC APS bundle

Perform this procedure to permanently remove an SC APS bundle from the 5620 SAM and NE configurations.

1 Right-click on the APS Bundle object in the Equipment view of the navigation tree and choose Delete from the contextual menu. A dialog box appears.

2 Click on the View Dependencies button. A dialog box appears.

3 Click on the OK button to proceed.

4 Select the I understand the implications of this action check box.

5 Click on the Yes button. The 5620 SAM deletes the SC APS bundle.

Procedure 37-8 To delete an MC APS group or bundle

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Perform one of the following.

   a Choose MC APS Group (APS) from the object drop-down list.

   b Choose MC APS Bundles (APS) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC APS groups or MC APS bundles appears.

4 Select an entry in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. A dialog box appears.

6 View the dependency information.

7 Click on the OK button.

8 Select the I understand the implications of this action check box.

9 Click on the Yes button. The 5620 SAM deletes the MC APS group or bundle and the corresponding configuration on each member site.

38 — MC peer groups

38.1 MC peer groups overview

An MC peer group is a 5620 SAM object that defines the relationship between two peer NEs to provide system redundancy in an Ethernet network. An MC peer group configuration includes a list of protocols and objects with state information that is to be synchronized between the peers.

The 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, 7710 SR, and 7750 SR each support the creation of up to 20 MC peer groups using Ethernet ports in access mode. An MC peer group can contain one or more of the following child group objects:

- MC endpoint group (only for 7450 ESS, 7710 SR, and 7750 SR, Release 7.0 or later)—see chapter 39
- MC LAG group—see chapter 40
- MC synchronization group—see chapter 41
- MC ring group—see chapter 42

When you create a child group object, the 5620 SAM automatically creates the child group members using the peer objects in the MC peer group.

The 5620 SAM automatically discovers MC peers that are configured on managed NEs and creates an MC peer group if the source address of each peer matches the peer address of the other. If an MC peer address on an NE is changed after discovery, for example, using a CLI, the 5620 SAM deletes the MC peer group but does not delete the peer configuration on either NE. When the mismatch is corrected, the 5620 SAM recreates the MC peer group.

When the MC peer addresses match but the 5620 SAM detects another MC peer group configuration mismatch, the 5620 SAM raises an alarm and displays a check mark beside the Asymmetrical Configuration Detected indicator on the General tab of the MC Peer Group properties form. The alarm information includes the type of configuration mismatch. When the mismatch is corrected, the alarm and check mark clear.

38.2 Workflow to manage MC peer groups

1. Create an MC peer group.
2. Create an MC endpoint group, if required, as described in chapter 39.
3. Create an MC LAG, if required, as described in chapter 40.
4. Create an MC synchronization group, if required, as described in chapter 41
5. Create an MC ring group, if required, as described in chapter 42.

38.3 MC peer groups management procedures

Use the following procedures to perform MC peer group management tasks.

Procedure 38-1 To configure an MC peer group

Note — The 7210 SAS-M24F, 7210 SAS-M24F2XFP, and 7210 SAS-M24F2XFP [ETR] do not support MC LAGs.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list.

3 Perform one of the following:

a Configure an existing MC peer group. Perform the following:

i Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

ii Select an MC peer group and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

iii Go to step 4.

b Create an MC peer group by performing the following:

Note — At least one MC peer must be a 5620 SAM-managed NE. The 5620 SAM raises an alarm when an MC peer group contains an unmanaged NE.

i Click on the Create button. The MC Peer Group (Create) form opens with the General tab displayed.

ii Click on the Select button in the First Element panel to choose the first site for the peer group. The Select Site Info form opens.

iii Select an NE in the list and click on the OK button. The Select Site Info form closes, and the site name and system IP address are displayed on the MC Peer Group (Create) form.

iv To specify an interface other than the NE system interface for MC peer communication, click on the Select button beside the Source Address parameter. The Select a virtual router interface form opens.

Note 1 — Only numbered, non-multicast IPv4 interfaces are listed.

Note 2 — You can also enter a valid interface IP address.

v Select an interface in the list and click on the OK button. The interface address is listed on the MC Peer Group (Create) form.

vi Click on the Select button in the Second Element panel to choose the second site for the peer group. The Select Site Info form opens.

vii Select an NE in the list and click on the OK button. The Select Site Info form closes, and the site name and system IP address are displayed on the MC Peer Group (Create) form.

viii To specify an interface other than the NE system interface for MC peer communication, click on the Select button beside the Source Address parameter. The Select a virtual router interface form opens.

Note 1 — Only numbered, non-multicast IPv4 interfaces are listed.

Note 2 — You can also enter a valid interface IP address.

ix Select an interface in the list and click on the OK button. The interface address is listed on the MC Peer Group (Create) form.

4 Configure the following parameters in the First Element panel:

- Source Address
- Peer Name

  If Peer Name parameter is not configure, the peer IP address is used by the MC endpoint.
- Description
- Authentication Key
- Administrative State

5 Configure the following parameters in the Second Element panel:

- Source Address
- Peer Name

  If Peer Name parameter is not configure, the peer IP address is used by the MC endpoint.
- Description
- Authentication Key
- Administrative State

6 Click on the Peer Synchronization tab button.

7 Configure the parameters:

- Sync Administrative State
- IGMP
- IGMP Snooping
- Subscriber Management
- SRRP
- MC Ring
- MLD Snooping
- Subscriber Host Tracking

8 Click on the Apply button.

9 Click on the Associated Groups tab button.

10 Create an MC LAG, if required.

i Right-click on the MC LAG object in the components tree and choose Create MC LAG from the contextual menu. The MC LAG (Create) form opens.

ii Perform steps 7 to 11 in Procedure 40-1.

11 Create an MC synchronization group, if required.

i Right-click on the MC Sync Group object in the components tree and choose Create MC Sync Group from the contextual menu. The MC Sync Group (Create) form opens.

ii Perform steps 6 to 12 in Procedure 41-1.

12 Create an MC Ring Group, if required.

i Right-click on the MC Ring Group object in the components tree and choose Create MC Ring Group from the contextual menu. The MC Ring Group (Create) form opens.

ii Configure the Name parameter.

iii Click on the Select button beside the Synchronization Tag parameter. The Select Multi-Chassis Sync Group form opens.

iv Choose an MC synchronization group from the list and click on the OK button. The Select Multi-Chassis Sync Group form closes and the MC synchronization group is displayed on the MC Ring Group (Create) form.

13 Create an MC endpoint group, if required.

i Right-click on the MC Endpoint Group object in the components tree and choose Create Endpoint Group from the contextual menu. The MC Endpoint Group (Create) form opens.

ii Perform steps 2 to 5 in Procedure 39-1.

14 Click on the OK button. The MC Peer Group (Create) form closes.

15 Close the Manage Node Redundancy form.

Procedure 38-2 To configure an MC peer

Perform this procedure to modify an existing MC peer when there is a configuration mismatch with the other peer in an MC peer group.

Note — The MC peer parameters are configurable only when there is a configuration mismatch, which is indicated when the Neighbor Match check box on the MC Peer (Edit) form is unselected.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

4 Select an MC peer group and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

5 Click on the Members tab button.

6 Select an entry in the list and click on the Properties button. The MC Peer (Edit) form opens with the General tab displayed.

7 Configure the parameters:

- Description
- Source Address
- Authentication Key
- Administrative State

8 Perform the following to configure the MC LAG group parameters.

i Click on the MC LAG tab button.

ii Configure the parameters:

- Keepalive Interval (deciseconds)
- Lost Connection Wait Interval
- Administrative State

9 Perform the following to configure the MC synchronization group parameters.

i Click on the Synchronization Protocol tab button.

ii Select an entry in the list and click on the Properties button. The MC Peer Sync (Edit) form opens.

iii Configure the parameters:

- Synchronize IGMP
- Synchronize IGMP-Snooping
- Synchronize Subscriber Management
- Synchronize SRRP
- Synchronize MC Ring
- Synchronize MLD Snooping
- Synchronize Subscriber Host Tracking

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MC Peer Sync (Edit) form closes.

12 Close the MC Peer (Edit) form.

13 Close the MC Peer Group (Edit) form.

14 Close the Manage Node Redundancy form.

Procedure 38-3 To perform an on-demand protocol synchronization between MC peer group members

Perform this procedure to distribute the most recent protocol synchronization configuration to each member of an MC peer group. This is required when the configurations do not match, for example, after the configuration is changed locally on only one MC peer using a CLI. When the peer configurations do not match, the 5620 SAM raises an alarm and displays a check mark beside the Asymmetrical Configuration Detected indicator on the General tab of the MC Peer Group properties form.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC peer groups is displayed.

3 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

4 Click on the Synchronize Protocols tab button.

5 Click on the Re-Synchronize button. The member configurations are synchronized.

6 Close the MC Synchronization (Edit) form.

7 Close the Manage Node Redundancy form.

Procedure 38-4 To delete an MC peer group

Caution — Deleting an MC peer group removes all of the MC configurations that are associated with the MC peer group, such as the following:

- MC LAG groups
- MC synchronization groups
- MC ring groups

Ensure that you specify the correct MC peer group for deletion in this procedure.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC peer groups is displayed.

4 Select one or more MC peer groups in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. A Warning form opens.

6 View the dependency information.

7 Select the I understand the implications of this action check box.

8 Click on the Yes button. The 5620 SAM deletes the MC peer group and the corresponding configuration on each member site.

9 Close the Manage Node Redundancy form.

39 — MC endpoint groups

39.1 MC endpoint groups overview

An MC endpoint group consists of two MC endpoint peers that are configured as peers in a pair of sites. Multiple VPLS endpoints can use the MC endpoint peer. The endpoints must be on a 7450 ESS, 7750 SR, or 7710 SR, Release 7.0 or later, and support pseudo-wire redundancy. Each endpoint can be associated with different destinations, with a maximum of two spoke SDPs for each endpoint. The endpoints communicate with each other to get the associated status of the spoke SDPs, which ensures that only one spoke SDP is active at any time; the other spoke SDPs have a standby status. The grouping of multiple spoke SDPs that are associated with the two MC endpoint peers eliminates traffic loops in a VPLS or B-VPLS.

An MC endpoint group includes:

- two MC endpoint peers that can be used by a spoke SDP, which is under mc-endpoint and relies on mc-ep-peer in the CLI
- an MC protocol that is used for:
  - determination of which MC endpoint peers are active or standby
  - synchronization of the pseudo-wire information that is between the MC endpoint peers
  - fault detection using centralized BFD. The MC endpoint protocol contains a keep-alive mechanism because BFD cannot detect whether an MC endpoint peer is shut down or if there is a configuration problem.
- T-LDP signaling, which is used to communicate whether the pseudo-wire is active or standby to other gateway pairs. The other gateway pairs may not have an MC endpoint.

An MC peer group that is managed by the 5620 SAM contains two MC peers. Each MC peer is configured as the peer of the other MC peer. An MC peer group must be created before you create MC endpoint group. See chapter 38 for more information about MC peer groups.

BFD

The MC endpoint protocol uses the keep-alive mechanisms. The MC endpoint protocol also supports BFD to eliminate traffic loops. See Procedure 39-1 for information about how to configure an MC endpoint group for BFD.

39.2 Workflow to manage MC endpoint groups

1 Create an MC peer group, as described in chapter 38.

2 Create an MC endpoint group.

3 Create and configure the VPLS, as described in chapter 68.

i Create a site.

ii Create an endpoint.

- set the Endpoint Type parameter to Multi Chassis
- configure the EndPoint ID parameter
- select a multichassis endpoint peer

iii Configure spoke SDP binding.

4 Create an MC LAG, if required as described in chapter 40.

5 Create an MC synchronization group, if required as described in chapter 41.

6 Create an MC ring group, if required, as described in chapter 42.

39.3 MC endpoint groups management procedures

Use the following procedures to perform MC endpoint group management tasks.

Procedure 39-1 To configure an MC endpoint group

1 Create an MC peer group, as described in steps 1 to 13 of Procedure 38-1.

2 Configure the Description parameter.

3 Configure the parameters for the MC Endpoint on First Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

4 Configure the parameters for the MC Endpoint on Second Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

5 Click on the OK button.

6 Create a VPLS, site, and VPLS endpoint, as described in steps 1 to 21 of Procedure 68-1.

Note — In step 21iii of Procedure 68-1, set the Endpoint Type parameter to Multi Chassis and perform steps 21iv to 21x.

7 Click on the Yes button.

8 Perform one of the following:

a Create a redundant spoke SDP binding under an endpoint, as described in steps 5 to 38 of Procedure 68-5.

b Create a spoke SDP binding for the site, as described in steps 8 to 38 of Procedure 68-5.

Procedure 39-2 To modify an MC endpoint group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Endpoint Group (Multi-Chassis) from the Select Object Type drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC endpoint groups is displayed.

4 Choose an MC endpoint group and click on the Properties button. The MC Endpoint Group (Edit) form opens with the General tab displayed.

5 Configure the Description parameter.

6 Configure the parameters for the MC Endpoint on First Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

7 Configure the parameters for the MC Endpoint on Second Site:

- System Priority
- Keep-Alive Interval (deciseconds)
- Hold On Neighbor Failure
- Administrative State
- Passive Mode Enabled
- BFD Enabled
- Boot Timer

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The MC Endpoint Group form closes.

Procedure 39-3 To delete an MC endpoint group

Caution — When you perform this procedure, the MC endpoint group is deleted from the 5620 SAM and member NE configurations. In addition, deleting an MC endpoint group removes all of the MC configurations that are associated with the MC peer group.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Endpoint Group (Multi-Chassis) from the object list.

3 Configure the filter criteria and click on the Search button. A list of MC endpoint groups is displayed.

4 Choose one or more MC endpoint groups in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. A Warning window opens.

6 Review the dependency information.

7 Select the I understand the implications of this action check box.

8 Click on the Yes button. The 5620 SAM deletes the MC endpoint group and the corresponding configuration for each member site.

If there are MC endpoints that use the MC endpoint group, you cannot delete the MC endpoint group. Remove the MC endpoints from the MC endpoint group and repeat steps 1 to 9.

9 Close the Manage Node Redundancy form.

40 — MC LAG groups

40.1 MC LAG groups overview

A LAG is a group of physical ports that form one logical link between two NEs to increase bandwidth, allow load balancing, and provide seamless redundancy. LAG support over multiple devices provides node-level redundancy in addition to link-layer redundancy using a switchover function. An MC LAG configuration provides redundant L2 access connectivity that extends beyond link-layer protection by allowing two devices to share a common LAG end point.

An MC LAG configuration includes one active member NE and one standby member NE. The active and standby NEs synchronize the link state information to facilitate link-layer messaging between an access node and each NE. This active and standby NE coupling provides a synchronized forwarding plane to and from the access node. LACP is used to manage the active and standby states of the available LAG links; only the links of one member NE at a time are active.

The 7450 ESS, 7710 SR, and 7750 SR support the creation of MC LAG groups using Ethernet ports in Access mode.

Note — You can create an MC LAG group only from within an existing MC peer group. See chapter 38 for more information about MC peer groups.

When you use the 5620 SAM to change the MC LAG configuration on an NE, the 5620 SAM automatically updates the MC LAG configuration on the other NE. When you change the MC LAG configuration on an NE using, for example, a CLI, the 5620 SAM detects the configuration mismatch between the NEs and raises an alarm. The alarm information includes the type of configuration mismatch.

MC synchronization

When subscriber management is enabled on an NE in an MC LAG configuration, the NE maintains dynamic state information for each subscriber host. The active and standby NEs synchronize this information to ensure uninterrupted service delivery in the case of an MC LAG switchover.

See chapter 41 for more information about MC synchronization.

40.2 Workflow to manage MC LAG groups

1. Create one or more LAGs using Ethernet access ports, as required. See chapter 17 for more information.
2. Create an MC peer group. See chapter 38 for more information about creating MC peer groups.
3. Create an MC LAG group.

40.3 MC LAG groups management procedures

Use the following procedures to perform MC LAG management tasks.

Procedure 40-1 To create an MC LAG group

Perform this procedure to create an MC LAG group or to modify an existing MC LAG group. Consider the following before you create an MC LAG group:

- You can create an MC LAG member only on an Ethernet MDA.
- MC LAG member ports must be in Access mode.
- The 5620 SAM assigns the same LACP key, system ID, and system priority to each MC LAG member.
- MC LAGs are not supported when MAC subnetting is enabled.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list.

3 Click on the Search button. A list of MC peer groups is displayed.

4 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens.

5 Click on the Associated Groups tab button.

6 Right-click on the MC Lag object in the navigation tree and choose Create MC LAG Group. The MC LAG Group (Create) form opens.

7 Configure the parameters:

- LACP Key
- System ID
- System Priority
- Description

8 Configure the PBB Source Backbone MAC LSB parameters:

- Use LACP Key
- MAC LSB (hex)

Note — The parameters are only configurable in chassis mode D on the 7750 SR, 7750 SR-c12, and 7450 ESS. An MC LAG has two members. The parameters can be configured only when both peers are PBB-capable; for example, if the peers are either the 7750 SR or 7450 ESS in chassis mode D, or the 7750 SR-c12. If both peers are PBB-incapable, the PBB parameters are not displayed.

9 Perform the following steps to choose the LAG for the first MC LAG member.

i Click on the Select button beside the LAG ID parameter in the First Site panel. The Select LAG form opens.

ii If no LAGs are listed, you can create a LAG by clicking on the Create button and performing steps 4 to 23 of Procedure 17-23.

iii Select a LAG in the list and click on the OK button. The Select LAG form closes and the MC LAG (Create) form displays the LAG information.

10 Perform the following steps to choose the LAG for the first MC LAG member.

Note — If you are configuring access dual-homing with local switching over PBB tunnels, the L2 access interfaces must be on LAGs that participate in the MC LAG. See Procedure 67-11 to configure L2 access interfaces.

i Click on the Select button beside the LAG ID parameter in the Second Site panel. The Select LAG form opens.

ii If no LAGs appear in the list, you can create a LAG by clicking on the Create button and performing steps 4 to 23 of Procedure 17-23.

iii Select a LAG in the list and click on the OK button. The Select LAG form closes and the MC LAG (Create) form displays the LAG information.

11 Click on the OK button. The MC LAG (Create) form closes, and the new MC LAG object is displayed below the MC LAG object in the navigation tree on the MC Peer Group (Edit) form.

12 Close the MC Peer Group (Edit) form.

13 Close the Manage Node Redundancy form.

Procedure 40-2 To configure an MC LAG group member

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC LAG Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC LAGs is displayed.

4 Select an MC LAG in the list and click on the Properties button. The MC LAG Group (Edit) form opens with the General tab displayed.

5 Configure the MC LAG parameters that are common to each member, if required:

- LACP Key
- System ID
- System Priority
- Description

6 Click on the States tab button.

7 Click on the Properties button beside the Administrative State field in the MC Peer Communication section of the First Site panel. The NE Synchronization (Edit) form opens with the General tab displayed.

8 Configure the MC LAG member by performing the following steps.

i Click on the MC LAG tab button. The General tab is displayed.

ii Configure the parameters:

- Keepalive Interval (deciseconds)
- Lost Connection Wait Interval
- Administrative State

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The NE Synchronization (Edit) form closes.

v Close the MC LAG Group (Edit) form.

9 Click on the Properties button beside the Administrative State field in the MC Peer Communication section of the Second Site panel. The NE Synchronization (Edit) form opens with the General tab displayed.

10 Repeat step 8.

11 Close the MC LAG Group (Edit) form.

12 Close the Manage Node Redundancy form.

Procedure 40-3 To delete an MC LAG group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC LAG Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC LAG groups is displayed.

4 Select one or more MC LAG groups in the list and click on the Delete button. A dialog box appears.

5 Click on the View Dependencies button. An information dialog box appears.

6 View the dependency information.

7 Click on the OK button.

8 Click on the Yes button. The 5620 SAM deletes the MC LAG group and the corresponding configuration on each member site.

Note — If you change the default values of the Keepalive Interval (deciseconds) and Lost Connection Wait Interval parameters in step 8ii of Procedure 40-2, the MC LAG group configuration of the member sites is not removed. You can view the MC LAG member information under the LAG icon in the network view of the navigation tree.

9 Close the Manage Node Redundancy form.

41 — MC synchronization groups

41.1 MC synchronization groups overview

When subscriber management is enabled on an NE, the NE maintains dynamic subscriber-host state information. The state information must be synchronized between the active and standby NEs in a redundant configuration to ensure that service delivery is uninterrupted if a switchover occurs.

The 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, 7710 SR, and 7750 SR support the creation of MC synchronization groups using Ethernet ports in Access mode.

Note — You can create an MC synchronization group only from within an existing MC peer group. See chapter 38 for more information about MC peer groups.

MC synchronization can be used to ensure that the following dynamic state information is synchronized:

- Basic and enhanced subscriber management
- IGMP snooping in VPLS
- IGMP on IES or VPRN group interfaces
- SRRP in VPRN

You create an MC synchronization group inside an MC peer group using a unique synchronization tag to define the pair of NEs and the two ports or LAGs on which the dynamic state information is synchronized. The synchronization is applied to all SAPS on the port or LAG that have the same synchronization tag.

A synchronization tag can be applied to a specified VLAN range on a port or LAG. All of the SAPs in the VLAN range are assigned the synchronization tag. The SAPs that are not in the VLAN range are not synchronized.

Note 1 — Only ports and LAGs that use Dot1 Q or QinQ encapsulation support MC synchronization.

Note 2 — MC synchronization group VLAN ranges are configurable only after MC synchronization group creation.

Note 3 — If the 5620 SAM detects a port or VLAN range configuration mismatch in an MC synchronization group during NE discovery, the 5620 SAM raises an alarm.

MC synchronization and dual-homed L2/L3 CO

MC synchronization is typically used in a dual-homed L2 or L3 CO configuration. For example, an access node that aggregates several subscriber lines can be dual-homed to a redundant pair of NEs. Dynamic subscriber-host state information on the NE must be synchronized with the redundant peer to ensure that service delivery in unaffected if a switchover occurs. See chapters 70 and 71 for more information about L2 and L3 CO dual homing.

MC synchronization for dual homing requires the configuration of protocol synchronization on the MC peer group that defines the redundant pair of NEs. See Procedure 38-1 for more information about configuring protocol synchronization on an MC peer group.

41.2 Workflow to manage MC synchronization groups

1 Create an MC peer group. See chapter 38 for information about MC peer groups.

2 Create an MC synchronization group.

3 Configure MC peer synchronization ports or VLAN ranges.

4 Configure protocol synchronization for the MC synchronization group.

41.3 MC synchronization groups managment procedures

Use the following procedures to perform MC synchronization management tasks.

Procedure 41-1 To create an MC synchronization group

Note — The 7210 SAS-M24F, 7210 SAS-M24F2XFP, and 7210 SAS-M24F2XFP [ETR] do not support MC LAGs.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC peer groups is displayed.

3 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

4 Click on the Associated Groups tab button.

5 Right-click on the MC Sync Group object in the navigation tree and choose Create MC Sync Group from the drop-down menu. The MC Sync Group (Create) form opens.

6 Configure the parameters:

- Synchronization Tag
- Description
- Sync Tag Config Level

7 Specify the port or LAG on the first NE.

Click on the Select button beside the Port/LAG Name parameter in the First Element panel. The Select Port/LAG - MC Sync Group form opens.

Note — If you set the Sync Tag Config Level parameter to VLAN Range Level, only Dot1 Q and QinQ-encapsulated Ethernet ports or LAGs in Access mode are listed.

8 Select a port or LAG in the list and click on the OK button. The Select Port/LAG - MC Sync Group form closes, and the port or LAG information is displayed on the MC Sync Group (Create) form.

9 Specify the port or LAG on the second NE.

Click on the Select button beside the Port/LAG Name parameter in the Second Element panel. The Select Port/LAG - MC Sync Group form opens.

Note — Only ports or LAGs that have the same encapsulation type as the port or LAG on the first NE are listed.

10 Select a port or LAG in the list and click on the OK button. The Select Port/LAG - MC Sync Group form closes, and the port or LAG information is displayed on the MC Sync Group (Create) form.

11 If you set the Sync Tag Config Level parameter to VLAN Range Level, perform the following steps to specify the VLAN ranges that the MC synchronization group is to monitor.

Note — The VLAN ranges that you configure are applied to the configuration of each site in the MC synchronization group.

i Click on the Apply button. The form displays additional tabs.

ii Click on the First Site VLAN Entries tab button.

iii Click on the Add button. The VLAN Range (Create) form opens.

iv Configure the parameters:

- Minimum Outer Encap Value
- Maximum Outer Encap Value
- Minimum Inner Encap Value
- Maximum Inner Encap Value

The Minimum Inner Encap Value and Maximum Inner Encap Value parameters are configurable only when the encapsulation type of the associated ports or LAGs is Q in Q.

v Click on the OK button. The VLAN Range (Create) form closes.

vi Repeat steps 11 iii to v to add another VLAN range, if required.

12 Close the MC Sync Group (Create) form.

13 Close the MC Peer Group (Edit) form.

14 Close the Manage Node Redundancy form.

Procedure 41-2 To configure protocol synchronization between MC peer group members

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Peer Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC peer groups is displayed.

3 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens with the General tab displayed.

4 Click on the Synchronize Protocols tab button.

5 Configure the parameters:

- Sync Administrative State
- IGMP
- IGMP Snooping
- Subscriber Management
- SRRP
- MC Ring
- MLD Snooping
- Subscriber Host Tracking

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The MC Synchronization (Edit) form closes.

8 Close the Manage Node Redundancy form.

Procedure 41-3 To delete an MC synchronization group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Sync Group (Multi-Chassis) from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of MC synchronization groups is displayed.

4 Select one or more MC synchronization groups in the list and click on the Delete button. A dialog box appears.

Caution — Deleting an MC synchronization group that is associated with an MC ring group disables the protocol synchronization between the member sites in the MC ring group.

5 Click on the Yes button. The 5620 SAM deletes the MC synchronization group and the corresponding configuration on each member site.

6 Close the Manage Node Redundancy form.

42 — MC ring groups

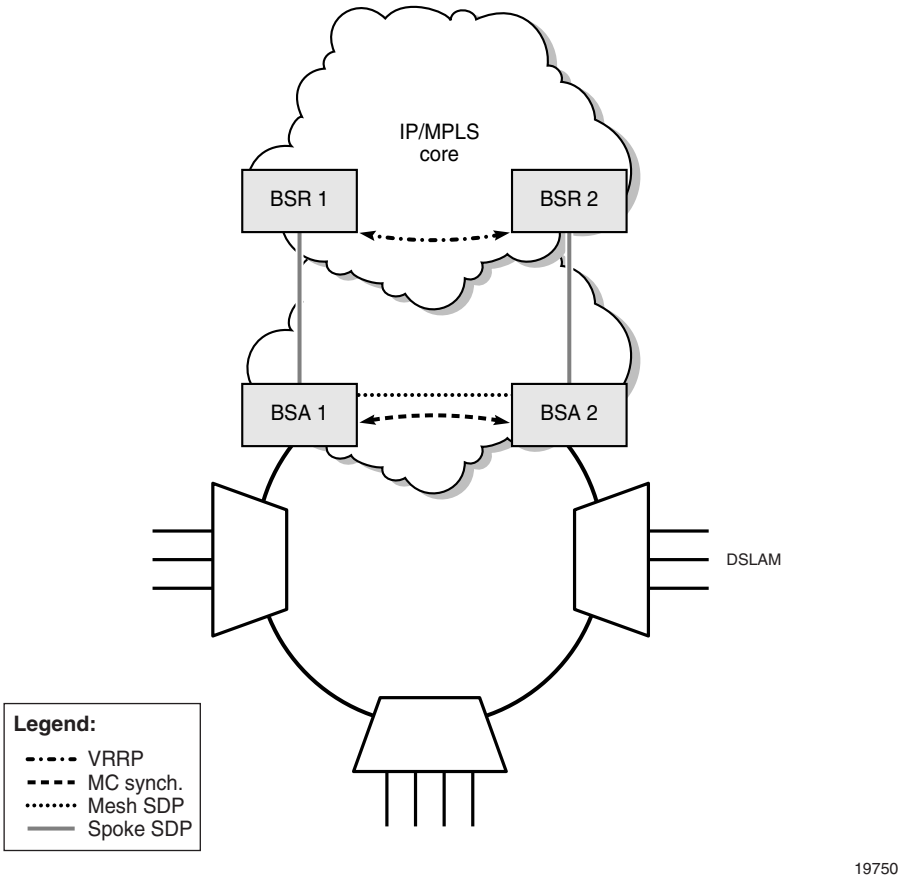
42.1 MC ring groups overview

5620 SAM MC ring groups are an extension of the dual-homing support available in TPSDA networks. MC ring groups provide aggregation redundancy in networks that have multiple access nodes, called ring nodes in the context of MC ring groups, connected in a single ring.

The 7210 SAS-M, 7450 ESS, 7710 SR, and 7750 SR support the creation of MC ring groups using Ethernet ports in Access mode.

Figure 42-1 shows a simple subscriber aggregation network in which a single ring of access nodes, such as DSLAMs, is connected to a BSA in a VPLS. Each BSA is connected to an IES or VPRN L3 interface on a BSR using a spoke SDP. Each BSR L3 interface aggregates the subscriber traffic in one subnet.

Figure 42-1 Simple subscriber aggregation network



Note 1 — BTV distribution is typically implemented in a separate VPLS that uses one SAP per access node.

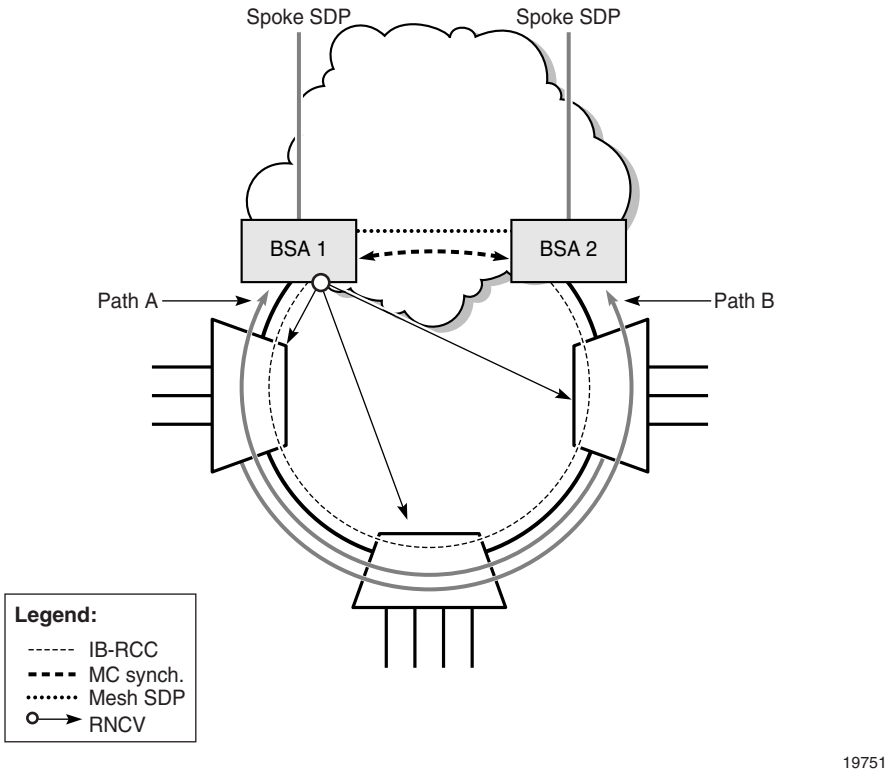
Note 2 — An MC ring group does not support a ring that has more than one break.

Steady-state condition

When an MC ring group is configured, the operation of a typical dual-homed ring is as shown in Figure 42-2. A steady-state condition is defined by the following.

- The participating BSAs have matching MC ring configurations.
- The In-Band Ring Control Connection, or IB-RCC, is operationally up.
- The MC ring is operationally up.

Figure 42-2 Dual-homed ring, steady-state condition



The IB-RCC is set up using a BFD session between IES or VPRN IP interfaces on BSA 1 and BSA 2. This connection requires a separate ring VLAN.

Note — You can create an MC ring group only from within an existing MC peer group. See chapter 38 for more information about MC peer groups.

In the steady state, the ring is fully closed and each ring node has two paths to the VPLS core; these are shown as Path A and Path B. To prevent a communication loop, a ring node can use only one path for VLAN traffic. The VLAN range can be explicitly assigned to Path B on each BSA; by default, the SAP uses Path A. The VLAN range assignment for each path must be the same on each BSA. A SAP in the conflict range is assigned to Path A, regardless of the local configuration.

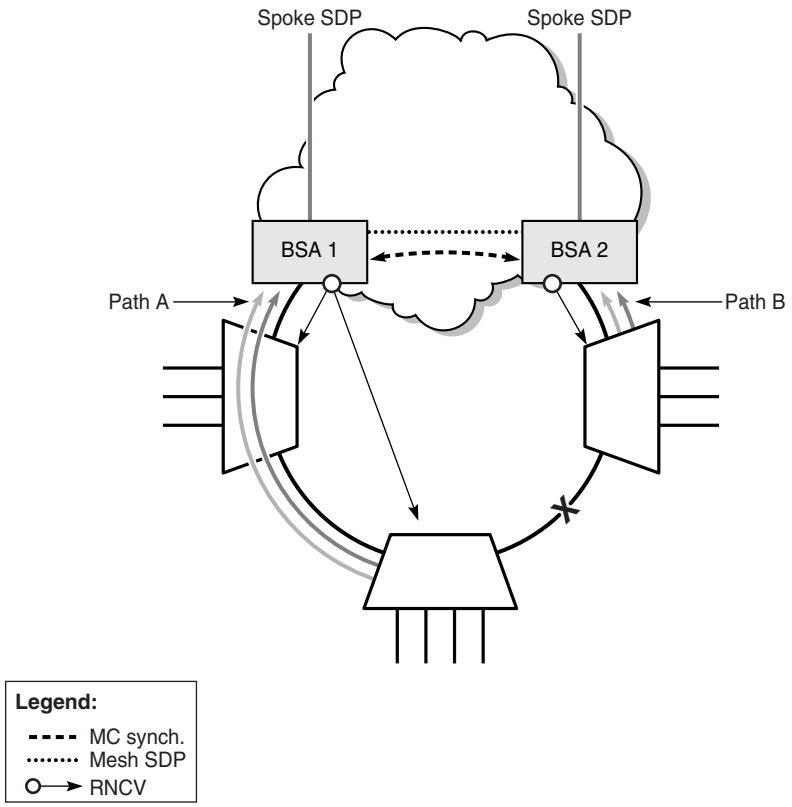
Each SAP in the path that ends on the master BSA is operationally up. Each subscriber-host forwarding database entry associated with the SAP points to the SAP. Each SAP in the path that ends on the standby BSA is operationally down. Each subscriber-host forwarding database entry associated with the SAP points to the mesh SDP that connects to the master BSA.

The master BSA periodically performs a Ring Node Connectivity Verification, or RNCV, check. The loss of connectivity to a ring node does not automatically trigger a switchover to the other path; if the IB-RCC BFD session is up, the ring is considered closed, and the master and standby BSA roles do not change.

Broken ring condition

A broken ring condition occurs when there is a link failure or ring node failure, as shown in Figure 42-3. In this condition, the IB-RCC is operationally down. Each ring node has only one path to the VPLS core.

Figure 42-3 Dual-homed ring, broken-ring condition



Each BSA becomes the master for the ring nodes that it can reach, and performs as described in the steady-state condition. Each L2 SAP on each BSA is operationally up, except the SAPs that are explicitly excluded from the MC ring control.

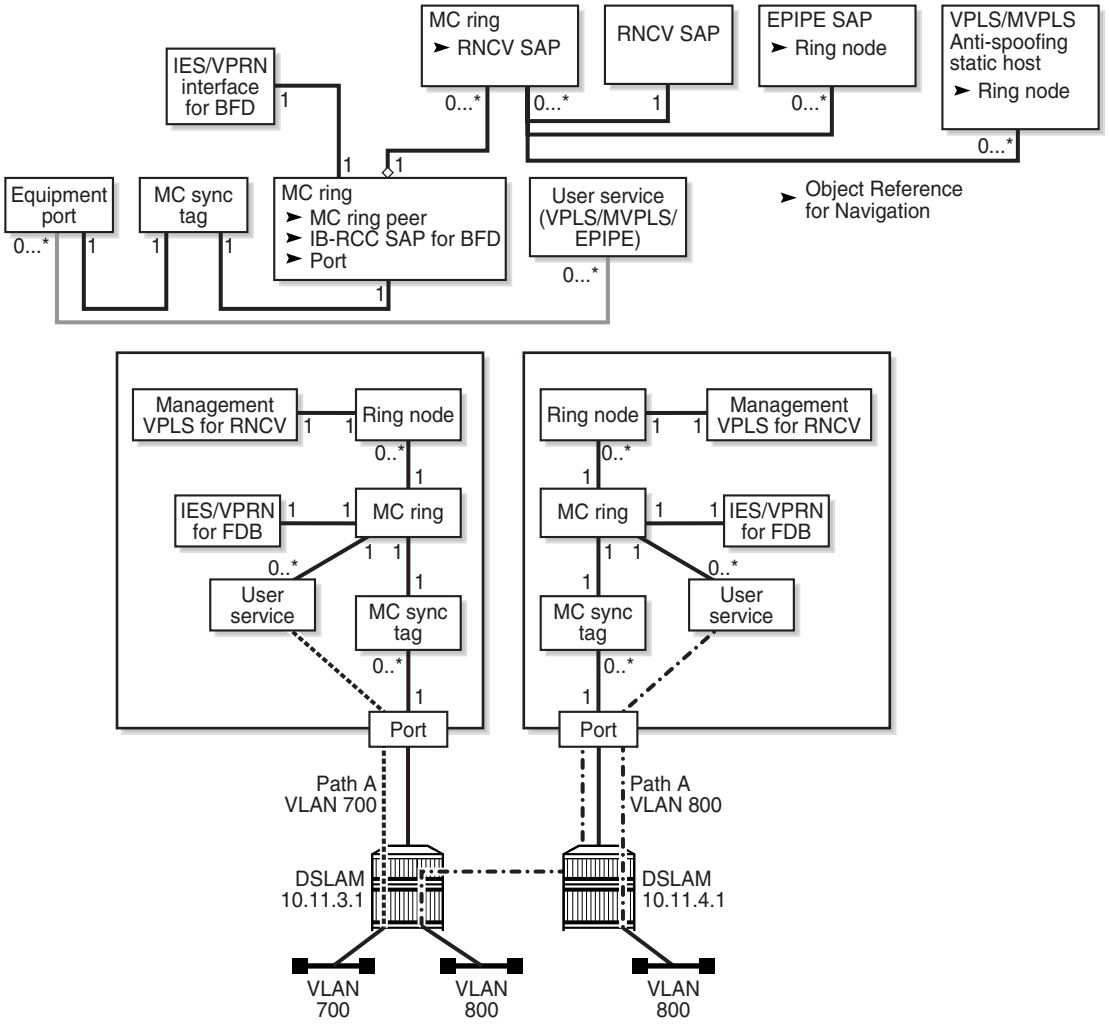
In the broken-ring condition, each BSA performs an RNCV check because each is a master. The forwarding database entry for each subscriber host behind a unreachable ring node points to the mesh SDP.

When the MC ring connectivity is restored, one BSA is the master for Path A and the other BSA is the master for Path B.

Object relationships

Figure 42-4 shows the MC ring and ring node object relationships with equipment and service objects.

Figure 42-4 MC ring group object relationships



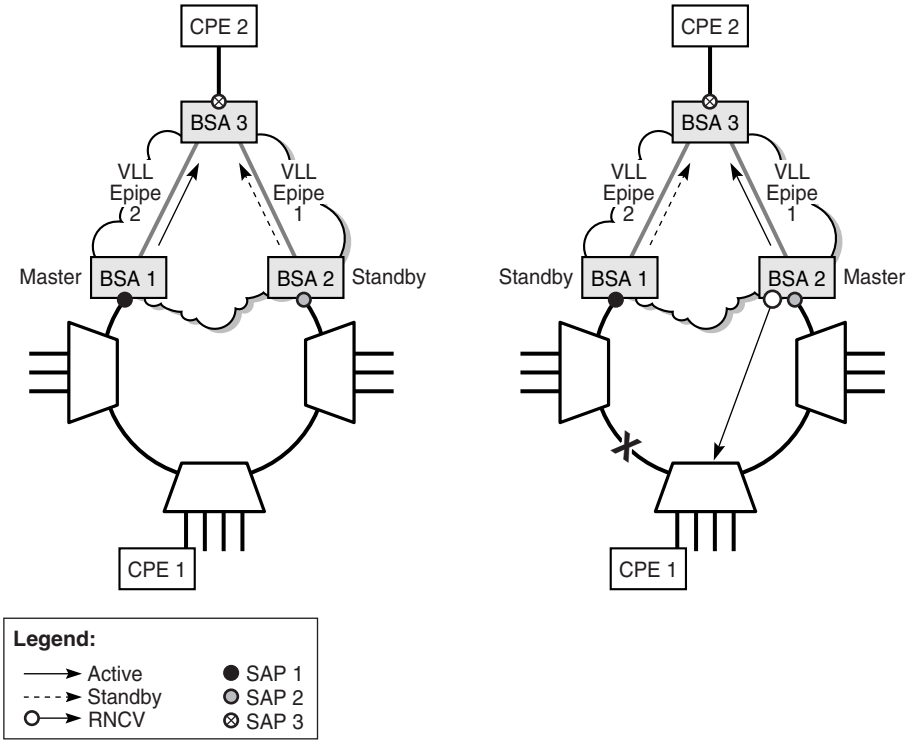
An MC ring has a one-to-one relationship with an MC synchronization tag. An MC ring uses one IES or VPRN service for IB-RCC. An MC ring can have multiple ring nodes, and each ring node can use only one SAP for RNCV.

When an MC ring group is correctly configured, each BSA L2 SAP is protected by the ring. The service that contains these protected SAPs is referred to as the user service. The service that is used for RNCV is an MVPLS that can also contain user SAPs and be a user service.

MC ring group and redundant VLL Epipe access operation

An MC ring group can connect to a VLL SAP to support redundant VLL Epipe access. Figure 42-5 shows a sample configuration using a VLL Epipe.

Figure 42-5 Dual-homed VLL Epipe configuration



CPE 1 connects to a ring node that has access to each BSA through a VLAN that is provisioned on each ring node. The SAP on each BSA uses the same VLAN tag.

In the closed ring on the left, BSA 1 is the master and sends an active status notification to BSA 3 on a VLL Epipe. BSA 2, the standby, sends a standby status notification. Based on this information, BSA 3 chooses a path to reach CPE 2.

In the broken ring on the right, the BSA that can use RNCV to reach CPE 1 becomes the master and sends an active status notification to BSA 3 on a VLL Epipe.

In each scenario, only one SAP is operationally up at a time, and each Epipe must be operationally up. If the ring node of CPE 1 is operationally down, neither BSA can reach the ring node, so each SAP and Epipe is operationally down.

MC ring groups and subscriber hosts

Each subscriber host on a SAP that is protected by an MC ring group must be associated with a ring node to determine whether the subscriber host is reachable by the BSA. Each VLL Epipe used for forwarding from an MC ring group must be explicitly configured with the name of a ring node in the MC ring. See Procedure 42-3 for information about configuring VLL Epipes for use with an MC ring group.

When subscriber management is enabled on a VPLS SAP, each dynamic subscriber host is automatically associated with a ring node. Static hosts on a VPLS SAP require explicit configuration. The following must be true before you can turn up an MC ring on a VPLS SAP that has one or more static hosts, or turn up a static host on a VPLS SAP in an operational MC ring:

- Subscriber management is enabled.
- The following are configured on the static host:
  - the name of a ring node in the MC ring group
  - subscriber identification
  - a subscriber profile
  - an SLA profile

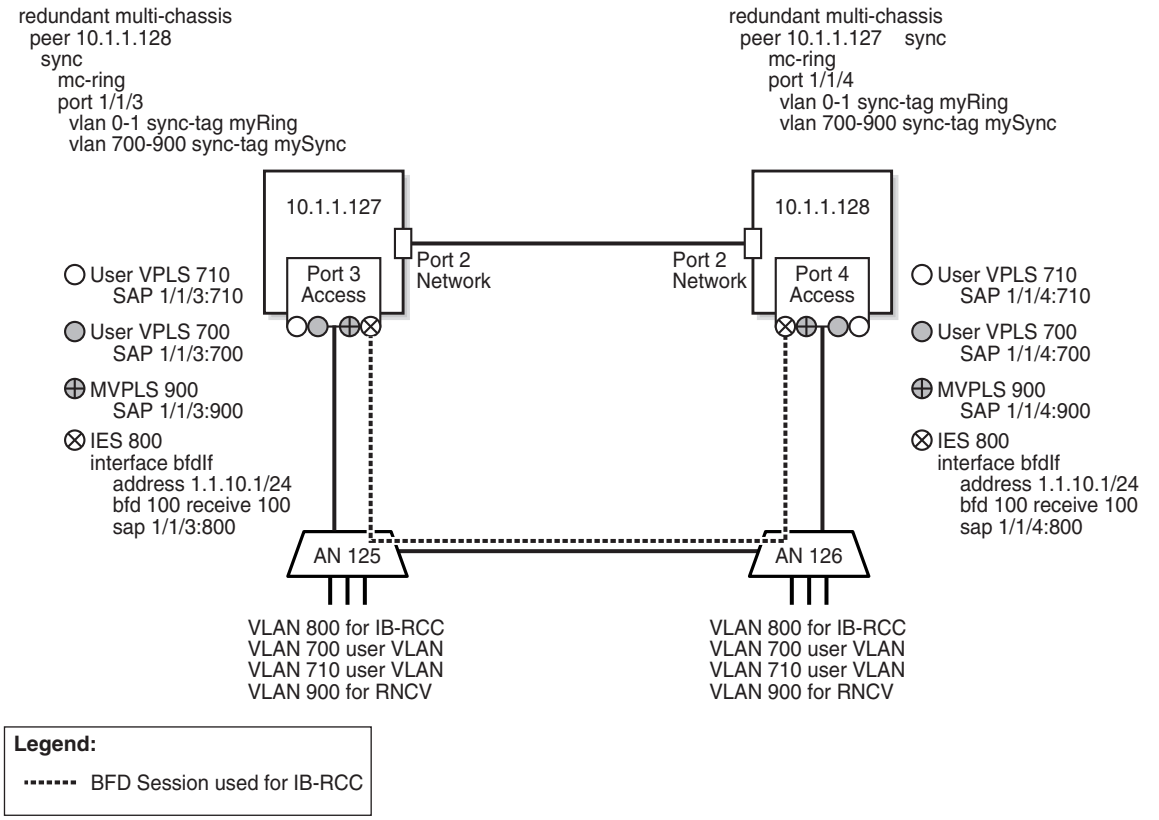
42.2 Workflow to manage MC ring groups

The following are the high-level steps required to perform MC ring group management.

NE preconfiguration

1 Configure physical connectivity between the two BSAs and the ring nodes, as shown in Figure 42-6. Each port must be operationally up.

Figure 42-6 MC ring group preconfiguration



2 Configure a routing protocol on each BSA to enable IP communication. See chapter 28 for information about configuring routing protocols.

3 Configure an MVPLS for RNCV on the BSAs. See chapter 68 for information about configuring MVPLS.

4 Create an MC peer group that has the two BSAs as members and has MC ring synchronization enabled. See chapter 38 for information about MC peer groups.

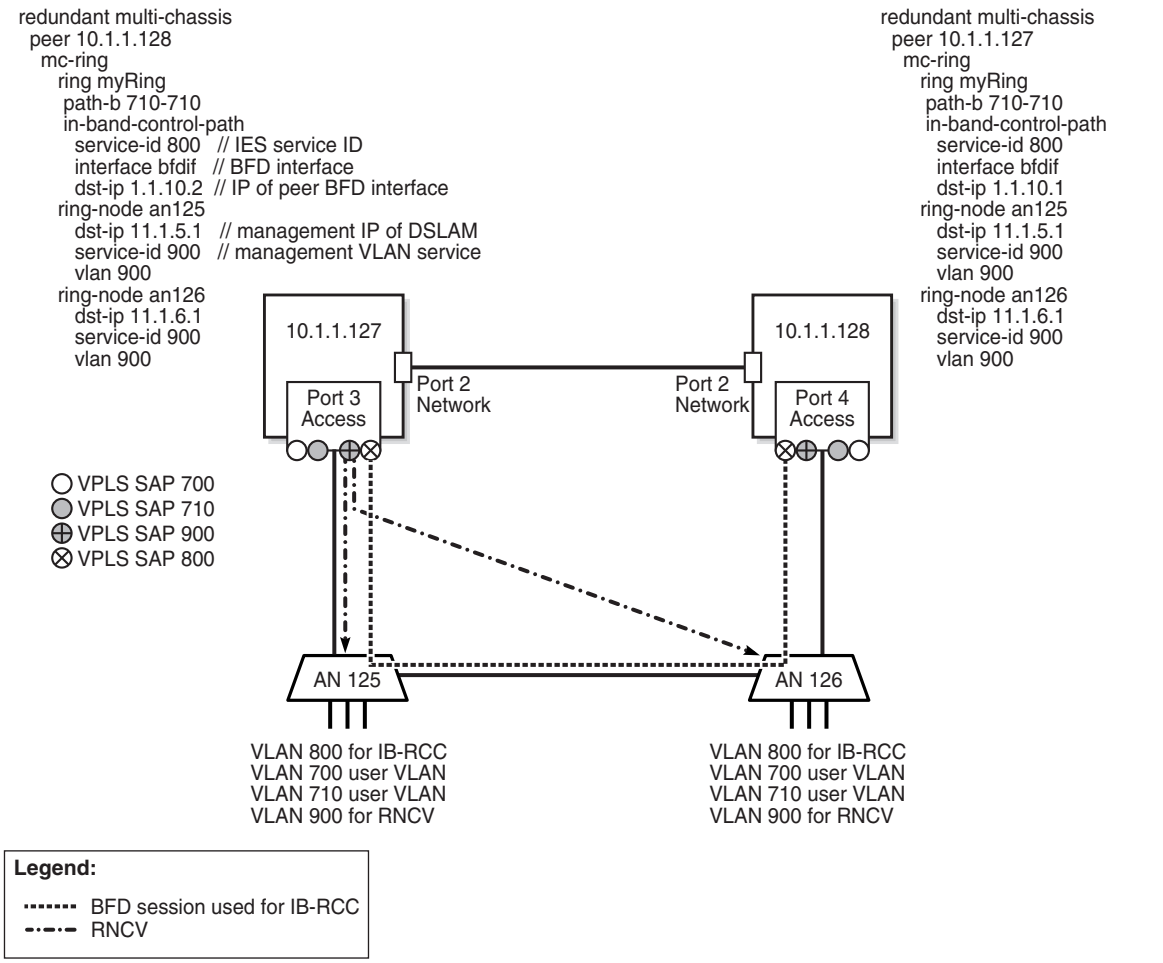
5 In the MC peer group, create an MC synchronization group that specifies each BSA access port. The MC synchronization group can synchronize the port or a VLAN range. See chapter 41 for information about MC synchronization groups.

6 Configure each ring node with the VLAN tag used for BFD to enable BFD communication through the ring. After this, each BSA SAP should be operational.

MC ring group configuration

7 Use the 5620 SAM to create an MC ring group that contains the BSAs, which are shown as 10.1.1.127 and 10.1.1.128 in Figure 42-7.

Figure 42-7 MC ring configuration



8 Create the ring nodes in the MC ring group. For each ring node, you must specify the management IP address of a ring node as the destination IP address and assign one VLAN for connectivity checking, shown in Figure 42-7 as VLAN 900.

9 Create the user VPLS and assign a SAP to each of the two BSA access ports. You can configure a protecting SAP on each BSA to provide SAP-level redundancy, if required. See chapter 68 for more information.

10 If the VPLS is to send traffic to an IES or a VPRN service, perform the following steps.

- **i** Create a spoke SDP from each VPLS site in the MC ring group to the IES or VPRN service.
- **ii** Configure traffic forwarding to the IES or VPRN service. See Procedure 42-2 for more information.

11 If the VPLS is to send traffic to redundant VLL Epipes, perform the following steps.

i Create a redundant VLL Epipe from each VPLS site in the MC ring group to the BSA that is the common endpoint of the VLL Epipes.

ii Configure traffic forwarding to each VLL Epipe service. See Procedure 42-3 for more information.

12 If the VPLS is to send traffic to an IES or a VPRN service, create a spoke SDP from the VPLS to the IES or VPRN service. See Procedure 42-2 for information about configuring the spoke SDP to send traffic from the MVPLS to an IES or a VPRN service.

13 Turn up the MC ring.

At this point, the following statements apply to the Figure 42-7 configuration.

- VPLS SAP 700 is operationally up on BSA 10.1.1.127 and operationally down on BSA 10.1.1.128.
- VPLS SAP 710 is operationally down on BSA 10.1.1.127 and operationally up on BSA 10.1.1.128.
- The operational state of the ring is Connected.

To test the configuration, you can shut down an access-node port in the ring to break the ring. As a result, the BSA SAPs should remain operationally up, but the operational state of the ring changes to Broken.

42.3 MC ring groups management procedures

Use the following procedures to perform MC ring group management tasks.

Procedure 42-1 To create an MC ring group

Note — You cannot create an MC ring SAP on a VPLS site that is the endpoint of redundant spoke SDPs.

1 Perform the NE preconfiguration steps in the workflow of this chapter.

2 Before you can deploy an MC ring to the participating BSAs, you must create an MC synchronization group. Perform 41-1 to create an MC synchronization group for the BSAs.

3 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

4 Choose MC Peer Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of previously created MC peer groups is displayed. See chapter 38 for information about creating MC peer groups.

5 Select an MC peer group in the list and click on the Properties button. The MC Peer Group (Edit) form opens.

6 Click on the Associated Groups tab button.

7 Right-click on the MC Ring Group object and choose Create MC Ring Group from the drop-down menu. The MC Ring Group (Create) form opens.

8 Configure the parameters:

- Name
- Synchronization Tag

9 Click on the Apply button. The form displays additional tabs.

10 Click on the Properties button in the Multi-Chassis Ring on First Site panel. The MC Ring (Edit) form opens with the General tab displayed.

11 Configure the parameters:

- Interface Name
- Service ID
- Destination IP Address

12 Perform the following steps to create a ring node.

i Click on the Components tab button.

ii Right-click on the MC Ring object and choose Create MC Ring Node. The MC Ring Node (Create) form opens.

iii Configure the parameters:

- Ring Node Name
- SAP Service ID
- SAP Outer Encapsulation Value
- SAP Inner Encapsulation Value
- Source IP Address
- Destination IP Address
- Source MAC Address
- Interval (minutes)

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The MC Ring Node (Create) form closes.

vi Repeat steps 12 ii to v to create an additional ring node, if required.

13 To configure a VLAN range for traffic that is to use the non-default path through the MC ring, perform the following steps.

i Click on the Path B VLAN Range tab button.

ii Click on the Add button. The Path B VLAN Range (Create) form opens.

iii Configure the parameters:

- Start VLAN Value
- End VLAN Value

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The VLAN range entry is displayed on the MC Ring (Edit) form.

14 To configure a VLAN range for traffic that is not to be protected by the MC ring, perform the following steps.

i Click on the Exclude VLAN Range tab button. The Exclude VLAN Range (Create) form opens.

ii Click on the Add button. The Path B VLAN Range (Create) form opens.

iii Configure the parameters:

- Start VLAN Value
- End VLAN Value

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The VLAN range entry is displayed on the MC Ring (Edit) form.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The MC Ring (Edit) form closes.

17 Click on the Properties button in the Multi-Chassis Ring on Second Site panel. The MC Ring (Edit) form opens with the General tab displayed.

18 Repeat steps 11 to 16.

19 Close the MC Ring Group (Create) form.

Procedure 42-2 To configure L3 forwarding from a VPLS or MVPLS to an IES or VPRN service

Perform this procedure to configure MC ring group traffic forwarding through a BSA spoke SDP to a BSR L3 access interface in an IES or VPRN service, as shown in Figure 42-1. See chapter 68 for information about creating and configuring VPLS and MVPLS services.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services is displayed.

3 Select the appropriate VPLS or MVPLS in the list and click on the Properties button. The service properties form opens.

4 Click on the Components tab button.

5 Right-click on a site and choose Properties from the contextual menu. The site properties form opens.

6 Click on the Default Gateway tab button.

7 Configure the parameters, which specify the IP and MAC address of the default gateway to which the VPLS is to forward L3 traffic.

8 Click on the OK button. The site properties form closes.

9 Click on the OK button. The service properties form closes.

Procedure 42-3 To configure an MC ring group for redundant VLL Epipe access

Perform this procedure to configure traffic forwarding from a BSA SAP in an MC ring group through a VLL Epipe to a BSA SAP outside the ring group, as shown in Figure 42-5. See chapter 67 for information about creating and configuring VLL Epipe services.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services is displayed.

3 Select the appropriate VLL Epipe service in the list and click on the Properties button. The Epipe Service (Edit) form opens.

4 Click on the Components tab button.

5 Right-click on an L2 access interface and choose Properties from the contextual menu. The L2 Access Interface (Edit) form opens with the General tab displayed.

6 Perform one of the following to specify a ring node in the ring group that terminates on the port associated with the L2 access interface.

   a Perform the following steps to select the ring node from a list.

      i Click on the Select button in the MC Redundancy panel. The Select form opens.

      ii Select a ring node in the list and click on the OK button. The Select form closes, and the ring node name is displayed on the L2 Access Interface (Edit) form.

   b Type the name of the ring node in the MC Ring Node field.

7 Click on the OK button. The L2 Access Interface (Edit) form closes, and a dialog box appears.

8 Click on the OK button. The Epipe Service (Edit) form reappears.

9 Click on the OK button.A dialog box appears.

10 Click on the Yes button. The Epipe Service (Edit) form closes.

Procedure 42-4 To turn up the MC rings in an MC ring group

Note 1 — You cannot administratively enable an MC ring group in one operation; you must turn up the MC rings in the MC ring group individually.

Note 2 — If a Problems Encountered form is displayed when you try to turn up an MC ring, you can perform one or both of the following to view information about the problem.

- Select the listed problem and click on the Properties button.
- View the Operational State and Failure Reason fields on the State tab of the MC ring properties form.

The 5620 SAM performs a series of checks to determine whether an MC ring can be turned up. The checks include verifying the following:

- The synchronization tag is configured on the BSA.
- The VLAN-level synchronization tag is valid.
- The IES or VPRN interface for the IB-RCC is configured.
- BFD is enabled on the IB-RCC interface.
- The IES or VPRN interface is operationally up.
- The IB-RCC interface is not in use by another MC ring.
- The IB-RCC interface is on the port used for MC synchronization.
- The IB-RCC destination IP address is configured.
- The IB-RCC destination IP address is not the same as the IB-RCC source IP address.
- The IB-RCC destination IP address is not in the same subnet as the IB-RCC source IP address.
- The MVPLS or VPLS site is not configured as an endpoint for redundant spoke SDPs.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Ring Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC ring groups is displayed.

3 Select an MC ring group in the list and click on the Properties button. The MC Ring Group (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a Turn up the MC ring using the MC ring properties form.

Note — Using this method enables you to view real-time MC ring status information while the 5620 SAM turns up the MC ring.

i Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on First Site panel. The MC Ring (Edit) form opens.

ii Click on the State tab button.

iii Set the Administrative State parameter to Up.

iv Click on the Apply button. A dialog box appears.

v Click on the Yes button. The 5620 SAM tries to turn up the MC ring.

vi View the dynamically updated information in the Operational State field.

vii Close the MC Ring (Edit) form.

viii Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on Second Site panel. The MC Ring (Edit) form opens.

ix Repeat steps 4 a ii to vii.

b Turn up the MC ring using the navigation tree. Perform the following steps.

i Click on the Components tab button.

ii Right-click on the first site object and choose Turn Up from the contextual menu. A dialog box appears.

iii Click on the Yes button. The 5620 SAM tries to turn up the MC ring.

iv Right-click on the second site object and click on the Turn Up button. A dialog box appears.

v Click on the Yes button. The 5620 SAM tries to turn up the MC ring.

5 Close the MC Ring Group (Edit) form.

Procedure 42-5 To view the operational status of MC ring group components

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Ring Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC ring groups is displayed.

3 Select an MC ring group in the list and click on the Properties button. The MC Ring Group (Edit) form opens with the General tab displayed.

4 Click on the Properties button beside a site that hosts an MC ring. The MC Ring (Edit) form opens.

5 Click on the State tab button.

6 View the dynamically updated information in the Operational State field. The Operational State is one of the following:

- Unknown—the 5620 SAM cannot determine the operational state
- Shut Down—the MC ring is administratively down
- Config Error—the MC ring has a configuration error
- No Peer—the peer MC ring is not configured
- Connected—the MC ring is operational
- Broken—the RNCV check fails
- Local Broken—the MC ring site cannot connect to a ring node
- Conflict—the MC ring configuration conflicts with another configuration
- Testing Ring—an RNCV check is in progress
- Peer Down—the peer MC ring site is inoperable
- Waiting For Peer—the peer MC ring site is initializing

7 Click on the Components tab button.

8 Right-click on a ring node object and choose Properties from the contextual menu. The MC Ring Node (Edit) form opens with the General tab displayed.

9 Click on the State tab button.

10 View the dynamically updated information in the Local Operational State and Remote Operational State fields. The Operational State is one of the following:

- Unknown—the 5620 SAM cannot determine the operational state
- Not Provisioned—the ring node configuration is incomplete
- Config Error—the ring node is misconfigured
- Not Tested—no RNCV check result is available
- Testing—an RNCV check is in progress
- Connected—the ring node is operational
- Disconnected—the ring node cannot be reached

11 Close the MC Ring Node (Edit) form.

12 Close the MC Ring (Edit) form.

13 Close the MC Ring Group (Edit) form.

Procedure 42-6 To delete an MC ring group

Caution — Deleting an MC ring group removes all of the child objects that are associated with the MC ring group, such as the following:

- MC rings
- ring nodes

Ensure that you specify the correct MC ring group for deletion in this procedure.

Note 1 — You must set the administrative state of an MC ring to Down before you can delete the MC ring.

Note 2 — Before you can set the administrative state of an MC ring to Down, you must administratively disable each VPLS or MVPLS SAP in the ring, regardless of the path they use.

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC Ring Group (Multi-Chassis) from the object drop-down list and click on the Search button. A list of MC ring groups is displayed.

3 Select an MC ring group in the list and click on the Properties button. The MC Ring Group (Edit) form opens with the General tab displayed.

4 Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on First Site panel. The MC Ring (Edit) form opens.

5 Click on the State tab button.

6 Set the Administrative State parameter to Down.

7 Click on the Apply button. A dialog box appears.

8 Click on the Yes button. The 5620 SAM shuts down the MC ring.

9 Close the MC Ring (Edit) form.

10 Click on the Properties button beside the Site ID parameter in the Multi-Chassis Ring on Second Site panel. The MC Ring (Edit) form opens.

11 Repeat steps 5 to 9.

12 Select the MC ring group in the list and click on the Delete button. A dialog box appears.

13 Click on the View Dependencies button. A Warning form opens.

14 View the dependency information.

15 Select the I understand the implications of this action check box.

16 Click on the Yes button. The 5620 SAM deletes the MC ring group and the corresponding configuration on each member site.

17 Close the Manage Node Redundancy form.

Policy management

59 — Format and range policies

43 — Policies overview

43.1 Policies overview

The 5620 SAM supports the template-based creation of rules. These rules are called policies. The types of policies are:

- service management
- routing management
- network management
- 7250 SAS and Telco
- OmniSwitch QoS
- OmniSwitch Ethernet services

A 5620 SAM operator can distribute or delete policies on sites and NEs that are within their span of control.

Policies are global or local in scope. Global policies are created using the 5620 SAM. Local policies are instances of global policies that are assigned to individual NEs. Depending on the distribution mode of a local policy, when you modify a global policy using the 5620 SAM, the local instance is also updated to ensure that the policy instances are synchronized. If a local policy differs from the corresponding global policy because of changes to the global policy, a warning alarm is raised against the local policy. After a global policy is updated and distributed to the participating NEs, the 5620 SAM clears the mismatch alarms associated with the local policy.

To identify local and global policy mismatches, you can perform a policy audit that compares the local and global instances of a policy, and then review the differences. An audit can be performed on local policies of NEs that are in the user span of control and policies that the user license supports.

You can audit all policies in the network or on selected NEs in the following ways:

- by policy group
- by policy type
- by global policy

If there is a mismatch between a local policy instance and the global instance, an alarm is raised against the local policy. The 5620 SAM clears the alarms from previous audits if the mismatch condition no longer exists.

Warning — Alcatel-Lucent recommends that you change a policy on an NE using only the 5620 SAM or an OSS client. This ensures that there is no mismatch in policy IDs or policy configurations between the managed NEs and the 5620 SAM.

Creating or modifying a policy using a CLI may lead to inconsistencies in the policy configuration throughout the network. See Procedure 43-8 for information about identifying policy discrepancies using a policy audit.

Depending on the results of an audit, the mode of the local policy may change. If the audit discovers differences between the local and global policies, you can change the mode to allow only local configuration. When the audit discovers that the local policy and global policy match, the local mode can be changed to synchronize with global policies. For example, when you need the 5620 SAM to discover new NEs, set the mode parameter to local configuration only to ensure that unique policies are not modified when a global policy is updated. The audit results can be reviewed to determine whether a policy should remain local.

The 5620 SAM supports the partial distribution of global policies. Before a global policy is distributed to the NEs, the 5620 SAM determines whether the global policy, policy properties, and the policy entries are applicable for each NE to which the policy is to be applied. If an NE does not support the policy, property, or entry defined in a global policy, the policy is partially distributed to the NE. The inapplicable policy, property, or entry is not distributed to the NE. An alarm is not raised if a policy is partially distributed. When you use the 5620 SAM GUI or OSS, failure of distribution to an NE does not affect distribution to other NEs.

Global policies are created in draft mode. This allows operators to verify that the policy is correctly configured before they distribute the policy to the NEs. The 5620 SAM creates a global policy in draft mode for newly discovered local policies. When the policy is approved for distribution, you can change the mode to released, which also distributes the policy to existing local definitions. The 5620 SAM saves the latest released version of the global policy. You can monitor policy distribution using the Task Manager. See Procedure 2-14 for information about the Task Manager.

When there is no global policy associated with a local policy, the 5620 SAM automatically creates a global policy that is identical to the first discovered local policy. If the local policy is incomplete, the 5620 SAM creates an incomplete global policy. The following read-only parameters describe the initialization phases of a global policy:

- Discovery State
  - In Progress—The global policy is created as part of a specific NE resynchronization during the full NE resynchronization or NE discovery. The global policy does not yet match any local policy and is waiting for completion.
  - Completed—At the end of the full NE resynchronization, when the resynchronization is successful, the global policy is completely updated from the first discovered local policy.
  - Failed—At the end of the full NE resynchronization, if the resynchronization is not successful, the global policy is not updated from the first discovered local policy. A failed global policy is updated during the next successful full NE resynchronization, or the policy can be manually synchronized with a specific local policy. The global policy remains in the Failed state after a 5620 SAM server failure or activity switch.
  - Initialize—The global policy is created by SNMP trap notification. The global policy may need to be manually synchronized with the specific local policy.
  - N/A (default)—The global policy is created or modified by a 5620 SAM user.

- Origin
  - Site ID—The global policy is created as part of a specific NE resynchronization or by SNMP notification.
  - User Name—The global policy is created by a 5620 SAM user.

Note 1 — If you attempt to modify a global policy with an "In Progress" Discovery State, the following occurs:

- When discovery or full resynchronization of the NE is ongoing, the modification fails.
- When discovery or full resynchronization of the NE is completed, modifications using OSS proceed, although a warning appears and allows you to cancel the modification. If the modification is not cancelled, the Discovery State is changed to N/A, and the global policy is not updated to match the local policy.
- When a global policy is modified, the Discovery State is reset to N/A.

Note 2 — At any time during discovery or a full resynchronization, you can use the SyncTo method from OSS or synchronize the global policy from any local policy.

When a discovery or full resynchronization of an NE fails and there is no 5620 SAM server failure or activity switch, all global policies that are waiting for completion are changed to Failed for the Discovery State. If you start another full resynchronization of the failed NE, the 5620 SAM tries again to complete the global policies from the NE that is part of the resynchronization and which has the Failed or In Progress Discovery State. The 5620 SAM also attempts completion of the synchronization of global policies that have a Failed or an In Progress State until a server failure or an activity switch occurs.

Table 43-1 describes the recommended operator actions to recover global policies when the Discovery State remains In Progress or Failed.

Table 43-1 Actions to recover global policies

Discovery State	5620 SAM server failure	NE state	Recovery action
In Progress/Failed	No	Resync Failed	Retry a full resynchronization or synchronization from another local policy
In Progress/Failed	No/Yes	Removed/Unmanaged	Synchronization from another local policy
In Progress/Failed	Yes	Resync Completed	Synchronization from another local policy
In Progress/Failed	Yes	Resync Failed	Retry a full resynchronization and synchronization from another local policy

The 5620 SAM supports the ability to scale policy deployment. If you release a large global policy to multiple NEs using one deployer, you may degrade system performance. An operator can configure the maximum number of objects that a deployer can send. The 5620 SAM uses this value to calculate how many NEs can be deployed per deployer. The default value is 10 000 objects per deployer. Table 43-2 provides an example of possible parameter settings to deploy a global policy that contains 1000 objects.

In the example below, there is one deployer per site. When the parameter setting is less than the number of entries in the policy, the 5620 SAM does not use more than one deployer for one site. If the parameter setting is too high, the 5620 SAM uses one deployer for all sites which may impact system performance. See Procedure 43-10 for more information about configuring the maximum number of objects per deployer.

Table 43-2 Example of policy deployment

Policy distribution maximum number of objects per deployer	number of objects in a global policy	Maximum number of sites per deployer
0	—	All sites
1	—	1 site
500	1000	1 site
1000	1000	1 site
5000	1000	5 sites
10 000	1000	10 sites
100 000	1000	100 sites

Service management policies specify how service traffic is handled by network resources such as interfaces, ports, daughter cards, and circuits. The policies can be used by multiple resources on multiple services. Service management policies include access ingress, access egress, MSAP policies, and network policies.

Routing management policies specify routing configuration according to specifically defined parameters. The 5620 SAM supports the following routing management policy types:

- routing
- MPLS administrative group
- VRRP priority control

Service and routing management policies are globally and seamlessly distributed to devices when they are used by resources on the device. They can also be manually distributed to devices. Subsequent changes to policies are distributed and affect all participating resources. Policy configurations can also be changed locally when you configure a network resource, for example, during service configuration or modification. These changes do not affect the global policy.

Network management policies specify how the 5620 SAM communicates with network resources, handles alarms, manages statistics, and stores information. Examples of network management policies are alarm, mediation, and accounting policies.

7250 SAS and Telco policies specify how 7250 SAS and Telco devices are configured and used to provide BTV VLAN, L2 VPN VLANs, and super-VLAN Internet services.

OmniSwitch QoS and Ethernet service policies specify how OmniSwitch devices are configured and used to provide VLAN and SVLAN services.

Time of day policies consist of time range policies and time of day suite policies. Time range policies specify multiple schedules (start and end dates and times) that you can assign to time of day suites or to ACL filter entries. A time of day suite policy is a collection of policies, such as ACL filters, access ingress and egress, and QoS schedulers, to which a time range policy has been assigned. In addition, you can assign time of day suite policies to aggregation schedulers and L2 and L3 access interfaces.

Table 43-3 describes the policies that are configured using the 5620 SAM. Unless otherwise stated in the table, the policies are described in more detail in this volume.

Table 43-3 5620 SAM Policy Types

Policy type	Policy	Applied to	Description	Menu option
Service management	Access Ingress	Access interface	Defines ingress classification, policing, shaping, and marking on the ingress side of the interface	Policies→QoS→SROS QoS→Access Ingress→Access Ingress
	7210 Access Ingress	Access SAP	Defines up to 18 forwarding class meters and meter parameters for traffic classification. Defines match criteria to map flows to the meters based on any one of the criteria (IP or MAC).	Policies→QoS→SROS QoS→Access Ingress→7210 Access Ingress
	Access Egress	Access interface	Defines egress classification, policing, shaping, and marking on the egress side of the interface	Policies→QoS→SROS QoS→Access Egress→Access Egress
	7210 Access Egress	Access port	Defines up to eight forwarding class queues and queue parameters for traffic classification. Defines forwarding class to remarking values. Maps forwarding classes to the queues.	Policies→QoS→SROS QoS→Access Egress→7210 Access Egress
	Network	Network interface	Defines egress QoS marking and ingress QoS interpretation for traffic on core network IP interfaces	Policies→QoS→SROS QoS→Network→Network
	7210 Network	Uplink port	Defines ingress Dot1p to forwarding class mapping and profile state. Defines the egress queuing parameters associated with each forwarding class.	Policies→QoS→SROS QoS→Network→7210 Network

(1 of 8)

Policy type	Policy	Applied to	Description	Menu option
Service management (continued)	7210 Network [(1)]	Network port [(1)]	Defines ingress Dot1p or DSCP value mapping to forwarding classes. Defines unicast meters. Only unicast meters with range 1-8 are allowed. Defines the egress forwarding class to Dot1p or DSCP value markings. Remarking of QoS bits.	Policies→QoS→SROS QoS→Network→7210 Network
		Network interface [(1)]	Defines ingress LSP-Exp value mapping to forwarding classes. Defines forwarding class to meter mapping. Defines unicast or multicast meter. Multicast meters are only supported for interface type policy. Defines the egress forwarding class to LSP-Exp value markings. Remarking of QoS bits.	
	Network Queue	Network daughter card Network port	Defines the default burst allocations for queues based on the queue's forwarding class	Policies→QoS→SROS QoS→Network Queue→Network Queue
	7210 Network Queue	Uplink port	Defines forwarding class mappings to network queues and queue characteristics for the queues	Policies→QoS→SROS QoS→Network Queue→7210 Network Queue
	Shared Queue	Network daughter card	Defines distribution of traffic over core network	Policies→QoS→SROS QoS→Shared Queue
	Slope	Access port Network daughter card Network port	Defines RED slope behavior	Policies→QoS→SROS QoS→Slope→WRED Slope Policies→QoS→SROS QoS→Slope→HSMDA WRED Slope
	7210 Slope	Access and uplink ports	Enables or disables the high-slope and low-slope parameters in the egress pool	Policies→QoS→SROS QoS→Slope→7210 Slope
	Scheduler	Access ingress interface Access egress interface	Defines hierarchical rate limiting and scheduling to govern queue scheduling	Policies→QoS→SROS QoS→Scheduler→Scheduler Policies→QoS→SROS QoS→Scheduler→HSMDA Scheduler
	Port Scheduler	Egress ports and channels	Defines hierarchical bandwidth allocation and scheduling at the egress port level	Policies→QoS→SROS QoS→Scheduler→Port Scheduler
	7210 Port Scheduler	Access and uplink ports	Defines the parameters for the port scheduler	Policies→QoS→SROS QoS→Scheduler→7210 Port Scheduler
	Policer Control	Ingress or egress SAPs Subscriber Contexts	Provides control hierarchy for policer objects configured on SAPs or subscriber contexts	Policies→QoS→SROS QoS→Scheduler→Policer Control
	Named Pool Buffer	Network daughter card and network port	Allows the operator to override the default pool allocation behavior	Policies→QoS→SROS QoS→Buffer Pool→HSMDA Pool Policies→QoS→SROS QoS→Buffer Pool→Named Buffer Pool

(2 of 8)

Policy type	Policy	Applied to	Description	Menu option
Service management (continued)	Ingress Queue Group Template	Access interface	Used for Access Ingress Queue Group creation on Ethernet access ports	Policies→QoS→SROS QoS→Queue Group→Ingress Template
	Egress Queue Group Template	Access interface	Used for Access Egress Queue Group and Network Egress Queue Group creations on Ethernet ports	Policies→QoS→SROS QoS→Queue Group→Egress Template
	Ethernet CFM	Ethernet services	Defines the Maintenance Domain for Ethernet services (VPLS, EPIPE, VPRN and IES) including SAP and SDP bindings	Tools→Ethernet CFM→Maintenance Domain
	802_1X	Ethernet ports	Defines the RADIUS server authentication policy for Ethernet ports	Policies→Layer2→802_1x
	ACL IP Filter	Network interface Access interface Circuit	Controls network traffic into or out of an interface or circuit based on IPv4 matching criteria	Policies→Filter→ACL IP Filter
	ACL IPv6 Filter	Network interface Access interface Circuit	Controls network traffic into or out of an interface or circuit based on IPv6 matching criteria	Policies→Filter→ACL IPv6 Filter
	ACL MAC Filter	Access interface Circuit	Controls network traffic into or out of an interface or circuit based on MAC matching criteria	Policies→Filter→ACL MAC Filter
	ATM QoS	Access interface	Defines ATM ingress and egress classification, policing, shaping, and marking	Policies→QoS→SROS QoS→ATM QoS
	9500 MPR QoS	Access interface	Defines ATM classification, policing, and marking	Policies→QoS→9500 MPR QoS→9500 ATM QoS
	Multicast Package	VPLS instance	Assigns a common set of multicast groups to all 7450 ESSs or 7750 SRs in an MVR VPLS. See chapter 68 for more information.	Policies→Multicast→Multicast Package
	Egress Multicast Group	VPLS instance	Creates an EMG to which SAPs can be applied on the access port of a VPLS	Policies→Multicast→Egress Multicast Group
	Subscriber identification	SAP	Associates residential subscriber hosts with subscribers for the allocation of network resources. See chapter 64 for more information.	Policies→Residential Subscriber
	Policy Sync Group	AA Group Policy	Designate an AA group policy as the master policy and add one or more AA group policies to Policy Sync Group members. Overwrite or add the contents of the master policy to one or more of its members. See chapter 73 for more information.	Policies→Policy Sync Group
	MC MLPPP Ingress QoS Profile	APS and ASAP MLPPP bundles	Create and configure user-defined ingress QoS profiles for MC MLPPP bundles.	Policies→QoS→SROS QoS→MLPPP→Ingress QoS Profile

(3 of 8)

Policy type	Policy	Applied to	Description	Menu option
Service management (continued)	MC MLPPP Egress QoS Profile	APS and ASAP MLPPP bundles	Create and configure user-defined egress QoS profiles for MC MLPPP bundles.	Policies→QoS→SROS QoS→MLPPP→Egress QoS Profile
	MCFR Ingress QoS Profile	MLFR bundles	Create and configure user-defined ingress QoS profiles for MLFR bundles.	Policies→QoS→SROS QoS→MCFR→MLFR Ingress QoS Profile
	MCFR Egress QoS Profile	MLFR bundles	Create and configure user-defined egress QoS profiles for MLFR bundles.	Policies→QoS→SROS QoS→MCFR→MLFR Egress QoS Profile
Auto tunnel management	Manage rule-based tunnels	—	Create and configure rule-based tunnel policies	Policies→Auto Tunnels→Rule-Based Groups
	Manage auto tunnel rules	—	Create and configure auto-tunnel rules	Policies→Auto Tunnels→Auto Tunnel Rules

(4 of 8)

Policy type	Policy	Applied to	Description	Menu option
Routing management	Routing	Routing instance	Manages route policies. See chapter 27 for more information.	Policies→Routing→Statement Policies→Routing→Prefix List Policies→Routing→Community Policies→Routing→Damping Policies→Routing→AS Path
	IKE Policy	IPsec tunnels IPsec gateways	Create and configure IKE policies. See chapter 32 for more information.	Policies→ISA Policies→IKE
	ISA-IPSec Transform	IPsec tunnels IPsec security associations IPsec tunnel templates	Create and configure IPsec transform policies. See chapter 32 for more information.	Policies→ISA Policies→IPSec Transform
	ISA-IPSec Static Security Association	OSPFv3 interfaces Virtual links	Create and configure IPsec static security association policies. See chapter 32 for more information.	Policies→IPSec Static Security Association
	ISA-IPSec Tunnel Template	IPsec gateways	Create and configure IPsec transform policies. See chapter 32 for more information.	Policies→IPSec Tunnel Template
	Admin Group (MPLS)	MPLS interfaces LSPs LSP paths	Configures MPLS administrative groups and defines the groups to which an MPLS interface, LSP, or LSP path belongs. See chapter 27 for more information.	Policies→MPLS→ Administrative Group
	LSP Template MVPN (MPLS)	P2MP LSPs	Configures and manages P2MP LSPs. See chapters 28 and 29 for more information.	Policies→MPLS→LSP Template MVPN
	Shared Risk Link Group (MPLS)	MPLS interfaces LSP paths	Configures Shared Risk Link Groups and associates the groups to one or more MPLS interfaces. See chapters 27 and 29 for more information.	Policies→MPLS→ Shared Risk Link Group
	NAT	Routing instances	Create and configure NAT for use in IES and VPRN services.	Policies→ISA Policies→NAT Policy
	VRRP	VRRP instance	Applies a VRRP priority-control policy to non-owner VRRP instances in a virtual router. See chapter 36 for more information.	Policies→VRRP
Routing management (continued)	PW Template	PE routers used for VPLS services	Enables a VPLS PE router to discover the other PE routers that are part of the same VPLS domain or in another BGP VPLS.	Manage→Service→Service PW Template

(5 of 8)

Policy type	Policy	Applied to	Description	Menu option
Network management	Alarm	Alarm logs Alarms	Defines how the 5620 SAM handles individual incoming alarms, and how alarm logs are created and stored. See chapter 34 for more information.	Administration→Alarm Settings
	File	—	Manages files on the device. See the *5620 SAM Statistics Management Guide* for more information.	Tools→Statistics→File Policies
	Accounting	Network interface Access interface Circuit	Manages accounting policies. See the *5620 SAM Statistics Management Guide* for more information.	Tools→Statistics→Accounting Policies
	NE Deployment, Backup, Software Upgrade	5620 SAM	Defines how the 5620 SAM communicates with the network. See chapter 21 for more information.	Administration→NE Maintenance
	Mediation	5620 SAM	Defines how the 5620 SAM polls the network. See chapter 13 for more information.	Administration→Mediation
	Remote Network Management	5620 SAM	Maps remote network monitoring events to information alarms in the 5620 SAM GUI.	Tools→Remote Network Management (RMON)
7250 SAS and Telco management	Multicast Package	Broadcast TV VLAN services	Defines the set of broadcast channels that are multicast across a ring group in a BTV VLAN. See chapter 65 for more information.	Policies→Multicast→Multicast Package
	7250 SAS and Telco Node QoS Level	7250 SAS and Telco devices and ports	Defines QoS policies applied to a 7250 SAS or Telco device. See chapter 65 for more information.	Policies→QoS→7250 SAS and Telco QoS
	7250 SAS and Telco ACL Standard IP	7250 SAS and Telco devices and ports	Controls network traffic on 7250 SAS or Telco VLANs based on IP address and subnet mask matching criteria. See chapter 65 for more information.	Policies→Filter→ 7250 SAS and Telco ACL Standard IP Filter
	7250 SAS and Telco ACL Extended IP	7250 SAS and Telco devices and ports	Controls network traffic on 7250 SAS or Telco VLANs based on several IP matching criteria. See chapter 65 for more information.	Policies→Filter→7250 SAS and Telco ACL Extended IP Filter
	7250 SAS and Telco ACL IGMP	7250 SAS and Telco devices and ports	Manages how BTV host devices access multicast BTV streams. See chapter 65 for more information.	Policies→Filter→7250 SAS and Telco ACL IGMP Filter
	7250 SAS and Telco ACL MAC	7250 SAS and Telco devices and ports	Controls network traffic on 7250 SAS or Telco VLANs based on MAC matching criteria. See chapter 65 for more information.	Policies→Filter→7250 SAS and Telco ACL MAC Filter

(6 of 8)

Policy type	Policy	Applied to	Description	Menu option
OmniSwitch policies	QoS	VLAN and stacked VLAN services	QoS policies are used for traffic prioritization, bandwidth shaping, and Layers 2, 3, and 4 filtering.	Policies→QoS→AOS QoS Policies
	Ethernet Service	SAPs and UNI ports	A SAP is associated with a stacked VLAN service. A SAP profile defines values for ingress bandwidth sharing, rate limiting, customer VLAN tag processing (translate or preserve), and priority mapping (inner to outer tag or fixed value). A UNI profile is associated with a UNI port and configures how a variety of protocol control packets are processed on the UNI port. Processing actions include Tunnel, Drop, Peer, and MAC Tunnel.	Policies→Layer 2→AOS Ethernet Service
RADIUS-based Accounting	RADIUS Accounting Policy	Subscriber profiles	Sends accounting information to the RADIUS server when a subscriber logs in or logs out of a session	Policies→RADIUS Based Accounting
Diameter policy	Diameter	Residential Subscriber	Specifies common diameter protocol parameters to be inherited by associated diameter peers.	Policies→Residential Subscriber
Time of day policies	Time Range	Time of day suite policy entries and ACL filter policy entries	Specifies multiple schedules that can be used by time of day suite policies or ACL filter policies	Policies→Time of Day→Time Range
	Time of Day Suite	Aggregation scheduler policies and L2 and L3 access interfaces	A collection of policies, such as ACL filters, access ingress and egress, and QoS schedulers, to which time range policies have been assigned	Policies→Time of Day→Time Of Day Suite
MSAP policy	MSAP	Capture SAPs L2 access interfaces MSAPs L2 and L3 access interfaces	Specifies how parameters are applied in the creation of an MSAP.	Policies→Residential Subscriber
IGMP policy	IGMP	Subscriber profile	Associates subscriber profiles with static multicast group and static source IP addresses.	Policies→Residential Subscriber
BGP Peering policy	BGP Peering	Residential subscriber host	Applies BGP peering configuration to residential subscriber host.	Policies→Residential Subscriber
RCA audit policies	RCA Audit Policy	VLL, VPLS, and VPRN services and physical links	Associates RCA audit policies to VPRN, VPLS, and VLL services and to physical links. See chapter 77 for more information.	Policies→Network and Service Audits

(7 of 8)

Policy type	Policy	Applied to	Description	Menu option
Format and range policies	Format Policy	All services, LSPs, L2 and L3 access interfaces	Specifies the text format of names and descriptions of services, LSPs, L2 and L3 access interfaces. Format policies must be associated with users and user groups.	Administration→Format and Range
	Range Policy	All services, LSPs, L2 and L3 access interfaces	Specifies the ID number range for services, LSPs, L2 and L3 access interfaces. Range policies must be associated with users and user groups.	
7705 SAR Fabric Profile policy	7705 SAR Fabric	Daughter cards on the 7705 SAR	7705 SAR Fabric Profile policies specify the fabric shaping rate (kb/s) to the daughter card in the slot specified by the rate.	Policies→QoS→SROS QoS→7705 SAR Fabric

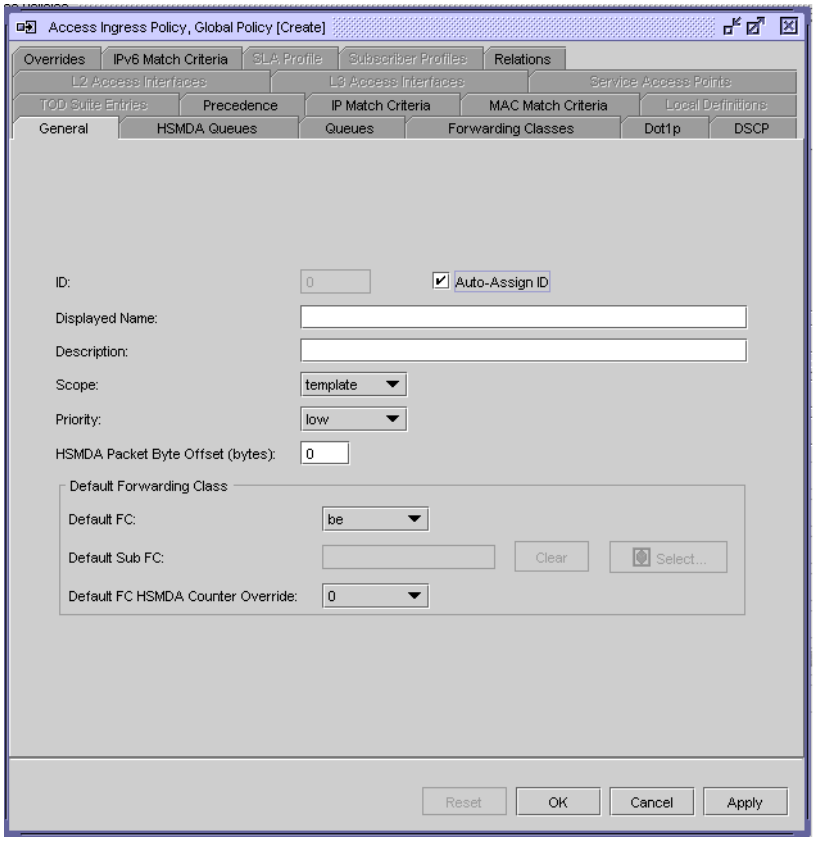
(8 of 8)

Note

(1) Applies to the 7210 SAS-M24F, Release 1.1 R4 or later, 7210 SAS-M24F2XFP, and 7210 SAS-M24F2XFP [ETR].

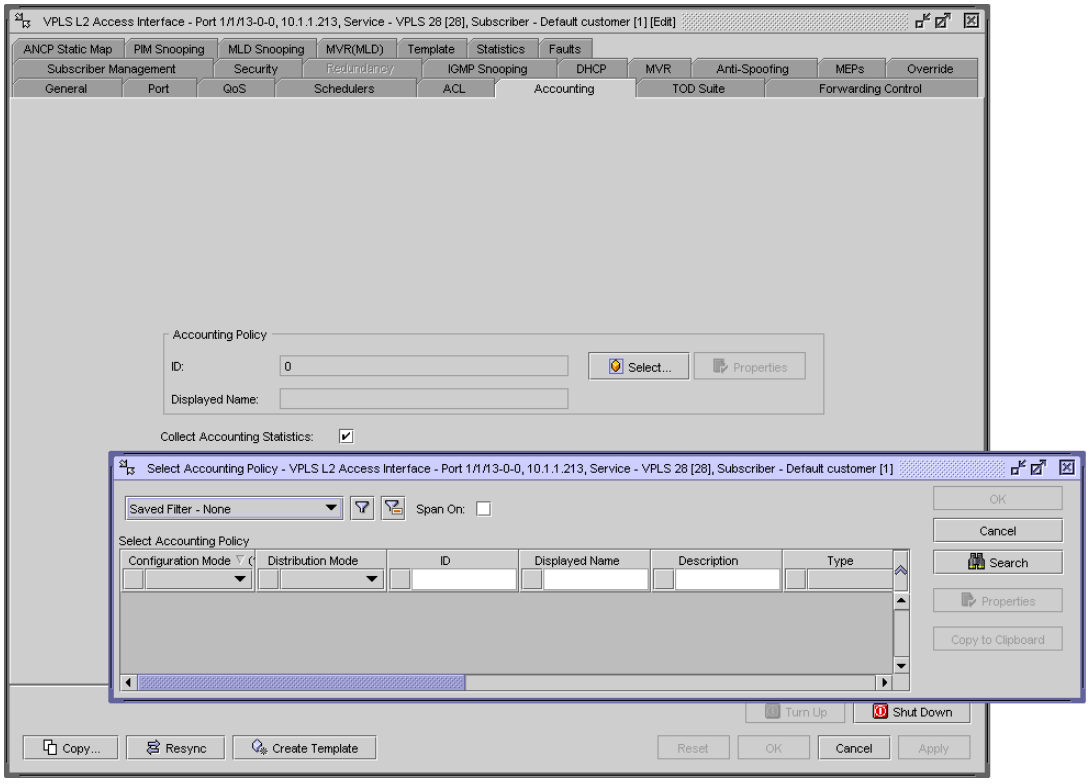
The 5620 SAM supports the creation and modification of policies using configuration forms. For example, Figure 43-1 shows the Access Ingress Policy creation form with the General tab displayed. Standard parameters such as Displayed Name and Description, as well as parameters specific to the policy type, appear on the form.

Figure 43-1 Access Ingress Policy creation form - General tab



You can apply policies to resources during service creation or modification. You can also apply policies to resources before or after configuring the service by choosing and modifying the resource from the Manage Equipment or Manage Services form. Figure 43-2 shows the Select Accounting Policy form that opens during L2 Interface configuration.

Figure 43-2 Create L2 Access Interface form - Select Accounting Policy step



Policy distribution

The 5620 SAM supports the template-based creation of rules which are called policies. The types of policies are:

- service management
- routing management
- network management
- 7250 SAS and Telco
- OmniSwitch QoS
- OmniSwitch Ethernet services

43.2 Workflow to create and assign policies

1 Create the required policies.

2 Distribute the policies.

Note 1 — You do not need to explicitly distribute a policy; a policy is distributed to a device when it is assigned to a resource on the device.

Note 2 — When you distribute a policy to a 7705 SAR, all values within that policy must be supported by that 7705 SAR; otherwise, the distribution of the policy to that 7705 SAR is blocked.

3 Assign policies to resources during service configuration or modification.

43.3 Policies procedures

Use the following procedures to perform 5620 SAM policies tasks.

Procedure 43-1 To distribute a policy

Use this procedure to manually distribute policies used by network resources and to configure the distribution mode of local policies. Policies are also distributed to a device when the policy is assigned to a resource on that device.

When you distribute a global policy, local policies using the Sync With Global distribution mode allow the NE to receive the policy.

Note — Local policies using the Local Edit Only distribution mode do not allow the NE to receive the distribution of a global policy. You must ensure that the policy distribution mode for the local policy is set to Sync With Global if you want the NE to receive the distribution of a global policy.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to distribute. The appropriate policies manager form opens.

2 Choose Global from the Policy scope drop-down menu.

3 Click on the Search button.

4 Choose the policy or policies that you want to distribute.

5 When the policy is in draft configuration mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution by performing one of the following:

   a To release a from a *Policy_Type* Global (Edit) form, click on the Properties button. The *Policy_Type* Global (Edit) form opens.

   b To release a policy from a policies manager form, click on the Release button. Go to step 10.

   c If the policy has previously been released, go to step 10.

Warning — When you switch the configuration mode of the global policy to released, the policy is distributed to existing local definitions.

6 Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears.

7 Click on the Yes button. The policy configuration mode changes to Released.

8 View the local policy, if necessary, by clicking on the Local Definitions tab button and double-clicking on the local policy in the list.

9 Close the local policy form.

10 Click on the Distribute button. The Distribute form opens.

11 Select one or more rows in the Available Nodes list.

12 Click on the right arrow button. The chosen site or sites move to the Selected Nodes panel on the right side of the form.

13 Click on the Distribute button. The policy is distributed to the site or sites.

Note — Distribution failures are reported in a pop-up message. You can view the error message to determine the cause of the failure and which NE or NEs were affected. Distribution failures are also reported using JMS.

14 Close the Distribute form. The policy manager form reappears.

15 View the devices to which a policy is distributed.

   i Choose the policy.

   ii Click on the Properties button. The policy form opens.

   iii Click on the Local Definitions tab button. The device information for the chosen policy is displayed.

16 Configure the distribution mode of the local definitions by performing the following:

i Click on the Distribution Mode button. The Distribution Mode - *Policy* form opens.

ii Choose Sync With Global, Local Edit Only, or All from the Distribution Mode parameter drop-down menu. The sites that are configured with the selected distribution mode are listed.

iii Choose one ore more rows from the Available Nodes list.

iv Click on the right arrow button. The chosen site or sites move to the Selected Nodes panel on the right side of the form.

v Depending on the distribution mode of the chosen site or sites, perform one of the following steps:

- Click on the Sync With Global button.
- Click on the Local Edit Only button.

vi Close the Distribution Mode - *Policy* form. The policy manager form reappears.

17 To distribute additional policies, perform steps 4 to 15.

Procedure 43-2 To modify a policy

Use this procedure to change existing policies and entries within policies using the 5620 SAM client GUI. Alternatively, you can use the CLI. The changes are applied immediately to all resources where the policy is applied.

When you modify policy match criteria, for example, the IP match criteria for an access ingress policy, click on the Refresh button to ensure that the 5620 SAM client GUI displays the latest set of match criteria.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to edit.

The Manage *Policy Type* form opens.

2 Choose Global from the Policy scope drop-down menu.

3 Click on the Search button. A list of search results is displayed on the form.

4 Choose the policy that you want to edit.

5 Click on the Properties button. The policy configuration form opens.

6 Perform one of the following:

a If the configuration mode of the policy is set to Released, go to step 7

b If the configuration mode of the policy is set to Draft, configure the parameters, as required, and go to step 13.

7 Configure the parameters, if required. When you modify the configuration, the 5620 SAM changes the configuration mode of the policy to Draft.

8 When you modify filter entries for policies with filters, click on the appropriate tab button and click on the Refresh button to list the filter entries.

9 Click on the Apply button. A dialog box appears.

10 Click on the Yes button.

11 Perform one of the following steps:

a Compare the global policy with the existing local definitions to verify whether you need to reset the policy configuration to the previously released global policy configuration. Perform steps 8 to 10 of Procedure 43-9.

b Go to step 12.

12 Perform one of the following steps:

a Click on the Reset to Released button to reset the global policy configuration to the last released configuration of the policy and to cancel any modifications you entered in step 7. Go to step 15.

b Go to step 13.

13 Click on the Switch Mode button beside the Configuration Mode parameter to release the policy for distribution, if required. A dialog box appears.

14 Click on the Yes button. The policy is distributed to existing local definitions.

15 Click on the Local Definitions tab button to view the local instances of the global policy.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The policy configuration form closes and the policy manager form reappears.

18 Close the policy manager form.

Procedure 43-3 To delete a policy

Each service SAP and network interface is associated, by default, with the appropriate ingress, egress, or network policy (ID 1). You can replace the default policy with a customer-configured policy, but you cannot entirely remove a QoS policy. When you remove a QoS policy from a SAP or IP interface, the policy association reverts to the default policy (ingress or egress policy ID 1). The default policy cannot be deleted.

A QoS or ACL policy cannot be deleted until it is removed from the all SAPs or network ports where it is applied. When a policy is deleted, it is removed from the 5620 SAM, including the database and all devices.

Do not delete a routing policy from an NE that is associated with one or more services. Multiple services on the NE may use the policy.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to delete.

The Manage *Policy Type* form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. A list of search results is displayed in the bottom panel of the form.

4 Choose the policy that you want to delete.

5 Click on the Delete button. A dialog box appears.

6 Click on the Yes button. The policy configuration form closes and the policy manager form reappears. The policy is removed from the policy list.

Procedure 43-4 To copy or overwrite a policy

You can copy an existing QoS policy, rename the policy with a new QoS policy ID, or overwrite an existing policy ID.

1 Choose Policies→*QoS*→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to copy or overwrite.

The Manage *Policy Type* form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. A list of search results is displayed.

4 Choose the policy that you want to copy or overwrite. The Policy Type (Edit) form opens.

5 Click on the Copy button. The Policy Type (Create) form opens.

6 Configure the parameters as required.

7 Click on the Ok button. The Policy Type (Create) form closes and the Policy Type (Edit) reappears.

8 Close the Policy Type (Edit) form. The Manage *Policy Type* form reappears. The new policy is displayed in the list.

9 Close the Manage *Policy Type* form.

Procedure 43-5 To synchronize a policy

You can use the synchronize function to specify the local policy entry as global and redistribute it across all deployed associations. For example, if a policy is distributed to a wide range of devices and on one of these devices the policy was changed, you can use the synchronize command to synchronize the policy on the device and on the 5620 SAM. You must then distribute the policy to all participating devices, as described in Procedure 43-1.

Note — When you synchronize a policy that is in draft mode, the policy is not distributed to existing local definitions. When you synchronize a policy that is in released mode, the 5620 SAM sets the policy to draft mode. You must set the Configuration Mode parameter to Released to distribute the policy to existing local definitions. Only local policies that have the Distribution Mode parameter set to Sync With Global are affected.

1 Choose Policies→*Policy Type* from the 5620 SAM main menu, where *Policy Type* is the type of policy that you want to synchronize.

The Manage *Policy Type* form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. A list of search results is displayed.

4 Choose the policy or policies that you want to synchronize.

5 Click on the Synchronize button. The Synchronize form opens.

6 Choose the device to which the policy is to be synchronized from the Available Nodes list.

7 Click on the right arrow button. The chosen device moves to the panel on the right side of the form.

8 Click on the Synchronize button.

9 Click on the Cancel button to close the form.

Procedure 43-6 To perform a policy audit for policy groups and types

An audit compares all local policies with the associated global policies. A policy audit can be performed on all NEs in the network, or limited to a specific NE or group of NEs. All NEs are included in the audit unless they are explicitly chosen. A policy audit can be performed on policy groups and policy types. A policy audit cannot be started when another policy audit is in progress.

Note — Validation is performed to prevent policies from being audited if licensing and span of control prohibits.

If a user performs an audit on objects that are not within their span of control, or they do not have licensing permissions, the audit is aborted and a error message opens. The error message indicates which objects are prohibited.

Caution — If policy types, global policies are not specified, all policies for which the user has licensing permissions are included in the policy audit.

If NEs are not specified, all NEs that are in the user's span of control are included in the policy audit.

Performing a policy audit may take one or more hours to complete.

1 Choose Tools→Policies Audit from the 5620 SAM main menu. The Policy Audit - audit status (Edit) form opens with the General tab displayed.

2 Configure the parameters:

- Include Non Applicable Attributes
- Set to "Local Edit Only" upon finding of differences
- Set to "Sync with Global" upon finding of no differences

Note — The Set to "Local Edit Only" upon finding of differences and Set to "Sync with Global" upon finding of no differences parameters are configurable when the Include Non Applicable Attributes parameter is set to disabled.

3 Perform one of the following steps:

a To choose policy groups and policy types to be included in the audit, go to 4.

b If all policy groups and policy types are included in the audit, go to step 10 to set which NEs to include in the audit.

c If all policy groups and policy types and the entire network is included in the audit, go to step 11.

4 Click on the Policy Group Selection tab button.

5 Right-click on the Policy Audit icon and choose Select Policy Groups from the contextual menu. The Select Policy Groups form opens.

6 Select policy groups as required and click on the OK button. The chosen policy group keys appear below the Policy Audit icon.

7 Perform one of the following steps:

a If all policy types within the selected groups are included in the audit, go to step 10.

b To choose which policy types within the selected groups are included in the audit, go to step 8.

8 Right-click on a policy group icon and choose Select Policy types from the contextual menu. The Select Policy types - Policy Audit form opens.

9 Select policy types as required and click on the OK button. The chosen policy type icons appear below the Policy Audit icon.

10 Select NEs to include in the audit, if required.

i Click on the Network Element Selection tab to select an NE, or group of NEs to be audit.

ii Click on the Add button. The Select Site form opens.

iii Click on the Search button. A list of NEs is displayed.

iv Click on the NEs to be included in the audit.

v Click on the OK button. The Policy Audit *audit_status* (Edit) form refreshes to display a list of NEs.

11 Click on the Start Audit button.

To interrupt the audit while it is in progress, click on the Stop Audit button.

12 Close the Policy Audit form after the audit finishes.

13 A discrepancy between a global policy and a local instance of the policy generates an alarm. Monitor the dynamic alarm form to view alarms that are generated as a result of the policy audit.

Note — The distribution mode of a local policy may change depending on the parameters set in step 2.

14 Double-click on the alarm in the alarm form. The Alarm Info form opens.

15 Click on the View Alarmed Object button. The Global Policy (Edit) form opens.

16 Perform steps 8 and 12 of Procedure 43-9 to locate the discrepancies between the local and global policies.

17 Close the local and global *Policy_type* (Edit) forms.

Procedure 43-7 To perform a policy audit for multiple global policies with same type

An audit compares all local policies with the associated global policies. A policy audit can be performed on all NEs in the network, or limited to a specific NE or group of NEs. All NEs are included in the audit unless they are explicitly chosen. A policy audit can be performed on one or multiple global policies with the same type. A policy audit cannot be started when another policy audit is in progress.

Note — Validation is performed to prevent policies from being audited if licensing and span of control prohibits.

If a user performs an audit on objects that are not within their span of control, or they do not have licensing permissions, the audit is aborted and a error message opens. The error message indicates which objects are prohibited.

Caution — If NEs are not specified, all NEs that are in the user's span of control are included in the policy audit.

1 Choose Policies→ *Policy_Type* from the 5620 SAM main menu, where *Policy_Type* is the type of policy that you want to audit. The appropriate policies manager form opens.

2 Click on the Search button. A list of policies is displayed.

3 Choose one or multiple policies in the list.

4 Click on the Policy Audit button. A Policy Audit (Edit) form opens with the Global Policy Selection tab displayed and the selected policies listed.

5 Click on the Add button. The Select Policies form opens, displaying a list of global policies to be audited.

6 Select a policy or multiple policies in the list.

7 Click on the OK button. The Policy Audit (Edit) form is refreshed with the selected policies.

8 Click on the General tab button.

9 Configure the parameters:

- Include Non Applicable Attributes
- Set to "Local Edit Only" upon finding of differences
- Set to "Sync with Global" upon finding of no differences

Note — The Set to "Local Edit Only" upon finding of differences and Set to "Sync with Global" upon finding of no differences parameters are configurable when the Include Non Applicable Attributes parameter is set to disabled.

10 Perform one of the following:

- **a** To audit selected global policies on the entire network, go to step 12.
- **b** To audit selected global policies on selected NEs go to step 11.

11 Select NEs to include in the audit, if required.

- **i** Click on the Network Element Selection tab to select an NE, or group of NEs to be audit.
- **ii** Click on the Add button. The Select Site form opens.
- **iii** Click on the Search button. A list of NEs is displayed.
- **iv** Click on the NEs to be included in the audit.
- **v** Click on the OK button. The Policy Audit (Edit) form refreshes to display a list of NEs.

12 Click on the Start Audit button to proceed with the policy audit.

To interrupt the audit while it is in progress, click on the Stop Audit button.

13 A discrepancy between a global policy and a local instance of the policy generates an alarm. Monitor the dynamic alarm window to view alarms that are generated as a result of the policy audit.

14 Double-click on the alarm in the alarm window. The Alarm Info form opens.

15 Click on the View Alarmed Object button. The Global Policy (Edit) form opens.

16 Perform steps 8 and 12 of Procedure 43-9 to locate the discrepancies between the local and global policies.

17 Close the local and global *Policy_type* (Edit) forms.

Procedure 43-8 To perform a policy audit for global policy

An audit compares all local policies with the associated global policy. A policy audit can be performed on all NEs in the network, or limited to a specific NE or group of NEs. All NEs are included in the audit unless they are explicitly chosen. A policy audit cannot be started when another policy audit is in progress.

Caution — If NEs are not specified, all NEs that are in the user's span of control are included in the policy audit.

Note — Validation is performed to prevent policies from being audited if licensing and span of control prohibits.

If a user performs an audit on objects that are not within their span of control, or they do not have licensing permissions, the audit is aborted and a error message opens. The error message indicates which objects are prohibited.

1 Choose Policies→ *Policy_Type* from the 5620 SAM main menu, where *Policy_Type* is the type of policy that you want to audit. The appropriate policies manager form opens.

2 Click on the Search button. A list of policies is displayed.

3 Select a policy in the list.

4 Click on the properties button. The *Policy_Name* Global Policy (Edit) form opens.

5 Click on the Local Definitions tab button. A list of local policies is displayed.

6 Perform one of the following:

a To audit a specific local policy or a group of local policies, go to step 7.

b If all local policies in the list are included in the audit, go to step 8.

7 Select one or multiple local policies that you want to include in the audit.

8 Click on the Policy Audit button. A Policy Audit (Edit) form opens with the Network Element Selection tab displayed and a list of NEs corresponding to the selected local policies.

9 Click on the General tab button.

10 Configure the parameters:

- Include Non Applicable Attributes
- Set to “Local Edit Only” upon finding of differences
- Set to “Sync with Global” upon finding of no differences

Note — The Set to “Local Edit Only” upon finding of differences and Set to “Sync with Global” upon finding of no differences parameters are configurable when the Include Non Applicable Attributes parameter is set to disabled.

11 Click on the Start Audit button. To interrupt the audit while it is in progress, click on the Stop Audit button.

12 A discrepancy between a global policy and a local instance of the policy generates an alarm. Monitor the dynamic alarm window to view alarms that are generated as a result of the policy audit.

13 Double-click on the alarm in the alarm window. The Alarm Info form opens.

14 Click on the View Alarmed Object button. The Global Policy (Edit) form opens.

15 Perform steps 8 and 12 of Procedure 43-9 to locate the discrepancies between the local and global policies.

16 Close Global Policy *Policy_type* (Edit) form.

Procedure 43-9 To identify differences between a global and local policy or two local policies

Note — You can cancel the local audit at any time by clicking on the Local Audit Off button on the *Policy_type* (Edit) form.

1 Choose Policies→*Policy_type* from the 5620 SAM main menu, where *Policy_type* is the type of policy that you want to open and search for global and local differences. The Manage *Policy_type* form opens.

2 Choose Local from the Policy scope drop-down menu.

3 Click on the Select button beside the Local Node IP Address parameter. The Select a Network Element form opens.

4 Select a device in the list and click on the OK button. The Select a Network Element form closes and the Manage *Policy_type* form is updated with the NE IP address.

5 Click on the Search button. A list of search results is displayed.

6 Choose the local policy that you want to compare with another policy.

7 Click on the Properties button. The *Policy_type* (Edit) form opens.

8 Click on the Local Audit On button. The Local Audit form opens.

9 From the Policy scope drop-down menu:

- **a** Choose Global and go to step 11.
- **b** Choose Local and configure the Local Node IP Address parameter by using the Select button to choose a NE. The Select a Network Element form opens.
  - **i** Select an NE and click on the OK button. The Select a Network Element form disappears, and the policy manager form reappears with a list of the local policies for the chosen NE in the bottom panel.
  - **ii** Go to step 11.

10 Click on the OK button. The Local Audit form closes.

11 Perform one of the following steps:

a View the differences between the policies by clicking on the tab buttons that are highlighted with an arrow icon to indicate that differences exist on the policy forms. An arrow icon beside a property indicates that the property is modified. In lists, new entries are highlighted in pink and modified entries are highlighted in purple.

b Click on the Tree tab button on the local or global policy form. New items are highlighted in pink text. Modified items in the tree are highlighted in purple text.

12 Close the local and global *Policy_type* (Edit) forms.

Procedure 43-10 To configure the maximum policy objects per deployer

Perform this procedure to specify the maximum number of NEs to which a policy is distributed by one deployer.

Caution — Configure only the parameters specified in this procedure. Unauthorized configuration of the nms-server.xml file can seriously affect network management and degrade 5620 SAM performance.

1 Log in to the 5620 SAM main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory or folder, which is typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Search for the following XML tag:

```
<policyConfig policyDistributionMaxObjectsPerDeployer="10000"/>
```

6 Change the number, as required. A zero value or a negative number specifies one deployer or all sites, respectively. A one value specifies one deployer per site. The default is 10 000. Alcatel-Lucent recommends that you configure the value between 2000 and 100 000.

If the <numberOfObjectsPerPolicy> is greater than or equal to the <policyDistributionMaxObjectsPerDeployer> one deployer per site is used.

If the <numberOfObjectsPerPolicy> is less than the <policyDistributionMaxObjectsPerDeployer> the maxNumberOfSitesPerDeployer is calculated by policyDistributionMaxObjectsPerDeployer divided by the numberOfObjectsPerPolicy.

7 Save and close the nms-server.xml file.

44 — QoS policies

44.1 QoS policies overview

QoS policies define how network traffic is shaped and queued on one or more NEs. You can use the 5620 SAM to create QoS policies that regulate data throughput on the following:

- equipment, for example, ports and MDAs
- routing and forwarding points, for example, access and network interfaces

Access ingress policies

Access ingress policies are applied to access interfaces and specify QoS on ingress.

Access ingress policies define ingress service forwarding class queues and map flows to those queues. When an access ingress policy is created, it always has two queues defined that cannot be deleted: one for the default unicast traffic and one for the default multipoint traffic. These queues exist within the definition of the policy. The queues only get instantiated in hardware when the policy is applied to an access interface. In the case where the service does not have multipoint traffic, the multipoint queue is not instantiated.

In the simplest access ingress policy, all traffic is treated as a single flow and mapped to a single queue, and all flooded traffic is treated with a single multipoint queue.

The required access ingress policy elements include:

- a unique access ingress policy ID
- an exclusive scope for one-time use, or a template scope for use with multiple SAPs and interfaces
- at least one default unicast forwarding class queue
- at least one multipoint forwarding class queue

The optional access ingress policy elements include:

- additional unicast queues up to a total of 8 for each of the 8 forwarding classes
- 8 HSMDA queues that are automatically created when the policy is created; HSMDA queues are only used by HSMDA SAPs
- additional multipoint queues up to 3 per forwarding class for each type of multipoint traffic (broadcast, multicast and destination unknown unicast)
- QoS policy match criteria to map packets to a forwarding class
- A policer to control traffic flow rate.

Each queue can have unique queue parameters to allow individual policing and rate shaping of the flow mapped to the forwarding class. Mapping flows to forwarding classes is controlled by comparing each packet to the match criteria in the policy.

There is one default access ingress policy. The default policy gives all traffic equal priority with the same chance of being sent or dropped during periods of congestion.

Note — The 5620 SAM supports the configuration of HQoS scheduling mechanisms. HQoS provides the ability to rate limit across multiple queues from either single or multiple access interfaces for a specific customer. The building blocks for HQoS include access ingress, access egress, and scheduler policies.

See section 60.6 for a sample service configuration using HQoS.

Policy override

You can override some or all settings associated with an access ingress policy on an L2 or L3 access interface, SLA profile, or subscriber profile.

Note — You can override Access Ingress policies that have the Scope parameter set to template. See Procedure 44-1 for more information.

Forwarding classes

The 5620 SAM supports the configuration of eight forwarding classes and class-based queuing or policing on the managed devices. Each forwarding class is only important in relation to other forwarding classes. A forwarding class provides NEs with a method to determine the relative importance of one packet over another packet in a different forwarding class.

Queues are created for a specific forwarding class to determine how the queue output is scheduled into the switch fabric and the type of parameters that the queue accepts. The forwarding class of the packet, and the in-profile and out-of-profile states, determine how the packet is queued and handled at each hop along its path to a destination egress point. Forwarding classes may also be associated with policers instead of queues. Eight forwarding classes are supported. Table 44-1 lists the default definitions for the supported forwarding classes.

Although all forwarding classes support profile marking, it is a good network engineering practise to ensure that all high priority forwarding classes are in-profile (CIR=PIR) and all low priority forwarding classes are out-of-profile (PIR > CIR=0). This way, distinguishing packets as in-profile or out-of-profile only occurs for assured class types.

Table 44-1 Forwarding classes

Forwarding class ID	Forwarding class name	Forwarding class designation	DiffServ name	Class type	Intended
7	Network control	nc	nc2	High priority	For network control traffic
6	High-1	h1	nc1		For a second network control class or delay/jitter sensitive traffic
5	Expedited	ef	ef		For delay/jitter sensitive traffic
4	High-2	h2	h2		For delay/jitter sensitive traffic
3	Low-1	l1	af2	Assured	For assured traffic; default priority for network management traffic
2	Assured	af	af1		For assured traffic
1	Low-2	l2	cs1	Best effort	For best effort traffic
0	be	be			

Forwarding subclasses

You can use forwarding subclasses for additional access ingress packet classification. One or more subclasses can be associated with each forwarding class. The designations for forwarding subclasses are the same as those for the forwarding classes listed in Table 44-1. Each subclass assumes the behavior of its parent forwarding class. and in combination with the forwarding class provides a greater range of access ingress QoS classification possibilities.

Policers

You can add a policer to an access ingress policy to provide traffic flow limiting. Policers are associated with the forwarding classes defined in the access ingress policy. Policers can also be linked to a policer control policy, which maintains a hierarchy of multiple policer objects in the 5620 SAM system. Policers are linked to policer control policies by means of an arbiter. For more information, see "Policer control policies".

Traffic mapping

You can specify how you want to configure the mapping between the ingress traffic and ingress queue. Mapping is optional and can be based on combinations of customer QoS marking (Dot1p, DSCP, EXP, and precedence), and IP criteria or MAC criteria. Table 44-2 describes the options.

Adding an LspExp rule to a policy forces packets that match the specified MPLS LSP EXP criteria to override the existing forwarding class and enqueuing priority, based on the parameters specified in the LspExp rule. This functionality allows geographically distributed ISP sites to establish site-to-site interconnection service through a backbone network using VPLS/VLL. Each ISP site PE router connects to a 7x50 Ethernet L2 SAP in the backbone network, and traffic is encapsulated in a VPLS/VLL service tunnel. A maximum of eight LspExp rules are allowed on a single access ingress policy.

Table 44-2 Access ingress policy traffic mapping configuration options

Tab button	Use
Dot1p	Maps the Dot1p value of the ingress traffic to the ingress queue ID.
Dscp	Maps the DSCP value of the ingress traffic to the ingress queue ID.
LspExp	Maps the EXP value of the ingress traffic to the ingress queue ID.
Precedence	Maps the precedence value of the ingress traffic to the ingress queue ID.
IP Match Criteria	Maps the IP Match Criteria of the ingress traffic to the ingress queue ID.
MAC Match Criteria	Maps the MAC Match Criteria of the ingress traffic and ingress queue ID.

Access egress policies

Access egress policies are applied to access egress interfaces and specify QoS on egress.

Access egress policies define egress service queues and map forwarding class flows to queues. In the simplest access egress policy, all forwarding classes are treated like a single flow and mapped to a single queue.

The required access egress policy elements include:

- a unique access egress policy ID
- at least one defined default queue
- an exclusive scope for one-time use, or a template scope for use with multiple SAPs and interfaces

The optional egress policy elements include:

- additional queues up to a total of 8 separate queues for each of the 8 supported forwarding classes
- IEEE 802.1p priority value remarking based on forwarding class
- A policer to control traffic flow rate

Each queue in a policy is associated with one or more of the supported forwarding classes. Each queue can have its individual queue parameters allowing individual rate shaping of the forwarding classes mapped to the queue. More complex service queuing models are supported, where each forwarding class is associated with a dedicated queue.

The forwarding class determination per service egress packet is determined at ingress. If the packet ingresses the service on the same managed device, the service ingress classification rules determine the forwarding class of the packet. If the packet was received over a service tunnel, the forwarding class is marked in the tunnel transport encapsulation.

There is one default access egress policy. The default policy gives all traffic equal priority with the same chance of being sent or dropped during periods of congestion.

Policy override

You can override some or all settings associated with an access egress policy on an L2 or L3 access interface, SLA profile, or subscriber profile. See Procedure 44-40 for more information.

Note — You can override Access Egress policies that have the Scope parameter set to template. See Procedure 44-3 for more information.

Policers

You can add a policer to an access egress policy to provide traffic flow limiting. Policers are associated with the forwarding classes defined in the access ingress policy. Policers can also be linked to a policer control policy, which maintains a hierarchy of multiple policer objects in the 5620 SAM system. Policers are linked to policer control policies by means of an arbiter. For more information, see "Policer control policies".

Traffic mapping

You can specify how you want to configure the mapping between the egress traffic and egress queue. Mapping is optional and can be based on combinations of customer QoS marking (DSCP and precedence), and IP criteria. Table 44-2 describes the options.

Table 44-3 Access egress policy traffic mapping configuration options

Tab button	Use
Dscp	Maps the DSCP value of the ingress traffic to the ingress queue ID.
Precedence	Maps the precedence value of the ingress traffic to the ingress queue ID.
IP Match Criteria	Maps the IP Match Criteria of the ingress traffic to the ingress queue ID.

Network policies

Network policies are applied to network interfaces or access uplink ports and specify QoS on egress and ingress.

On ingress, a network policy maps incoming DSCP and EXP values to forwarding class and profile state for traffic received from the core network. On egress, the policy maps forwarding class and profile state to DSCP and EXP values for traffic to be transmitted into the core network.

Network queue policies

Network queue policies are applied to network ports, uplink ports, or daughter cards.

Network queue policies determine:

- the default burst allocations for queues based on the queue's forwarding class
- the CIR, PIR, and burst size parameters for the queue

You cannot use the same policy on devices of different releases. For example, if the 5620 SAM is managing a Release 7.0 7750 SR and a Release 8.0 7750 SR, you must create two network queue policies and distribute one to the Release 7.0 7750 SR and one to the Release 8.0 7750 SR.

For network egress, a network burst policy is associated with the network port buffer pool. For network ingress, the network burst policy is associated the network ingress buffer pool of the daughter card.

Network queue policies support multipoint queues and a variable number of forwarding classes. When you want to deploy a network queue policy to devices of different types, you may need to create an instance of the policy for each NE type. Policies that are configured for multipoint queues and a variable number of forwarding classes are deployed only to devices that support the functionality. Modification of an existing policy results in automatic deployment to participating NEs, so must be done with consideration of the policy features and devices involved.

Slope policies

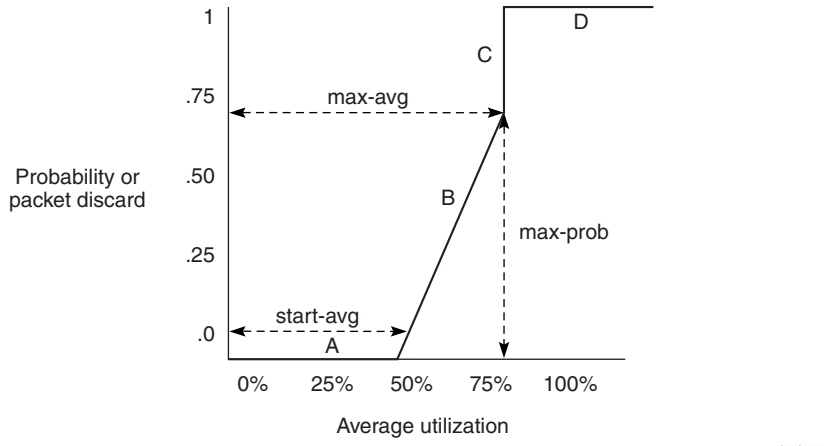
Slope policies are applied to access ports, network ports, and network daughter cards.

Slope policies define weighted RED slope characteristics for buffer pools. Low-priority and high-priority slopes are specified when you configure a slope policy. If a slope policy is not explicitly specified, a default policy is applied.

Each buffer pool supports a high-priority and a low-priority RED slope. The high-priority RED slope manages access to the shared portion of the buffer pool for the high-priority or in-profile packets. The low-priority RED slope manages access to the shared portion of the buffer pool for low-priority or out-of-profile packets. By default, the high-priority and low-priority slopes are disabled.

A RED slope is a graph with an X (horizontal) and Y (vertical) axis. The X axis plots the percentage of shared buffer utilization, from 0 to 100%. The Y axis plots the probability of packet discard marked from 0 to 1. The slope is defined as four sections, as shown in Figure 44-1.

Figure 44-1 RED slope characteristics



Section A is (0, 0) to (start-avg, 0). For this part of the slope, the packet discard value is always zero, which prevents the RED function from discarding packets when the shared buffer average utilization falls between 1 and start-avg.

Section B is (start-avg, 0) to (max-avg, max-prob). This part of the slope is linear where packet discard probability increases from zero to max-prob.

Section C is (max-avg, max-prob) to (max-avg, 1). This part of the slope shows the instantaneous increase of packet discard probability from max-prob to one. A packet discard probability of one results in an automatic discard of the packet.

Section D is (max-avg, 1) to (100%, 1). On this part of the slope, the shared buffer average utilization value of max-avg to 100% results in a packet discard probability of one.

HSMDA slope policies

The HSMDA slope policy controls the management of the HSMDA queue depth. The polices are applied to queues defined in the SAP ingress and SAP egress QoS to provide congestion control. Congestion control includes a defined maximum depth that the queue can reach when packets and RED of congestion and slope-based discards based on queue depth are accepted.

Note — The 5620 SAM does not support HSMDA slope policies on the 7710 SR, 7450 ESS-1, or 7750 SR-1.

Shared-queue policies

A shared-queue policy can be applied to daughter cards for optional use by SAPs. The 5620 SAM provides one shared-queue policy for all eight default queues. Each queue is associated with a default forwarding class.

Shared-queue QoS policies can be implemented to facilitate queue consumption on a daughter card; for example, when VPLS, IES, and VPRN services are scaled on one card. Instead of allocating multiple hardware queues for each unicast queue that is defined in an access ingress policy, SAPs with the shared-queuing feature enabled only allocate one hardware queue for each unicast queue.

However, the total amount of traffic throughput at ingress is reduced because ingress packets that are serviced by a shared-queuing SAP are recirculated for additional processing. This can reduce the available bandwidth by half. Shared queuing can also add latency. Network planners should consider these restrictions when they try to scale services on one daughter card.

Table 44-4 lists the queue IDs used by the 5620 SAM to identify the shared-queue types.

Table 44-4 Shared queue types

Shared-queue ID	Shared-queue type
1 to 8	Unicast
9 to 16	Multicast
17 to 25	Broadcast
26 to 32	Unknown

Note — Queue IDs 9 to 32 are also known as multipoint shared queues.

Shared policer output queue

To support hierarchical policing, a default policer-output-queues policy is applied automatically to each IOM that supports ingress policing. In SAM, this shared policer output queue is modeled in the same manner as the existing default shared queue, except that it has only 16 queues.

Multipoint shared-queue policies

Multipoint shared queues minimize the number of multipoint queues that are created for the following service components and subscriber profiles:

- ingress VPLS, IES, or VPRN SAPs
- ingress subscriber SLA profiles

Typically, ingress multipoint packets are handled by multipoint queues that are created for each SAP or subscriber SLA profile instance. In some cases, the number of SAPs or SLA profile instances are sufficient for the in-use multipoint queues to represent many thousands of queues on an ingress forwarding plane. If multipoint shared queuing is enabled for the SAPs or SLA profile instances on the forwarding plane, the multipoint queues are not created. Instead, the ingress multipoint packets are handled by the unicast queue that is mapped to the forwarding class of the multipoint packet.

Multipoint shared queues are a superset of shared queuing. With shared queuing on a SAP or SLA profile instance, only unicast packets are processed twice; once for the initial service-level queuing and a second time for switch fabric destination queuing. Shared queuing does not affect multipoint packet handling. Multipoint packet handling in normal service queuing is the same as shared queuing. Shared queuing for unicast packets is automatically enabled when you enable multipoint shared queuing.

The 5620 SAM supports multipoint shared-queue policies for the following services on the 7750 SR, 7450 ESS, 7710 SR:

- Layer 2: VPLS and MVPLS
- Layer 3: IES and VPRN

See the following chapters for more information about enabling multipoint shared queues for a service:

- chapter 68 for VPLS and MVPLS
- chapter 70 for IES
- chapter 71 for VPRN

You can also enable multipoint shared queues in an existing shared-queue policy. See the procedures in this chapter for more information about editing shared-queue policies.

Scheduler policies

Scheduler policies determine the order in which queues are serviced. All ingress and egress queues operate within the context of a scheduler. Multiple queues share the same scheduler. Schedulers control the data transfer between the following queues and destinations:

- service ingress queues to switch fabric destinations
- service egress queues to access egress ports
- network ingress queues to switch fabric destinations
- network egress queues to network egress interfaces

The are two types of scheduler policies:

- single-tier, in which queues are scheduled based on the forwarding class of the queue and the operation state of the queue relative to the queue CIR and PIR
- hierarchical or multi-tier, which allow the creation of a hierarchy of schedules where queues or other schedulers are scheduled by superior schedulers

Scheduler policies are applied to access ingress and access egress interfaces.

Single tier schedulers

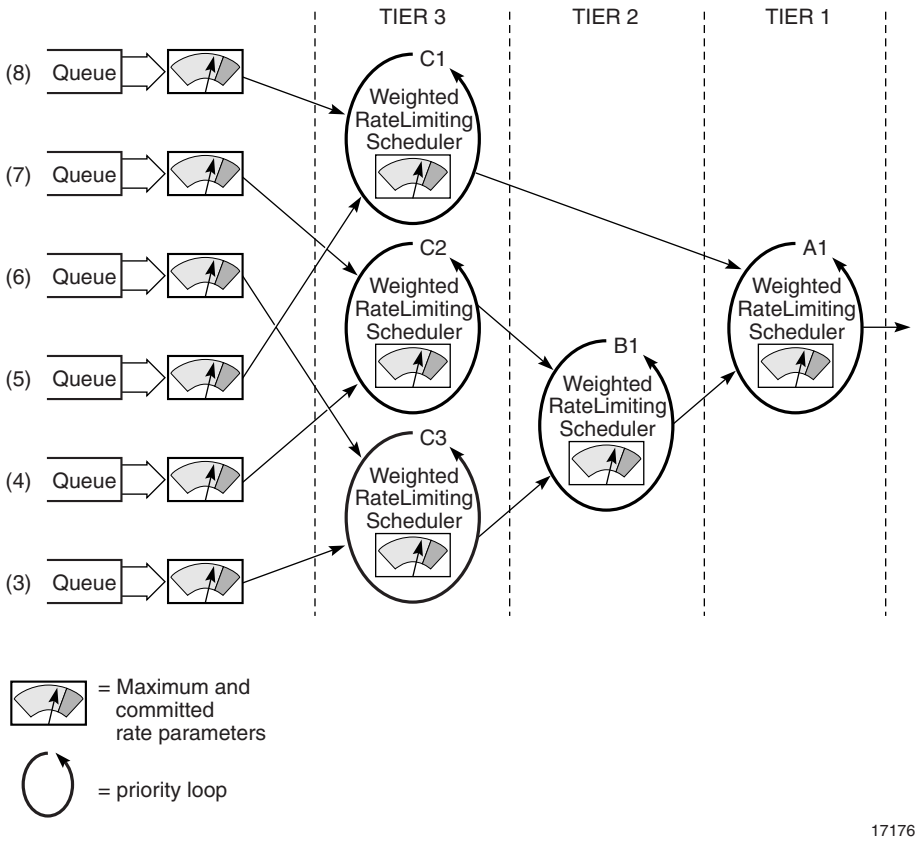
Single-tier scheduling is the default method of scheduling queues. Queues are scheduled with single-tier scheduler policies when no explicit hierarchical scheduler policy is defined or applied. In single-tier scheduling, queues are scheduled based on the forwarding class of the queue and the operational state of the queue relative to the queue CIR and PIR.

Hierarchical schedulers

Hierarchical scheduler policies are used for access ingress and access egress queues. Hierarchical scheduler policies allow you to create a hierarchy of schedulers where queues and other schedulers are scheduled by superior schedulers.

Virtual schedulers are created within the context of a hierarchical scheduler policy. A hierarchical scheduler policy defines the hierarchy and parameters for each scheduler. A scheduler is defined in the context of a tier. The tier level determines the scheduler's position in the hierarchy. Three tiers of virtual schedulers are supported, as shown in Figure 44-2.

Figure 44-2 Hierarchical scheduler and queue association



Tier 1 schedulers are defined without a parent scheduler. A scheduler can enforce a maximum rate of operation for all child queues and associated schedulers.

You can create a tier 2 scheduler without a parent tier 1 scheduler or a tier 3 scheduler without a parent tier 2 scheduler.

Policy override

You can override some or all settings associated with an ingress or egress scheduler policy on an L2 or L3 access interface or subscriber profile.

HSMDA scheduler policies

The HSMDA scheduler policy controls the scheduling of a set of HSMDA scheduler classes. The policies are assigned to egress HSMDA ports, and the ingress control scheduler between the HSMDA and ingress forwarding plane. The policies assigned to HSMDA egress ports define how all queues associated with the egress port are scheduled. Scheduler policies assigned to the ingress control scheduler between the HSMDA and ingress forwarding plane define how all ingress queues on the HSMDA, regardless of the ingress port, are scheduled.

Note — The 5620 SAM does not support HSMDA scheduler policies on the 7710 SR, 7450 ESS-1, or 7750 SR-1.

Port scheduler policies

Port scheduler policies determine the virtual scheduling of egress ports by allocating HQoS bandwidth based on the available bandwidth at the egress port level. A port scheduler is defined in the context of a tier. The tier level determines the position of the port scheduler in the hierarchy.

The first tier of the scheduling hierarchy manages the total frame bandwidth that the port scheduler allocates to the eight priority levels. The second tier receives bandwidth from the first tier in two priorities—a within-CIR distribution, and an above-CIR distribution. The within-CIR distribution of the second tier provides bandwidth to the third tier within-CIR distributions for each of the eight priority levels. The above-CIR distribution of the second tier provides bandwidth to the above-CIR distribution of the third tier for each of the eight priority levels.

Up to eight groups can be defined within each port scheduler policy. A group has a rate, an optional cir-rate, and inherits the highest scheduling priority of its member levels. In essence, a group receives bandwidth from the port and distributes it within the member levels of the group according to the weight of each level. Each level will compete for bandwidth within the group based on its weight under congestion situation. If there is no congestion, a priority level can achieve up to its rate (cir-rate) worth of bandwidth. One or more levels can map to the same group.

Note — When the agg-rate-limit is applied to queues of a subscriber which are mapped to different priority levels in the same weighted scheduler group, the bandwidth distribution to the queues will be based on the priority of the level.

Orphan queues or schedulers that are not explicitly associated with the port scheduler receive bandwidth after all parented queues and schedulers are allocated bandwidth.

Port scheduler policies are configured on ports and channels.

Policy override

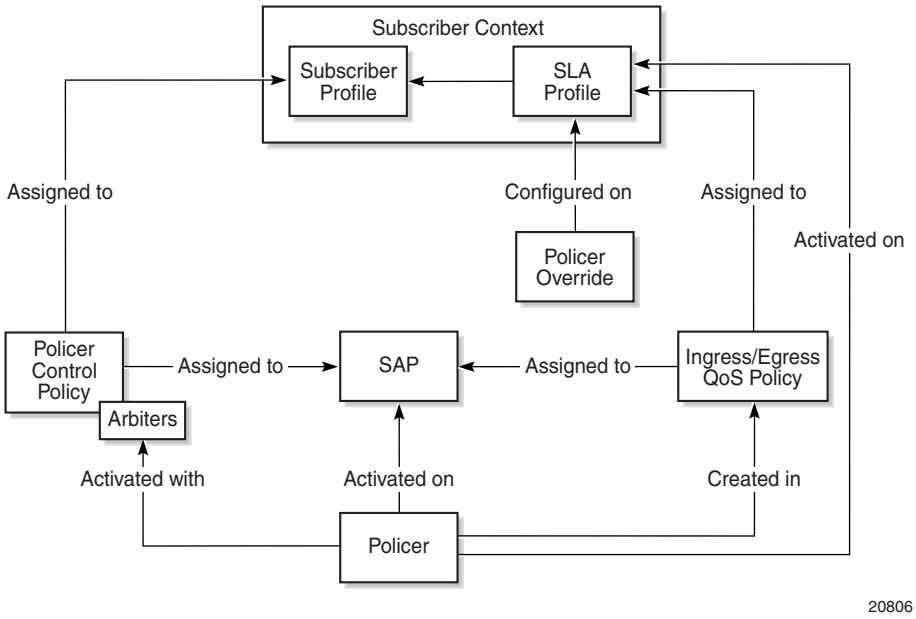
You can override some or all port scheduler settings associated with an access egress queue policy on an L2 or L3 access interface or SLA profile.

Policer control policies

Policer control policies allow you to create a control framework, under which policer objects associated with SAPs or subscriber contexts are configured with traffic control parameters. The policer object is applied to the SAP or subscriber context as part of an access ingress policy or access egress policy. The policer control policy is also applied to the SAP or subscriber context. The policer control policy provides the control framework, and policers are associated with the framework by means of arbiters.

When a policer control policy is applied to a SAP or subscriber context, the system creates a parent policer that is bandwidth limited by the policy's maximum bandwidth rate, as defined under the root arbiter. In addition to the root arbiter, the policy may also contain user defined child arbiters that provide bandwidth control for subsets of child policers.

Figure 44-3 Policer association with SAPs and user contexts under policer control hierarchy



A policer is created as part of an access ingress or access egress policy. The policer is configured with a parent arbiter name. When a policy containing a policer is applied to a SAP, the system scans the available arbiters on the SAP. If an arbiter exists with a name that matches the Parent Arbiter parameter on the policer, a policer to arbiter association is established and the policer becomes part of the policer control hierarchy.

In the case of subscriber contexts, the policer control policy is applied to the sub profile used by the subscriber. The system creates a unique policer control hierarchy for each subscriber associated with the sub profile. An access ingress or access egress policy containing a policer is applied to the subscriber SLA profile. The combination of the sub profile and SLA profile at the subscriber level provides the system with the information required to create the policer control hierarchy instance for the subscriber context.

Table 44-5 shows a sample workflow to configure a policer control hierarchy.

Table 44-5 Sample 5620 SAM policer control hierarchy configuration

Task	Description
1.Configure a policer control policy	Create arbiters and configure the parent/child relationship between arbiters to build a policer control hierarchy. To configure a policer control policy, see procedure 44-19.
2. Configure a policer on an access ingress or access egress policy	Create a policer in an access ingress or access egress policy to configure traffic control parameters. Assign a parent arbiter to the policer to associate it with the hierarchy configured in the policer control policy. To add a policer to an access ingress policy, see procedure 44-1. To add a policer to an access egress policy, see procedure 44-2.
3. Assign the policer control policy to a subscriber.	Assign the policer control policy to a subscriber that is configured with an access ingress or access egress policy that includes a policer. To assign a policer control policy to a subscriber, see procedure 64-2.
4. Assign the policer control policy to an access interface or a SAP.	Assign the policer control policy to an access interface or SAP that is configured with an access ingress or access egress policy that includes a policer. To assign a policer control policy to an IES L3 access interface, see procedure 70-1. To assign a policer control policy to an IES SAP, see procedure 70-8. To assign a policer control policy to a VPLS L2 access interface, see procedure 68-3. To assign a policer control policy to a VPLS B-L2 access interface, see procedure 68-13. To assign a policer control policy to a VPLS I-L2 access interface, see procedure 68-14. To assign a policer control policy to a VPRN L3 access interface, see procedure 71-2. To assign a policer control policy to a VPRN SAP, see procedure 71-11.

Named buffer pool policies

Named buffer pool policy is a QoS policy used to manage named pools. It allows you to create named pools to override the default buffer pool behavior by creating and allocating ingress and egress queues. Named pools are configured in the named buffer pool policy and are applied at the MDA and/or port ingress and egress level.

Named pools can be further defined in Q1 pools configuration. You can configure and assign queue pools to the following policies:

- Access Ingress
- Access Egress
- Network Queue
- Shared Queue

When a policy is associated at the MDA level, named pools defined in the policy allow queues from any port to be associated. When a policy is associated at the port level, named pools are only available to queues associated with that port. A named pool policy that is currently applied to a MDA or port can be deleted after all association between the policy and the MDA or port have been removed.

When buffer pools are created, renamed or deleted, queues mapped to the pools are moved to default pools. When a queue is moved, traffic that was destined for the queue is temporarily moved to a fail over queue. After the old queue is drained, and the new queue is created and associated with the buffer pool, the saved stats are loaded to the new queue and traffic is moved from the fail over queue to the new queue.

Table 44-6 describes a sample workflow to configure Named Buffer Pools and Q1 pools.

Table 44-6 Sample 5620 SAM Named Buffer Pools configuration

Task	Description
1.Configure a Named Pool Buffer Policy	To configure a named pool buffer policy, see Procedure 44-20.
2. Enable Named Pool mode	To enable named pools to be configured for a port or MDA, see Procedure 17-46.
3.Apply a Named Pool policy to a MDA	To apply a named pool policy to an MDA, see Procedure 17-41.
4.Apply a Named Pool policy to a port	To apply a named pool policy to a port, see Procedure 17-61.
5. Configure Q1 pools	To configure Q1 pools, see Procedure 44-26.
6.Assign Q1 pools to Access Ingress policies	To assign Q1 pools to Access Ingress policies, see Procedure 44-1.
7. Assign Q1 pools to Access Egress policies	To assign Q1 pools to Access Ingress policies, see Procedure 44-3.
8. Assign Q1 pools to Network Queue policies	To assign Q1 pools to Network Queue policies, see Procedure 44-12.
9. Assign Q1 pools to Shared Queue policies	To assign Q1 pools to Shared Queue policies, see Procedure 44-14.

Queue Group Template policies

Queue Group Template policies allow you to define the queuing and parenting structure for queue groups on Ethernet ports. The policy defines the number and types of queues within the port queue group, and provides the default queue parameters.

There are two types of Queue Group Template policies: Ingress Queue Group Template policy and Egress Queue Group Template policy.

- Ingress Queue Group Template policies are used for Access Ingress Queue Group creation on Ethernet access ports
- Egress Queue Group Template policies are used for Access Egress Queue Group and Network Egress Queue Group creations on Ethernet ports

Queue Group Template policies are used in the following network applications:

- Access SAP queue group applications
- Network port queue groups for network interfaces

See chapter 61 for more information about queue groups, the associated network components, and typical applications.

Default policer queue group

The system maintains a special default egress queue group template policy that is applied automatically to all Ethernet ports. The default policer-output-queues policy is configured with two queues:

- Queue 1: configured with a forwarding class value of Best Effort.
- Queue 2: configured with a forwarding class value of Expedite.

All other parameters are default. You cannot delete the default policer-output-queues policy.

7705 SAR fabric profiles

Each daughter card in a 7705 SAR can have two assigned fabric profiles, one for access ingress and one for network ingress. These policies are assigned from the Daughter Card tab of a daughter card slot properties form.

A 7705 SAR fabric profile includes a mode, which cannot be changed after profile creation, and one or more shaping rates. The mode types are Aggregate and Destination. In Aggregate mode, one rate defines the maximum fabric shaping rate that is distributed to each daughter card slot. In Destination mode, there is one fabric shaping rate for each daughter card slot.

HSMDA pool policies

The HSMDA pool policy is a QoS policy type that applies to the HSMDA. The policy can be assigned to an ingress or egress HSMDA to control how buffers are distributed between HSMDA queues. HSMDA pool policies do not apply to ports.

Note — The 5620 SAM does not support HSMDA pool policies on the 7710 SR, 7450 ESS-1, or 7750 SR-1.

ATM QoS policies

ATM QoS policies are used to specify how ATM traffic is managed by using ATM traffic descriptors, such as service category and shaping. You can create up to 2000 ATM QoS policies per router. ATM QoS policies are applied to access interfaces.

Note — For the 9500 MPR (ETSI 1.3), the maximum number of ATM traffic descriptors that are configurable on an NE is 1536, which is twice the maximum number of configurable VPs multiplied by the maximum number of ASAP cards that can be hosted (2x 128 x6).

MC MLPPP ingress and egress QoS profiles

MC MLPPP ingress QoS profiles are used to configure the reassembly timeout for each of the four MLPPP classes. You can create up to 128 ingress QoS profiles per NE.

MC MLPPP egress QoS profiles are used to specify queue and queue scheduling parameters for each of the four MLPPP classes.

MCFR ingress and egress QoS profiles

MCFR ingress QoS profiles are used to configure the reassembly timeout for each of the four MLFR classes. You can create up to 128 ingress QoS profiles per NE.

MCFR egress QoS profiles are used to specify queue and queue scheduling parameters for each of the four MLFR classes.

7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco policies

7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco policies are used to create and apply QoS policies to these NEs and ports.

Note — The 5620 SAM supports the distribution of policies on the 7450 ESS, 7750 SR, 7710 SR, Release 6.3 or earlier Telco devices, and on the 7250 SAS and 7250 SAS-ES, prior to Release 2.0.

When a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco ACL IGMP packet filter policy entry is created from a multicast package policy, the multicast source IP address is used to specify the multicast source IP address portion of the IGMP packet filter.

OmniSwitch QoS policies

OmniSwitch QoS provides a way to control traffic flows through the switch based on configured policies. The control may be simple such as allowing or denying traffic, or complicated such as remapping 802.1p bits from a Layer 2 network to ToS values in a Layer 3 network.

The OmniSwitch supports the following types of QoS policies:

- basic QoS—to control traffic prioritization and bandwidth shaping
- ACLs—for Layer 2, 3, and 4 filtering

A QoS policy contains a condition and an action. The condition specifies parameters that the switch checks in incoming traffic flows, such as the destination address or ToS bits. The action specifies what the switch does with traffic that matches the condition; for example, the switch may queue the traffic flow with a higher priority or reset the ToS bits.

Ethernet service policies are used to create UNI and SAP profiles. The profiles are applied to stacked VLAN SAPs and UNIs to control traffic and specify options to manage certain traffic types.

7210 SAS QoS policies

The main types of 7210 SAS QoS policies are:

- QoS policies for classification, defining metering and queuing attributes, and marking
- slope policies that define default buffer allocations and RED slope definitions
- port scheduler policies that determine how queues are scheduled

The 5620 SAM supports the following types of 7210 SAS QoS policies:

- 7210 Access Ingress
- 7210 Port Access Egress
- 7210 Access Egress
- 7210 Network
- 7210 Network Queue
- 7210 Slope
- 7210 Queue Management
- 7210 Port Scheduler
- 7210 Remarking

Table 44-7 lists the types of 7210 SAS QoS policies and describes the policy characteristics.

Table 44-7 7210 SAS QoS policies

Policy type	Applied to	Traffic type affected	Description
7210 Access Ingress	Access port SAP	Ingress	• supports only policing using meters, not rate shaping
7210 Port Access Egress	Access port SAP	Egress	• defines the SLA for service packets as they egress on the SAP
7210 Access Egress	Access port	Egress	• eight queues per port, each forwarding class mapped to a queue • remarking is always turned on • only supports dot1p remarking
7210 Network	Uplink port, network port, or network interface (1)	Ingress and egress	• only supports ingress rate limiting using meters • eight forwarding classes per port • traffic mapping to forwarding classes based on Dot1p, DSCP, or LSP-Exp value markings (2) • supports srTCM, trTCM, trTCM (RFC 2698), and trTCM (RFC 4115)
7210 Network Queue	Uplink port	Egress	• eight hardware queues per port • fixed mapping of forwarding class to queues

(1 of 2)

Policy type	Applied to	Traffic type affected	Description
7210 Slope	Access or uplink port	Egress	• only supports simple RED • low slope drops out-of-profile packets • high slope drops in-profile packets
7210 Queue Management		Egress	• defines slope parameters that determine a WRED profile for each queue
7210 Port Scheduler	Access or uplink port	Egress	• defines scheduling among the queues and the weight proportion for each queue
7210 Remarking	Access or uplink port	Egress	• configures the remarking behavior for the NE at the egress of the access SAPs, ports, and IP interfaces

(2 of 2)

Notes

(1) The 7210 SAS-E supports the 7210 Network QoS Policy on uplink ports. The 7210 SAS-M, Release 1.1 R4 or later, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7210 SAS-X24F2XFP support the 7210 Network QoS Policy on network ports and network interfaces.

(2) Dot1p and DSCP only apply to network ports and LSP-Exp only applies to network interfaces.

See the 7210 SAS-E OS Quality of Service Guide for more information about 7210 SAS QoS and QoS policies.

44.2 QoS policies procedures

This section contains procedures relating to the configuration and maintenance of QoS policies.

Procedure 44-1 To configure an access ingress policy

1 Choose Policies→QoS→SROS QoS→Access Ingress→Access Ingress from the 5620 SAM main menu. The Manage Access Ingress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Access Ingress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- ID
- Displayed Name
- Description
- Scope
- Priority
- HSMDA Packet Byte Offset (bytes)
- Default FC
- Default FC HSMDA Counter Override

The packets that are received on an ingress SAP using this policy are classified to the specified default forwarding class. See Table 44-1 for more information about forwarding classes.

4 Click on the HSMDA Queues tab button. Eight default queues are displayed.

i Select a queue and click on the Properties button. The Access Ingress HSMDA Queue (Create) form opens with the General tab displayed.

ii Modify the parameters, if required:

- Displayed Name
- Description
- Policed

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

iii Click on the Select button in the HSMDA Slope Policy panel to choose a slope policy. The Select HSMDA Slope Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select HSMDA Slope Policy form closes and the policy information is displayed on the Access Ingress HSMDA Queue (Create) form.

v Click on the CIR/PIR tab button.

vi Configure the parameters:

- CIR (Kbps)
- PIR (Kbps)
- CIR Adaptation
- PIR Adaptation

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Access Ingress Policy (Create) form reappears.

5 Click on the Queues tab button.

The two default queues that cannot be deleted are displayed—the default unicast traffic queue (ID 1) and the default multipoint traffic queue (ID 11).

i Click on the Add button. The Queue form opens with the General tab displayed.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Pool Name
- Multicast
- Scheduler
- Mode
- Expedite
- Policed

Note 1 — You can use the Select button beside the Pool Name parameter to configure the parameter.

Note 2 — Before you can configure the Pool Name parameter, you must create a Q1 pool using Procedure 44-26.

iii Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Queue (Edit) form.

v Click on the CIR/PIR tab button.

vi Configure the parameters:

- CIR (Kb/s)
- PIR (Kb/s)
- CIR Adaptation
- PIR Adaptation

Ensure that the CIR value is lower than the PIR value.

vii Click on the Burst Size tab button.

viii Configure the parameters:

- Committed Burst Size (KB)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit

The parameters are configurable when the Default check box above each is deselected.

Ensure that the Committed Burst Size (KB) value is lower than the Maximum Burst Size (bytes) value.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Access Ingress Policy (Create) form reappears.

xi To configure additional queues, return to step i. You can add up to 32 queues.

6 Click on the Policer tab button.

i Click on the Add button. The Access Ingress Policer form opens.

ii On the General tab, configure the parameters:

- ID
- Description
- Parent Arbiter
- Stats Mode
- Packet Byte Offset

iii Click on the CIR/PIR tab button and configure the parameters:

- CIR (Kb/s)
- PIR (Kb/s)
- CIR Adaptation
- PIR Adaptation

iv Click on the Burst Size tab button and configure the parameters:

- Committed Burst Size (KB)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit

v Click on the OK button to save the changes. A dialog box appears.

vi Click on the OK button. The Access Ingress Policer form closes, and the Access Ingress Policy form reappears.

7 Click on the Forwarding Classes tab button. You can create one entry for each of the eight forwarding class types.

i Click on the Add button. The Forwarding Class (Create) form opens with the General tab displayed.

ii Configure the Forwarding Class parameter.

iii Perform any of the following:

- If you need to configure a queue group for some or all traffic types, complete steps iv and v.
- If you need to configure queues for some or all traffic types, complete step v.
- If you need to configure policers for some or all traffic types, complete step v.

iv On the Traffic Control panel, configure the Use Queue Group parameter for any of the Unicast, Broadcast, Multicast, and Unknown traffic types.

On the queues panel, click on the Select button beside the Queue Group Template Policy parameter and select a queue group template policy from the Select Queue Group Template Policy form.

Note — If the Use Queue Group parameter is enabled for the global policy, the Queue ID, Multipoint Queue ID, Broadcast Queue ID, and Unknown Queue ID, if selected, are validated against the specified Queue Group Template Policy. When the global policy is distributed to an NE that does not support queue groups, for example, an NE at Release 7.0 R2 or earlier, the 5620 SAM ignores the queue group-related parameters. The Queue ID is validated against the local queues for each local policy instance.

v On the Queues panel Configure the parameters:

- Queue ID

  The parameter must be set to a unicast ID. Set the parameter to 0 if you want the default queue ID to be used.
- Multipoint Queue ID

  The parameter must be set to a multicast ID. Set the parameter to 0 if you want the default queue ID to be used.
- Broadcast Queue ID

  The parameter must be set to a multicast ID. Set the parameter to 0 if you want the default queue ID to be used.
- Unknown Queue ID

  The parameter must be set to a multicast ID. Set the parameter to 0 if you want the default queue ID to be used.

vi On the Traffic Control panel, configure the Use Policer parameter for any of the Unicast, Broadcast, Multicast, and Unknown traffic types.

vii On the Policers panel, for each traffic type configured with the Use Policer parameter, configure the appropriate Policer ID parameter:

- Unicast Policer ID
- Multipoint Policer ID
- Broadcast Policer ID
- Unknown Policer ID

Click on the Select button beside each Policer ID parameter and select a policer from the list in the Select Policer form. The policer must be preexisting on the access ingress policy (see step 6.

viii Configure the parameters:

- In Remark
- Out Remark
- In Precedence

  The In Precedence parameter is configurable when the In Remark parameter is set to precedence.
- Out Precedence

  The Out Precedence parameter is configurable when the Out Remark parameter is set to precedence.
- In DSCP

  The In DSCP parameter is configurable when the In Remark parameter is set to dscp.
- Out DSCP

  The Out DSCP parameter is configurable when the Out Remark parameter is set to dscp.
- Profile
- Mark DE bit 1 as Out of Profile
- HSMDA Queue ID
- HSMDA Multicast Queue ID
- HSMDA Broadband Queue ID

The Multicast, Broadcast, and Unknown IDs must be set to multicast IDs. The default ID for multicast, broadcast, and unknown queues is 11.

ix Click on the Sub Classes tab button.

x Click on the Add button. The Forwarding SubClass form opens.

xi Configure the parameters:

- Displayed Name
- In Remark
- Out Remark
- In Precedence

  The In Precedence parameter is configurable when the In Remark parameter is set to precedence.
- Out Precedence

  The Out Precedence parameter is configurable when the Out Remark parameter is set to precedence.
- In DSCP

  The In DSCP parameter is configurable when the In Remark parameter is set to dscp.
- Out DSCP

  The Out DSCP parameter is configurable when the Out Remark parameter is set to dscp.
- Profile
- Mark DE bit 1 as Out of Profile

xii Click on the OK button. A dialog box appears.

xiii Click on the OK button. The Forwarding SubClasses form closes and the Forwarding Class form reappears.

xiv Click on the OK button. A dialog box appears.

xv Click on the OK button. The Forwarding Class (Create) form closes and the Access Ingress Policy form reappears.

8 Click on the Dot1p tab button.

i Click on the Add button. The Dot1p form opens.

ii Configure the parameters:

- Dot1p
- Forwarding Class
- Priority
- HSMDA Counter Overrides (bytes)

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Dot1p form closes and the Access Ingress Policy form reappears.

9 Click on the DSCP tab button.

i Click on the Add button. The DSCP form opens.

ii Configure the parameters:

- DSCP
- Forwarding Class
- Priority
- HSMDA Counter Overrides (bytes)

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The DSCP form closes and the Access Ingress Policy form reappears.

10 Click on the Precedence tab button.

i Click on the Add button. The Precedence form opens.

ii Configure the parameters:

- Precedence
- Forwarding Class
- Priority
- HSMDA Counter Overrides (bytes)

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Precedence form closes and the Access Ingress Policy form reappears.

11 Click on the IP Match Criteria tab button to configure IPv4 match criteria.

i Click on the Add button. The IP Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Forwarding Class
- Priority
- HSMDA Counter Overrides (bytes)
- Protocol
- Fragment
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- DSCP
- Source Port
- Destination Port

The Source Port and Destination Port parameters appear only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The IP Match form closes and the Access Ingress Policy form reappears.

12 Click on the MAC Match Criteria tab button.

i Click on the Add button. The MAC Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Forwarding Class
- Priority
- Frame Type
- Source MAC
- Mask
- Destination MAC
- ATM VCI
- Mask
- Dot1p
- Mask
- DSAP
- Mask
- SSAP
- Mask
- SNAP OUI
- SNAP PID
- Ether Type

The Source MAC, Destination MAC, Dot1p parameters, and the Mask parameter associated with each, are configurable when the check box for each parameter is selected.

The DSAP, DSAP Mask, SSAP, and SSAP Mask parameters are configurable when the Frame Type parameter value is e802dot2LLC.

The SNAP OUI and SNAP PID parameters are configurable when the Frame Type parameter value is e802dot2SNAP.

The Ether Type parameter is configurable only when the Frame Type parameter value is Ethernet II.

The ATM VCI parameter is configurable only when the Frame Type parameter value is ATM.

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The MAC Match form closes and the Access Ingress Policy form reappears.

13 Click on the IPv6 Match Criteria tab button.

i Click on the Add button. The IPv6 Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Forwarding Class
- Priority
- Protocol
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- DSCP
- Source Port
- Destination Port

The Source Port and Destination Port parameters appear only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The IPv6 Match form closes and the Access Ingress Policy form reappears.

14 Click on the Lsp Exp tab button.

i Click on the Add button. The Lsp Exp Create form opens.

ii Configure the parameters:

- LspExp
- Forwarding Class
- Priority
- HSMDA Counter Overrides (bytes)

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Lsp Exp Create form closes and the Access Ingress Policy form reappears.

15 Click on the Apply button to save the policy. The Access Ingress Policy form is refreshed with additional buttons.

16 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

17 Close the Access Ingress Policy form. The Manage Access Ingress Policies form reappears.

18 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 44-2 To configure a 7210 SAS access ingress policy

1 Choose Policies→QoS→SROS QoS→Access Ingress→7210 Access Ingress from the 5620 SAM main menu. The Manage 7210 Access Ingress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Access Ingress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Number of Qos Classifiers
- Default FC

The packets that are received on an ingress SAP using this policy are classified to the specified default forwarding class. See Table 44-1 for more information about forwarding classes.

4 Click on the Meter tab button.

i Click on the Add button. The Meter (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ID
- Rate Mode
- Multipoint

iii Click on the CIR/PIR tab and configure the parameters.

- CIR Adaptation
- PIR Adaptation
- CIR (kbps)
- PIR (kbps)

iv Click on the Burst Size tab button and configure the parameters:

- Committed Burst Size (kbps)
- Maximum Burst Size (kbps)

v Click on the OK button to save the changes. A dialog box appears.

vi Click on the OK button.

5 Click on the Forwarding Classes tab button.

i Click on the Add button. The Forwarding Class (Create) form opens.

ii Configure the parameters:

- Forwarding Class
- Meter ID
- Multicast Meter ID
- Broadcast Meter ID
- Unknown Meter ID

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button.

6 Click on the IP Match Criteria tab button to configure IP match criteria.

i Click on the Add button. The IP Match (Create) form opens.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Forwarding Class
- DSCP

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button.

7 Click on the MAC Match Criteria tab button.

i Click on the Add button. The MAC Match (Create) form opens.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Forwarding Class
- Frame Type
- Source MAC
- Mask
- Destination MAC
- Mask
- Dot1p
- Mask
- Ether Type

The Source MAC, Destination MAC, Dot1p, and the associated Mask parameters are configurable when the check box for each parameter is selected.

The Ether Type parameter is only configurable when the Frame Type parameter value is Ethernet II.

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button.

8 Click on the Apply button to save the policy. The 7210 Access Ingress Policy form is refreshed with additional buttons.

9 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 43 for more information.

10 Close the 7210 Access Ingress Policy form. The Manage 7210 Access Ingress Policies form reappears.

Procedure 44-3 To configure an access egress policy

1 Choose Policies→QoS→SROS QoS→Access Egress→Access Egress from the 5620 SAM main menu. The Manage Access Egress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Access Egress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- HSMDA Packet Byte Offset (bytes)

4 If you are creating a 7705 SAR MC MLPPP access egress policy, configure the Is 7705 SAR Multiclass MLPPP Policy parameter. Otherwise, go to step 5.

5 Click on the HSMDA Queues tab button. Eight default queues are displayed on the form.

i Select a queue and click on the Properties button. The Access Egress HSMDA Queue (Create) form opens with the General tab displayed.

ii Modify the parameters, if required:

- Displayed Name
- Description

iii Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Access Egress HSMDA Queue (Create) form.

v Click on the CIR/PIR tab button.

vi Configure the parameters:

- CIR (Kbps)
- PIR (Kbps)
- CIR Adaptation
- PIR Adaptation

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Access Egress Policy (Create) form reappears.

6 Click on the Queues tab button. One default queue is displayed on the form.

i Click on the Add button. The Queue (Create) form opens with the General tab displayed.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Pool Name
- Expedite
- Port Average Overhead (%)
- Scheduler
- Level
- Weight
- CIR Level
- CIR Weight
- Port Parent
- Level
- Weight
- CIR Level
- CIR Weight
- Use WRED Queue

Note 1 — You can use the Select button beside the Pool Name parameter to configure the parameter.

Note 2 — Before you can configure the Pool Name parameter, you must create a Q1 pool using Procedure 44-26.

The Scheduler, Level, Weight, CIR Level, and CIR Weight parameters in the Parent Scheduler panel are not configurable when the Port Parent parameter in the Port Parent panel is set to true.

iii Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

iv Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Queue form.

v Click on the CIR/PIR tab button.

vi Configure the parameters:

- CIR (Kb/s)
- PIR (Kb/s)
- CIR Adaptation
- PIR Adaptation

vii Click on the Burst Size tab button.

viii Configure the parameters:

- Committed Burst Size (KB)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit

Ensure that the Committed Burst Size (KB) value is lower than the Maximum Burst Size (bytes) value.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Access Egress Policy (Create) form reappears.

xi To create additional queues, go to step i. You can create up to eight queues.

7 Click on the Policer tab button.

i Click on the Add button. The Access Egress Policer form opens.

ii On the General tab, configure the parameters:

- ID
- Description
- Parent Arbiter
- Stats Mode
- Packet Byte Offset

iii Click on the CIR/PIR tab button and configure the parameters:

- CIR (Kb/s)
- PIR (Kb/s)
- CIR Adaptation
- PIR Adaptation

iv Click on the Burst Size tab button and configure the parameters:

- Committed Burst Size (KB)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit

v Click on the OK button to save the changes. A dialog box appears.

vi Click on the OK button. The Access Egress Policer form closes, and the Access Ingress Policy form reappears.

8 Click on the Forwarding Classes tab button.

i Click on the Add button. The Forwarding Class (Create) form opens.

ii Configure the Forwarding Class parameter.

iii Complete any of the following:

- If you want to configure a queue group, complete steps iv and v.
- If you want to configure a queue, complete step v.
- If you want to configure a policer, complete step vi.

iv On the Traffic Control panel, configure the Use Queue Group parameter.

On the queue panel, click on the Select button beside the Queue Group Template Policy parameter and select a queue group template policy from the Select Queue Group Template Policy form.

Note — If the Use Queue Group parameter is enabled for the global policy, the Queue ID is validated against the specified Queue Group Template Policy. When the global policy is distributed to an NE that does not support queue groups, for example, an NE at Release 7.0 R2 or earlier, the 5620 SAM ignores the queue group-related parameters. The Queue ID is validated against the local queues for each local policy instance.

v Configure the Queue ID parameter. Click on the Select button. The Select Queue - Forwarding Class - Access Egress Policy list form opens.

The parameter must be set to a unicast ID. Set the parameter to 0 if you want the default queue ID to be used. The default ID for unicast queues is 1.

vi On the Traffic Control panel, configure the Use Policer parameter.

Click on the Select button beside the Unicast Policer ID parameter and select a policer from the list in the Select Policer form. The policer must be preexisting on the access ingress policy (see step 7).

vii Configure the parameters. You can create one entry for each of the eight forwarding class types. The parameters include:

- dot1p
- In Profile
- Out Profile
- HSMDA Egress Profiling
- In Precedence
- Out Precedence
- In DSCP
- Out DSCP
- Mark DE bit
- Force DE value

viii Click on the OK button. A dialog box appears.

ix Click on the OK button. The Forwarding Class (Create) form closes and the Access Egress Policy (Create) form reappears with a list of the newly created forwarding classes displayed.

9 Click on the IP Match Criteria tab button.

i Click on the Add button. The IP Match form opens.

ii Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Protocol
- Fragment
- HSMDA Counter Override
- Forwarding Class
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- DSCP
- Source Port
- Destination Port
- Profile

The Source Port and Destination Port parameters appear only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The IP Match form closes and the Access Egress Policy form reappears.

10 Click on the DSCP tab button.

i Click on the Add button. The DSCP form opens.

ii Configure the parameters:

- DSCP
- HSMDA Counter Override
- Forwarding Class
- Profile

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The DSCP form closes and the Access Egress Policy form reappears.

11 Click on the Precedence tab button.

i Click on the Add button. The Precedence form opens.

ii Configure the parameters:

- Precedence
- HSMDA Counter Override
- Forwarding Class
- Profile

iii Click on the OK button to save the changes. A dialog box appears.

iv Click on the OK button. The Precedence form closes and the Access Egress Policy form reappears.

12 Click on the Apply button to save the policy. The Access Egress Policy form is refreshed with additional buttons.

13 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

14 Close the Access Egress Policy form. The Manage Access Egress Policies form reappears.

15 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 44-4 To configure a 7210 SAS port access egress policy

The 7210 SAS port access egress policy defines the SLA for service packets as they egress on the SAP. Eight queues are defined in the 7210 SAS policy. A 7210 SAS queue management policy can be associated with a queue to manage the buffer allocation for in-profile and out-of-profile packets. A 7210 SAS remarking policy with the type DOT1P or DOT1P-LSP-EXP SHARED can be associated with a 7210 SAS port access egress policy. The 7210 SAS port access egress policy can be associated with an Epipe or VPLS SAP.

1 Choose Policies→QoS→SROS QoS→Access Egress→7210 Port Access Egress from the 5620 SAM main menu. The Manage 7210 Access Egress Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.
- **b** Click on the Create button. The 7210 Port Access Egress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Egress Remark

4 Click on the Queues tab button. Eight default queues are displayed on the form.

- **i** Choose a queue and click on the Properties button. The PortAccessEgressQueue (Create) form opens with the General tab displayed.
- **ii** Configure the parameters:
  - ID
  - Displayed Name
  - Description
- **iii** Click on the CIR/PIR tab button.

iv Configure the parameters:

- CIR (Kbps)
- PIR (Kbps)
- CIR Adaptation
- PIR Adaptation

v Click on the OK button. A dialog box appears.

vi Click on the OK button.

5 Click on the Forwarding Classes tab button.

i Click on the Add button. The 7210 Network Egress Forwarding Class form opens.

ii Configure the parameters. You can create one entry for each of the eight forwarding class types.

- Forwarding Class
- In Profile
- Out Profile

iii Click on the OK button to close the 7210 Network Egress Forwarding Class (Create) form. A dialog box appears.

iv Click on the OK button.

v Repeat steps 5 i to 5 iv if you need to create additional rules. You can configure up to eight rules for one policy.

6 Click on the Apply button to save the policy. The 7210 Port Access Egress Policy form is refreshed with additional buttons.

7 Close the 7210 Port Access Egress Policy form. The Manage 7210 Port Access Egress Policies form reappears.

8 Click on the Distribute button to distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 43 for more information.

Procedure 44-5 To configure a 7210 SAS access egress policy

1 Choose Policies→QoS→SROS QoS→Access Egress→7210 Access Egress from the 5620 SAM main menu. The Manage 7210 Access Egress Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Access Egress Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Remarking

4 Click on the Select button in the Remarking Policy panel to choose a remarking policy. The Select Remarking Policy form opens.

5 Choose a remarking policy in the list and click on the OK button. The Select Remarking Policy form closes and the information is displayed.

6 Click on the Queues tab button. Eight default queues are displayed on the form.

i Choose a queue and click on the Properties button. The QueueEntry - 7210 Access Egress Policy (Create) form opens with the General tab displayed.

ii Modify the parameters, if required:

- ID
- Displayed Name
- Description
- Port Parent
- Weight
- CIR Level

iii Click on the Select button in the Queue Management Policy panel. The Select Queue Management Policy form opens.

iv Choose a queue management policy and click on the OK button. The Select Queue Management Policy form closes and the information is displayed.

v Click on the CIR/PIR tab button.

vi Configure the parameters:

- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

vii Click on the OK button. A dialog box appears.

viii Click on the OK button.

7 Click on the Apply button to save the policy. The 7210 Access Egress Policy form is refreshed with additional buttons.

8 Close the 7210 Access Egress Policy form. The Manage 7210 Access Egress Policies form reappears.

9 Click on the Distribute button to distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 43 for more information.

Procedure 44-6 To configure a network policy

1 Choose Policies→QoS→SROS QoS→Network→Network from the 5620 SAM main menu. The Manage Network Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Network Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Displayed Name
- Description
- Auto-Assign ID
- Default FC
- Default FC Profile
- LER Use DSCP
- Remark
- Force DSCP Remark

The Force DSCP Remark parameter only appears on the form if the Remark parameter is set to true.

4 Click on the Egress Forwarding Classes tab button. Eight default objects based on the eight forwarding classes, as described in Table 44-1, are displayed on the form. Configure the forwarding class parameters as required.

5 Double-click on a forwarding class. The network forwarding class form opens.

6 Configure the parameters:

- Use Queue Group
- Queue ID
- DSCP In Profile
- LSP Exp In Profile
- Dot1p In Profile
- Mark DE bit
- DSCP Out Profile
- LSP Exp Out Profile
- Dot1p Out Profile
- Force DE value

The Queue ID parameter is configurable only if the Use Queue Group is enabled. The Queue ID must be specified in the queue group template policy.

Note — If the Use Queue Group parameter is enabled for the global policy, the Queue ID is validated against the specified Queue Group Template Policy. When the global policy is distributed to an NE that does not support queue groups (for example, NEs with Release 7.0 R2 or earlier), the queue group-related properties are ignored.

7 Click on the OK button. The Forwarding Class (Create) form closes and a dialog box appears.

8 Click on the OK button. The Forwarding Class (Create) form closes and the Network Policy (Create) form reappears.

9 Specify how you want to configure the mapping between the ingress traffic and ingress queue by clicking on the appropriate tab button. Mapping is optional and can be based on combinations of customer QoS marking for LSP EXP Bits and Ingress DCSP. Table 44-8 describes the options.

Table 44-8 Network policy traffic-mapping configuration options

Tab button	Use
Ingress LSP EXP Bits	Maps the LSP EXP Bits of the ingress traffic to the ingress queue ID.
Ingress DCSP	Maps the DSCP of the ingress traffic to the ingress queue ID.
Ingress Dot1p	Maps the Dot1p tag of the ingress traffic to the ingress queue ID.

Perform the following substeps for each mapping that you want to configure.

i Click on the appropriate tab button.

ii Click on the Add button. A Create form opens.

iii Configure the parameters:

- Lsp Exp
- DSCP
- Dot1p
- Forwarding Class
- Profile

The Forwarding Class and Profile parameters appear on all forms. The Lsp Exp, DSCP, and Dot1p parameters appear only on the form with the same name as the parameter.

iv Click on the OK button to close the form. The policy form reappears with the newly created object displayed.

10 Click on the Apply button to save the policy. The Network Policy form is refreshed with additional buttons.

11 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

12 Close the Network Policy form. The Manage Network Policies form reappears.

13 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 44-7 To configure a 7210 SAS network policy

The network QoS policy consists of an ingress and egress component. The ingress component defines how Dot1p, DSCP, or LSP-Exp bits are mapped to an internal forwarding class and a profile state. The ingress component also defines how the forwarding classes are mapped to meters, and defines the meters of the QoS. The egress component performs remarking, which is enabled by default but can be configured. You can associate a 7210 SAS remarking policy with a 7210 SAS network policy. You can associate a 7210 SAS remarking policy with a 7210 SAS network policy.

1 Choose Policies→QoS→SROS QoS→Network→7210 Network from the 5620 SAM main menu. The Manage 7210 Network Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.
- **b** Click on the Create button. The 7210 Network Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Nw Mgr ID
- Policy Id
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Type
- Default FC
- Default FC Profile
- Remarking

4 Click on the Select button in the Remarking Policy panel. The Select Remarking Policy form opens.

5 Choose a remarking policy and click on the OK button. The Select Remarking Policy form closes and the information is displayed.

6 Click on the Egress Forwarding Classes tab button. Eight default objects based on the eight forwarding classes, as described in Table 44-1, are displayed on the form. Configure the forwarding class parameters, as required.

7 Double-click on a forwarding class. The 7210 Network Egress Forwarding Class (create) form opens.

8 Configure the parameters:

- Dot1p In Profile
- Dot1p Out Profile
- LSP Exp In Profile
- LSP Exp Out Profile
- DSCP In Profile
- DSCP Out Profile

9 Click on the OK button. The 7210 Network Egress Forwarding Class (create) form closes and a dialog box appears.

10 Click on the OK button.

11 Configure the mapping between the ingress traffic and ingress queue by clicking on the appropriate tab button. Table 44-9 describes the options.

Table 44-9 7210 SAS network policy traffic-mapping configuration options

Tab button	Use
Ingress LSP EXP Bits	Maps the LSP EXP Bits of the ingress traffic to the ingress queue ID.
Ingress DSCP	Maps the DSCP of the ingress traffic to the ingress queue ID.
Ingress Dot1p	Maps the Dot1p tag of the ingress traffic to the ingress queue ID.

Perform the following substeps for each mapping that you want to configure.

i Click on the appropriate tab button.

ii Click on the Add button. A Create form opens.

iii Configure the parameters:

- Lsp Exp
- DSCP
- Dot1p
- Forwarding Class
- Profile

The Forwarding Class and Profile parameters appear on all forms. The Lsp Exp, DSCP, and Dot1p parameters appear only on the form with the same name as the parameter.

iv Click on the OK button to close the form. The policy form reappears with the newly created object displayed.

12 Repeat step 11 for each new rule that you need to add. You can configure up to eight rules.

13 Click on the Ingress Meter tab button.

14 Click on the Add button. The Network Ingress Meter (create) form opens with the General tab displayed.

15 Configure the parameters:

- ID
- MultiPoint
- Mode

16 Click on the CIR/PIR tab button.

17 Configure the parameters:

- CIR Adaptation
- PIR Adaptation
- CIR (kbps)
- PIR (kbps)

18 Click on the Burst Size tab button.

19 Configure the parameters:

- Committed Burst Size (kbps)
- Maximum Burst Size (kbps)

20 Click on the Apply button. A dialog box appears.

21 Click on the OK button.

22 Repeat steps 15 to 21 if you need to create additional ingress meter rules.

23 Click on the Cancel button to close the NetWork Ingress Meter (Create) form.

24 Click on the Ingress FCMeter tab button.

25 Click the Add button. The 7210 Network Ingress Forwarding Class (create) form opens.

26 Configure the parameters:

- Forwarding Class
- Meter
- MultiCast-Meter

27 Click on the Apply button. A dialog box appears.

28 Click on the OK button.

29 Repeat steps 26 to 28 to add additional forwarding class mapping rules.

30 Click on the Cancel button to close the 7210 Network Ingress Forwarding Class (create) form.

31 Click on the Apply button. A dialog box appears.

32 Click on the OK button.

33 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 43 for more information.

Procedure 44-8 To configure a WRED slope policy

1 Choose Policies→QoS→SROS QoS→Slope→WRED Slope from the 5620 SAM main menu. The Manage Slope Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Slope Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

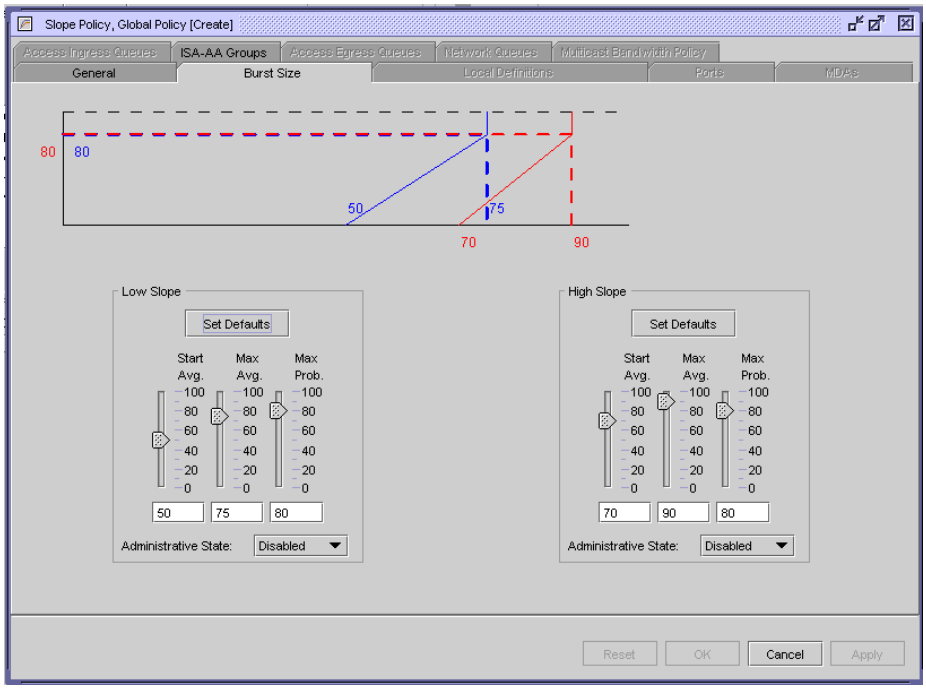
- Displayed Name
- Description
- Time Average Factor (weight)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

When packets are queued, shared buffer average utilization is calculated using the Time Average Factor for the buffer pool. The time average factor specifies the weighting between the previous shared buffer average utilization result and the new shared buffer utilization to determine the new shared buffer average utilization.

4 Click on the Burst Size tab button. The Burst Size form opens, as shown in Figure 44-4.

Figure 44-4 Slope policy form - Burst Size



Each buffer pool supports a high-priority RED slope and a low-priority RED slope. The high-priority RED slope manages access to the shared portion of the buffer pool for high-priority or in-profile packets. The low-priority RED slope manages access to the shared portion of the buffer pool for low-priority or out-of-profile packets. See "Slope policies" in this chapter for more information.

5 Configure the parameters for the Low Slope and the High Slope:

- Start Avg.
- Max Avg.
- Max Prob.
- Administrative State

6 Click on the Apply button to save the policy. The Slope Policy form is refreshed with additional buttons.

7 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

8 Close the Slope Policy form. The Manage Slope Policies form reappears.

9 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 44-9 To configure a 7210 SAS slope policy

The 7210 SAS supports SRED queue management. Default buffer pools are associated with each port. Each port has two associated buffer pools:

- access egress pool
- access uplink egress pool

Each pool is associated with a default slope policy that disables the low and high slopes within the pool.

1 Choose Policies→QoS→SROS QoS→Slope→7210 Slope from the 5620 SAM main menu. The Manage 7210 Slope Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Slope Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Burst Size tab button.

5 Configure the Low Slope and High Slope parameters:

- Administrative State
- Start Threshold
- Queue1 Drop Rate
- Queue2 Drop Rate
- Queue3 Drop Rate
- Queue4 Drop Rate
- Queue5 Drop Rate
- Queue6 Drop Rate
- Queue7 Drop Rate
- Queue8 Drop Rate

6 Click on the Queue Slope tab button. Eight default queues are displayed on the form.

7 Choose a queue and click on the Properties button. The QueueSlope, 7210 Slope Policy (Create) form opens.

8 Configure the Time Average Factor parameter.

9 Configure the parameters for the high slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

10 Configure the parameters for the low slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

11 Configure the parameters for the non-TCP slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The QueueSlope, 7210 Slope Policy (Create) form closes.

14 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 43 for more information.

15 Close the Slope Policy form. The Manage 7210 Slope Policies form reappears.

16 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 44-10 To configure an HSMDA WRED slope policy

1 Choose Policies→QoS→SROS QoS→Slope→HSMDA WRED Slope from the 5620 SAM main menu. The Manage HSMDA Slope Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The HSMDA Slope Policy (Create) form opens with the General tab displayed.

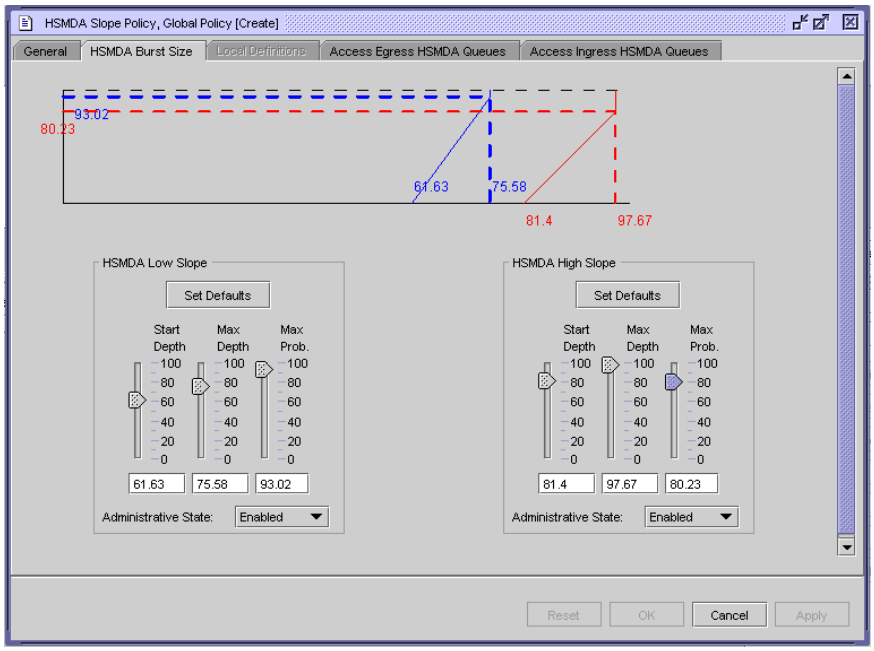
3 Configure the parameters:

- Displayed Name
- Description
- Queue MBS (bytes)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the HSMDA Burst Size tab button. The Burst Size form opens, as shown in Figure 44-5.

Figure 44-5 HSMDA Slope Policy form - Burst Size



Each buffer pool supports a high-priority RED slope and a low-priority RED slope. The high-priority RED slope manages access to the shared portion of the buffer pool for high-priority or in-profile packets. The low-priority RED slope manages access to the shared portion of the buffer pool for low-priority or out-of-profile packets. See "Slope policies" in this chapter for more information.

5 Configure the parameters for the Low Slope and the High Slope:

- Start Depth
- Max Depth
- Max Prob.
- Administrative State

6 Click on the Apply button to save the policy. The HSMDA Slope Policy form is refreshed with additional buttons.

7 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

8 Close the HSMDA Slope Policy form. The Manage HSMDA Slope Policies form reappears.

9 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 44-11 To configure a 7210 SAS queue management policy

Use a 7210 SAS queue management policy to configure slope parameters that specify a WRED profile for each queue. WRED is used to manage buffers during periods of congestion.

Note 1 — You can assign a 7210 SAS queue management policy to the queues of the following 7210 SAS policies:

- network queue policy
- access egress policy

Note 2 — You cannot modify a default 7210 SAS queue management policy.

1 Choose Policies→QoS→SROS QoS→Slope→7210 Queue Management from the 5620 SAM main menu. The Manage 7210 Queue Management Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Queue Management Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Scope
- Time Average Factor

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Configure the parameters for the burst size:

- Committed Burst Size (kbps)
- Maximum Burst Size (kbps)

5 Configure the parameters for the high slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

6 Configure the parameters for the low slope:

- Administrative State
- Start Average
- Max Average
- Max Probability

7 Click on the Apply button. The 7210 Queue Management Policy (Edit) form is refreshed with additional tab buttons.

8 Click on the following tab buttons to view information about a 7210 SAS queue management policy:

- Network Queues
- SAP Egress Queues
- Local Definitions
- Tree
- Faults

9 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 43 for more information.

10 Close the 7210 Queue Management Policy form. The Manage 7210 Queue Management Policies form reappears.

11 Click on the Search button to display the newly created policies in the bottom panel of the form.

Procedure 44-12 To configure a network queue policy

You cannot use the same policy on devices of different releases. For example, if the 5620 SAM manages a Release 7.0 7750 SR and a Release 8.0 7750 SR, you must create two network queue policies and distribute one to the Release 7.0 7750 SR and one to the Release 8.0 7750 SR.

1 Choose Policies→QoS→SROS QoS→Network Queue→Network Queue from the 5620 SAM main menu. The Manage Network Queue Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Network Queue Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button.

5 Click on the Queues tab button. Nine default queues are displayed on the form.

6 Perform one of the following:

a To configure a default queue, double-click on a queue in the list. The Entry, Network Queue Policy (Edit) form opens with the General tab displayed.

b To create a new queue, click on the Add button. The Entry, Network Queue Policy (Create) form opens with the General tab displayed.

7 Configure the parameters:

- ID
- Displayed Name
- Description
- Pool Name
- Multicast
- Expedite
- Port Average Overhead (%)
- Port Parent
- Level
- CIR Level
- Weight
- CIR Weight

Note 1 — You can use the Select button beside the Pool Name parameter to configure the parameter.

Note 2 — Before you can configure the Pool Name parameter, you must create a Q1 pool using Procedure 44-26.

8 Click on the Select button in the Slope Policy panel to choose a slope policy. The Select Slope Policy search form opens.

9 Select a policy in the list and click on the OK button. The Select Slope Policy form closes and the policy information is displayed on the Network Queue Policy form.

10 Click on the CIR/PIR tab button.

11 Configure the parameters:

- CIR (%)
- PIR (%)
- CIR Adaptation
- PIR Adaptation

12 Click on the Burst Size tab button.

13 Configure the parameters:

- High Priority Reserved (%)
- Committed Burst Size (%)
- Maximum Burst Size (%)

14 Click on the OK button. A dialog box appears.

15 Click on the OK button. The Entry, Network Queue Policy configuration form closes and the Network Queue Policy (Create) form reappears with a list of the network queues displayed.

16 Click on the Forwarding Classes tab button. Eight default objects based on the eight forwarding classes, as described in Table 44-1, are displayed on the form.

17 Perform one of the following:

a To configure a default forwarding class, double-click on a forwarding class in the list. The Forwarding Class, Network Queue Policy (Edit) form opens with the General tab displayed.

b To create a new forwarding class, click on the Add button. The Forwarding Class, Network Queue Policy (Edit) form opens with the General tab displayed.

18 Configure the parameters:

- Forwarding Class
  The Forwarding Class parameter can be configured only when you are creating a forwarding class network queue policy.
- Queue ID
- Multipoint Queue ID

19 Click on the OK button to close the forwarding class configuration form.

20 Click on the Distribute button to manually distribute the policy locally to devices. The Distribute - Network Queue form opens.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

The 5620 SAM automatically distributes an updated policy to a device when the policy is in use on the device.

i Select the devices in the Available Nodes panel to which you want to distribute the policy and click on the right arrow. The devices move to the Selected Nodes panel.

Note — A ninth queue is required to deploy a network queue policy to the 7450 ESS.

When there is no ninth queue, these devices do not appear in the Available Nodes panel.

ii Click on the Distribute button. The policy is distributed to the devices.

21 Click on the Apply button.

22 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

23 Close the Network Queue Policy form. The Manage Network Queue Policies form reappears.

24 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 44-13 To configure a 7210 SAS network queue policy

1 Choose Policies→QoS→SROS QoS→Network Queue→7210 Network Queue from the 5620 SAM main menu. The Manage 7210 Network Queue Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Network Queue (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

4 Click on the Queues tab button. Eight default queues are displayed on the form.

5 Double-click on a queue in the list. The NQueueEntry (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Displayed Name
- Description

7 Click on the Select button in the Queue Management Policy panel. The Select Queue Management Policy form opens.

8 Choose a queue management policy and click on the OK button. The Select Queue Management Policy form closes and the information is displayed.

9 Configure the parameters in the Port Parent panel:

- Port Parent
- Weight
- CIR Level

10 Click on the CIR/PIR tab button.

11 Configure the parameters:

- CIR (%)
- CIR Adaptation
- PIR (%)
- PIR Adaptation

12 Click on the OK button. The NQueueEntry (Create) form closes and a dialog box appears.

13 Click on the OK button. The 7210 Network Queue (Create) form reappears with a list of the network queues displayed.

14 Click on the Forwarding Classes tab button. Eight default objects based on the eight forwarding classes, as described in Table 44-1, are displayed on the form.

15 Click on the Cancel button to close the NQueueForwardingClass (View) form.

16 Click on the OK button to save the settings and close the 7210 Network Queue (Create) form.

17 Click on the Distribute button to manually distribute the policy locally to devices. The Distribute - Network Queue for 7210 form opens.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 43 for more information.

18 Click on the Apply button.

19 Close the Manage 7210 Network Queue Policies form.

Procedure 44-14 To modify a shared-queue policy

You cannot create shared-queue policies. Instead, you modify the existing default policy (default or policer-output-queues). Modification of shared-queue policies is supported on the 7750 SR and 7450 ESS.

Table 44-10 shows the default queue number, forwarding class, PIR, CIR, and CBS values for each shared queue.

Table 44-10 Shared queue default values

Queue #	FC	PIR (%)	CIR (%)	High priority reserved	CBS (%)	MBS (%)
1	be	100	0	10	3	25
2	l2	100	25	10	3	25
3	af	100	20	10	3	25
4	l1	100	25	10	10	50
5	h2	100	100	10	10	50
6	ef	100	100	10	10	50
7	h1	100	10	10	3	50
8	nc	100	10	10	1	50

The default behavior automatically chooses the expedited or non-expedited nature of the queue based on the forwarding classes mapped to it. As long as all forwarding classes mapped to the queue are expedited (nc, ef, h1 or h2), the queue is treated as an expedited queue by the hardware schedulers. When any non-expedited forwarding classes are mapped to the queue (be, af, l1 or l2), the queue is treated as best effort (be) by the hardware schedulers.

1 Choose Policies→QoS→SROS QoS→Shared Queue from the 5620 SAM main menu. The Manage Shared Queue Policies form opens.

2 Choose Local or Global from the Policy scope drop-down menu. When you set it to Local, you can specify the Local Node IP Address parameter and choose a device by using the Select button and selecting a device in the list.

3 Click on the Search button. The default shared-queue policy is listed.

4 Choose the policy in the list and click on the Properties button. The Shared Queue Policy (Edit) form opens with the General tab displayed.

5 Configure the Description parameter.

6 Click on the Queues tab button.

Table 44-11 list the queue IDs that are used by the 5620 SAM to identify the shared queue types.

Table 44-11 Shared queue types

Shared queue ID	Shared queue type
1 to 8	Unicast
9 to 16	Multicast
17 to 25	Broadcast
26 to 32	Unknown

There are 32 default queues are displayed on the form. Configure the queues as required. Only 16 queues are available for the policer-output-queues policy.

i Double-click on a queue in the list. The Queue configuration form opens with the General tab displayed.

ii Configure the Expedite and Pool Nameparameters.

Note — Before you can configure the Pool Name parameter, you must create a Q1 pool using Procedure 44-26.

iii Click on the CIR/PIR tab button.

iv Configure the parameters:

- CIR (%)
- PIR (%)

v Click on the Burst Size tab button.

vi Configure the parameters:

- High Priority Reserved (%)
- Committed Burst Size (%)
- Maximum Burst Size (%)

vii Click on the OK button. The queue configuration form closes and a dialog box appears.

viii Click on the OK button.

7 Click on the Forwarding Classes tab button.

Eight default objects based on the eight forwarding classes, as described in Table 44-10, are displayed on the form. You cannot associate different forwarding classes with the shared queues.

8 Click on the L2 Interfaces or L3 Interfaces tab button. (Applies to default shared queue policy only.)

9 Select an interface in the list and click on the Properties button. The L2 or L3 Access Interface form opens with the General tab displayed.

10 Click on the QoS tab button. (Applies to default shared queue policy only.)

11 Configure the Use Multipoint Shared Queue parameter.

12 Click on the OK button. The Shared Queue Policy form reappears.

13 Click on the Apply button to save the policy. The Shared Queue Policy (Edit) form refreshes.

To modify a local instance of the shared-queue policy, complete steps 1 to 5. Click on the Local Definitions tab. The shared-queue policies for each managed device are listed. Select a shared-queue policy in the list and click on the Properties button to modify the local instance of the policy. Complete steps 6 to 13.

Procedure 44-15 To configure a scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→Scheduler from the 5620 SAM main menu. The Manage Scheduler Policies form opens.

2 Perform one of the following:

   a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

   b Click on the Create button. The Scheduler Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Frame Based Accounting

4 Click on the Apply button.

5 Click on the Schedulers tab button.

   The scheduler defines bandwidth control that limits each child (other schedulers and queues) that are associated with the scheduler.

6 Click on the Add button. The Entry, Scheduler Policy (Create) form opens.

7 Configure the parameters:

- Displayed Name
- Description
- Tier

  The Tier parameter identifies the level of hierarchy with which a group of schedulers is associated. A parent is tier 1. Children are tier 2. Grandchildren are tier 3. You can create a tier 2 child scheduler without creating a parent tier 1 scheduler, and you can create a grandchild tier 3 scheduler without creating a child tier 2 scheduler.
- Summed CIR
- PIR (kbps)
- CIR (kbps)
- Parent Scheduler

  Click on the Select button to display a list of valid parent schedulers.
- Level
- CIR Level
- Weight
- CIR Weight
- Port Parent
- Level
- Weight
- CIR Level
- CIR Weight

The Parent Scheduler, Level, CIR Level, Weight, and CIR Weight parameters appear only when the Tier parameter is set to 2 or 3 and the Port Parent parameter is set to false.

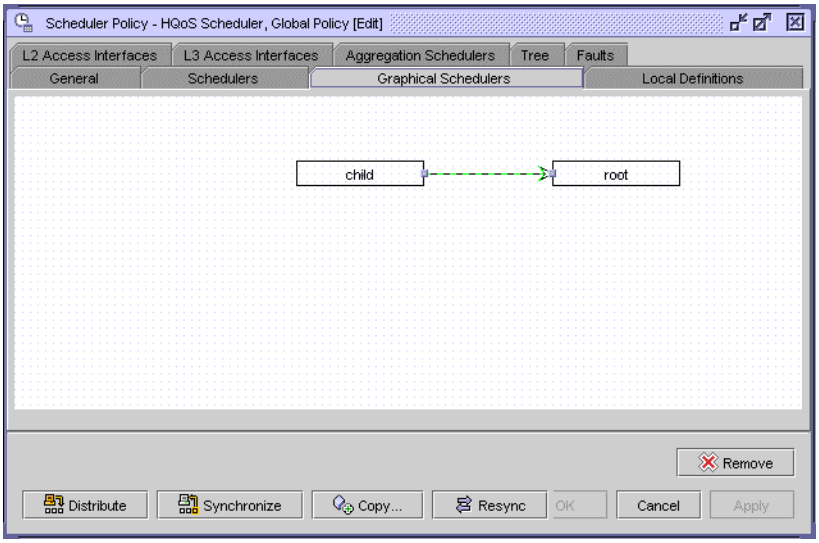
8 Click on the OK button. The Entry, Scheduler Policy (Create) form closes and a dialog box appears.

9 Click on the OK button. The newly configured scheduler is added to the list of schedulers.

10 To add additional schedulers to the policy, repeat steps 6 to 9.

11 Click on the Graphical Schedulers tab button to view a graphical display of the scheduler hierarchy within the scheduler policy. An example of the graphical display is shown in Figure 44-6.

Figure 44-6 Scheduler Policy form - Graphical Schedulers



12 Click on the Apply button.

13 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

14 Close the Scheduler Policy form. The Manage Scheduler Policies form reappears.

15 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 44-16 To configure an HSMDA scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→HSMDA Scheduler from the 5620 SAM main menu. The Manage HSMDA Scheduler Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The HSMDA Scheduler Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Maximum Rate (Mbps)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the HSMDA Group Rates tab button.

5 Configure the Rate (Mbps) parameter for group 1 and group 2.

6 Click on the HSMDA Scheduler Classes tab button.

7 Configure the parameters for classes 1 to 8:

- Group
- Weight
- Rate (Mbps)

The Group parameter must be configured with the same group (Group 1 or Group 2) for up to three sequential classes for each group. For example, when you configure Class 1 as Group 2, you can configure Class 2 and Class 3 as Group 2, but not as Group 1.

The Rate (Mbps) parameter is configurable when the Group parameter is set to None. The Weight parameter is configurable when the Group parameter is set to a value other than None.

8 Click on the Apply button.

9 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

10 Close the Scheduler Policy form. The Manage Scheduler Policies form reappears.

11 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 44-17 To configure a port scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→Port Scheduler from the 5620 SAM main menu. The Manage Port Scheduler Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Port Scheduler (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Maximum Rate (kbps)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

The Maximum Rate (kbps) parameter is configurable when the MAX check box is disabled.

4 Click on the Groups tab button.

5 Click on the Add button. The Port Scheduler Group (Create) form opens.

6 Configure the parameters:

- Displayed Name
- PIR (kbps)
- CIR (kbps)

The PIR (kbps) and CIR (kbps) parameters are configurable when the MAX check box is disabled for each.

7 Click on the Apply button. A dialog box appears.

8 Click on the OK button. The Port Scheduler Group (Create) form closes and the Port Scheduler (Create) form reappears.

9 Click on the Level tab button.

10 Click on the Select button in any of the Level panels to choose a port scheduler group from the list in the Select Group form. The port scheduler group must be preexisting on the port scheduler policy (see step 4).

11 Configure the parameters:

- PIR (kbps) (level 1)
- CIR (kbps) (level 1)
- Weight in group (level 1)
- PIR (kbps) (level 2)
- CIR (kbps) (level 2)
- Weight in group (level 2)
- PIR (kbps) (level 3)
- CIR (kbps) (level 3)
- Weight in group (level 3)
- PIR (kbps) (level 4)
- CIR (kbps) (level 4)
- Weight in group (level 4)
- PIR (kbps) (level 5)
- CIR (kbps) (level 5)
- Weight in group (level 5)
- PIR (kbps) (level 6)
- CIR (kbps) (level 6)
- Weight in group (level 6)
- PIR (kbps) (level 7)
- CIR (kbps) (level 7)
- Weight in group (level 7)
- PIR (kbps) (level 8)
- CIR (kbps) (level 8)
- Weight in group (level 8)
- Level
- Weight
- CIR Level
- CIR Weight

Note — Contiguous mapping of levels to a group is enforced. Priority levels cannot be added to a group unless the resulting set of priority levels is contiguous. When a level is not explicitly mapped to any group, it maps directly to the root of the port scheduler at its own priority.

The PIR (kbps) (level 1) to PIR (kbps) (level 8) and CIR (kbps) (level 1) to CIR (kbps) (level 8) parameters are configurable when the MAX check box is disabled for each.

The Weight in group (level 1) to Weight in group (level 8) parameters are configurable when a port scheduler group is associated with the port scheduler policy.

12 Click on the Apply button.

13 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

14 Close the Port Scheduler Policy configuration form. The Manage Port Scheduler Policies form reappears.

15 Close the Manage Port Scheduler Policies form.

Procedure 44-18 To configure a 7210 SAS port scheduler policy

1 Choose Policies→QoS→SROS QoS→Scheduler→7210 Port Scheduler from the 5620 SAM main menu. The Manage 7210 Port Scheduler Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The Port Scheduler (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Mode

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 If you selected a value of WeightedRoundRobin or WeightedDeficitRoundRobin for the Mode (mode) parameter, go to step 5. Otherwise go to step 7.

5 Click on the Queues tab button.

6 Configure the Weight parameter for queues 1 to 8.

7 Click on the Apply button.

8 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 43 for more information.

9 Close the Port Scheduler form. The Manage 7210 Port Scheduler Policies form reappears.

Procedure 44-19 To configure a policer control policy

1 Choose Policies→QoS→SROS QoS→Scheduler→Policer Control from the 5620 SAM main menu. The Manage Policer Control Policies form opens.

2 Perform one of the following steps.

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The Policer Control Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Arbiter tab button.

i Click on the Add button. The Arbiter (Create) form opens.

ii Configure the parameters:

- Arbiter Name
- Description
- Tier
- Priority Level
- Weight
- Frame Based Bandwidth Rate
- Parent Arbiter

  The Parent Arbiter parameter is configurable when the Tier parameter is set to 2.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The Arbiter (Create) form closes, and the Policer Control Policy form reappears.

5 (Optional step) Click on the Graphical Arbiters tab button to view a graphical display of the arbiter hierarchy within the policer control policy. You can perform any of the following steps.

   a Right-click on the grid and select New Arbiter from the drop-down menu. The Arbiter (Create) form opens. You can create a new arbiter, as described in step 4.

   b Right-click on an arbiter object and select Edit from the drop-down menu. The Arbiter (Edit) form opens. You can change the arbiter, as described in step 4.

   c Right-click on an arbiter and select Remove from the drop-down menu. The arbiter object is removed from the hierarchy.

   d Click on a Tier 2 arbiter object and draw a line to a Tier 1 arbiter object. The Tier 1 arbiter becomes the parent of the Tier 2 arbiter.

6 Click on the Tree tab button to view a hierarchical display of the policer control policy properties and sub components.

7 Click on the Priority Level tab button to configure the MBS contribution for eight priority levels. For each level, configure the following parameters:

- Cumulative MBS Contribution
- Fixed MBS contribution

8 Click on the Apply button.

9 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the network elements. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 43 for more information.

10 Close the Policer Control form. The Manage Policer Control Policies form reappears.

Procedure 44-20 To configure a named buffer pool policy

To associate a Named Buffer Pool to a MDA, see Procedure 17-41.

1 Choose Policies→QoS→SROS QoS→Buffer Pool→Named Buffer Pool from the 5620 SAM main menu. The Manage Named Buffer Pool Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Named Pool Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Default Weight
- MDA Weight
- Port Weight

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 To configure Q1 pools perform steps 3 to 10 in Procedure 44-26.

5 Click on the Apply button.

6 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

7 Close the Named Pool Policy form. The Manage Named Buffer Pool Policies form reappears.

8 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

9 Close the Manage Named Buffer Pool Policies form.

Procedure 44-21 To configure an ingress queue group template policy

1 Choose Policies→QoS→SROS QoS→Queue Group→Ingress Template from the 5620 SAM main menu. The Manage Ingress Queue Group Template Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Ingress Queue Group Template Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Queues tab button.

5 Perform one of the following:

a Specify a filter to search for and edit an existing queue. Use the filters to search for and open an existing queue by choosing a queue in the filtered list and clicking on the Properties button.

b Click on the Add button. The Ingress Queue, Ingress Queue Group Template Policy, Global Policy (Create) form opens with the General tab displayed.

6 Configure the parameters:

- ID
- Displayed Name
- Description
- Multicast
- Mode
- Policed
- Expedite

7 Configure the Named Buffer Pool parameter.

i Click on the Select button beside the Named Buffer Pool parameter. The Named Buffer Pool form opens.

Note — Before you can configure the Named Buffer Pool parameter, you must create a Named Buffer Pool policy using Procedure 44-20.

ii Specify a filter to search for existing policy.

iii Select the policy and click on the OK button. The Ingress Queue, Ingress Queue Group Template Policy, Global Policy (Create) form reappears.

8 Configure the Scheduler parameter.

i Click on the Select button beside the Scheduler parameter. The Schedulers form opens.

ii Specify a filter to search for existing scheduler.

iii Select the scheduler and click on the OK button. The Ingress Queue, Ingress Queue Group Template Policy, Global Policy (Create) form reappears.

iv Configure the parameters in the Scheduler Association panel.

- Level
- Weight
- CIR Level
- CIR Weight

9 Configure the CIR/PIR parameters.

i Click on the CIR/PIR tab button.

ii Configure the parameters:

- CIR (Kb/s)
- PIR (Kb/s)
- CIR Adaptation
- PIR Adaptation

Ensure that the CIR value is lower than the PIR value.

10 Configure the Burst Size parameters.

i Click on the Burst Size tab button.

ii Configure the parameters:

- Committed Burst Size (KB)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit

The parameters are configurable when the Default check box above each is deselected.

Ensure that the Committed Burst Size (KB) value is lower than the Maximum Burst Size (bytes) value.

iii Click on the OK button. A dialog box appears.

11 Close the Ingress Queue Group Template Policy form.

Procedure 44-22 To configure an egress queue group template policy

1 Choose Policies→QoS→SROS QoS→Queue Group→Egress Template from the 5620 SAM main menu. The Manage Egress Queue Group Template Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Egress Queue Group Template Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Queues tab button.

5 Perform one of the following:

a Specify a filter to search for and edit an existing queue. Use the filters to search for and open an existing queue by choosing a queue in the filtered list and clicking on the Properties button.

b Click on the Add button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form opens with the General tab displayed.

6 Configure the parameters:

- ID
- Displayed Name
- Description
- Port Parent
- Rate Type
- Expedite
- Level
- Weight
- CIR Level
- CIR Weight

The Level, Weight, CIR Level, and CIR Weight parameters are configurable only if the Port Parent parameter is set to True.

7 Configure the Named Buffer Pool parameter.

i Click on the Select button beside the Named Buffer Pool parameter. The Named Buffer Pool form opens.

Note — Before you can configure the Named Buffer Pool parameter, you must create a Named Buffer Pool policy using Procedure 44-20.

ii Specify a filter to search for existing policy.

iii Select the policy and click on the OK button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form reappears.

8 Configure the Scheduler parameter.

i Click on the Select button beside the Scheduler parameter. The Schedulers form opens.

Note — The Scheduler parameter is configurable only if you set the Port Parent parameter to False.

ii Specify a filter to search for existing scheduler.

iii Select the scheduler and click on the OK button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form reappears.

iv Configure the parameters in the Scheduler Association panel.

- Level
- Weight
- CIR Level
- CIR Weight

9 Configure the WRED Queue parameters.

i Select the Use WRED Queue parameter.

ii Click on the Select button beside the Displayed Name parameter. The Select WRED Queue Slope Policy form opens.

Note — Before you can select a WRED Queue Slope policy, you must create the policy using Procedure 44-8.

iii Specify a filter to search for existing policy.

iv Select the WRED Slope policy and click on the OK button. The Egress Queue, Egress Queue Group Template Policy, Global Policy (Create) form reappears.

10 Configure the CIR/PIR parameters.

i Click on the CIR/PIR tab button.

ii Configure the parameters:

The choice of CIP and PIR parameter definitions depends on the Rate Type parameter setting on the General tab.

- CIR (Kb/s) - if Rate Type parameter is set to Specific
- PIR (Kb/s) - if Rate Type parameter is set to Specific
- CIR (percentage) - if Rate Type parameter is set to Percentage
- PIR (Percentage) - if Rate Type parameter is set to Percentage
- CIR Adaptation
- PIR Adaptation

Ensure that the CIR value is lower than the PIR value.

11 Configure the Burst Size parameters.

i Click on the Burst Size tab button.

ii Configure the parameters:

- Committed Burst Size (KB)
- Maximum Burst Size (bytes)
- High Priority Reserved
- Burst Limit

The parameters are configurable when the Default check box above each is deselected.

Ensure that the Committed Burst Size (KB) value is lower than the Maximum Burst Size (bytes) value.

iii Click on the OK button. A dialog box appears.

12 Click on the Forwarding Classes tab button.

13 Perform one of the following:

a Specify a filter to search for and edit an existing forwarding class. Use the filters to search for and open an existing forwarding class by choosing a forwarding class in the filtered list and clicking on the Properties button.

b Click on the Add button. The Forwarding Class (Create) form opens.

14 Configure the parameters:

- Forwarding Class
- Queue ID

15 Close the Egress Queue Group Template Policy form.

Procedure 44-23 To configure a 7705 SAR fabric profile

1 Choose Policies→QoS→SROS QoS→7705 SAR Fabric from the 5620 SAM main menu. The Manage Fabric Profiles form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The 7705 SAR Fabric Profile (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Mode

4 Click on the Rates tab button. In Aggregate mode, one rate is displayed. In Destination mode, six rates are displayed. Perform one of the following:

a For Aggregate mode, configure the Aggregate Rate parameter to set the fabric shaping rate to the daughter card slots.

b For Destination mode, configure the Rate to MDA parameter for each daughter card slot to set the fabric shaping rate to each daughter card.

5 Click on the Apply button. The form changes to enable the other tabs.

6 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

7 Close the 7705 SAR Fabric form. The Manage 7705 SAR Fabric form is updated.

8 Click on the Search button to display the newly created profile or profiles in the bottom panel of the form.

9 Close the Manage 7705 SAR Fabric form.

Procedure 44-24 To configure a 7210 SAS remarking policy

The 7210 SAS remarking policy is used to configure the remarking behavior for the NE at the egress of the access SAPs, ports, and IP interfaces. A 7210 SAS remarking policy can be associated with the following 7210 SAS QoS policies:

- Port Access Egress Policy (the remarking policy must be DOT1P or DOT1P-LSP-EXP SHARED)
- Network Policy (the remarking policy must be LSP-EXP or DOT1P-LSP-EXP SHARED)
- Network Queue Policy (the remarking policy must be DOT1P-DSCP, DOT1P, or DSCP)

1 Choose Policies→QoS→SROS QoS→7210 Remarking from the 5620 SAM main menu. The Manage Remarking Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and choose a policy. Click on the Properties button to modify the policy.

b Click on the Create button. The 7210 Remarking Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Policy Id
- Auto-Assign ID
- Displayed Name
- Description
- Type

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button. The 7210 Remarking Policy (Edit) form appears with the General tab displayed.

5 Click on the Forwarding Classes tab button. Eight default objects based on the eight forwarding classes, as described in Table 44-1, are displayed on the form. Configure the forwarding class parameters, as required.

6 Double-click on a forwarding class. The 7210 Remark Forwarding Class (Edit) form opens.

7 Configure the parameters:

- Dot1P-LSP-EXP-Shared In Profile
- Dot1P-LSP-EXP-Shared Out Profile

8 Click on the OK button. The 7210 Remark Forwarding Class (Edit) form closes and the 7210 Remarking Policy (Edit) form appears.

9 Click on the OK button. A dialog box appears.

10 Click on the Yes button. The 7210 Remarking Policy (Edit) form closes and the Manage Remarking Policies form appears.

11 Click on the Search button to display a list of 7210 remarking policies.

12 Choose a 7210 remarking policy and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution, which also distributes the policy to existing local definitions. See chapter 43 for more information.

Procedure 44-25 To configure an HSMDA pool policy

To associate an HSMDA buffer pool with an MDA, see Procedure 17-41.

1 Choose Policies→QoS→SROS QoS→Buffer Pool→HSMDA Pool from the 5620 SAM main menu. The Manage HSMDA Pool Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The HSMDA Pool Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- System Reserve (%)

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Root Pools tab button.

5 Configure the Allocation Weight parameter for root pools 1 to 8.

The Allocation Weight parameter is configurable when the Default check box is disabled.

6 Click on the Class Pools tab button.

7 Configure the parameters for root pools 1 to 8:

- Root Parent
- Allocation Percent

The Allocation Percent parameter is configurable when the Default check box is disabled.

8 Click on the Apply button.

9 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

10 Close the HSMDA Pool Policy form. The Manage HSMDA Pool Policies form reappears.

11 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

12 Close the Manage HSMDA Pool Policies form.

Procedure 44-26 To configure Q1 pools

You must configure a Q1 pool to before you can assign the pool to an access ingress, access egress, network queue or shared queue policy.

1 Choose Policies→QoS→SROS QoS→Buffer Pool→Named Buffer Pool from the 5620 SAM main menu. The Manage Named Buffer Pool Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Named Pool Policy (Create) form opens with the General tab displayed.

3 Click on Q1 Pool tab button. A list of configured Q1 Pools is displayed.

4 Perform one of the following steps:

a Select an existing Q1 pool. A Ql Pool (Edit) form opens with the General tab displayed. Go to step 5.

b Click on the Add button. A Q1 Pool (Create) form opens with the General tab displayed. Go to step 5.

5 Configure the parameters:

- Pool Name
- Description
- Network Weight
- Access Weight

6 Click on the Select button beside the Displayed Name parameter. The Select Slope Policy - Q1 Pool list form opens.

7 Select a policy in the list and click on the OK button. The Select Slope Policy - Q1 Pool list form closes and the Q1 Pool (Create) form is refreshed with the slope policy information.

8 Configure the remaining parameters:

- Reserved CBS (%)
- Default Reserved CBS

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The Q1 Pool configuration form closes and the Named Pool Policy form reappears.

11 Click on the Ok button. A dialog box appears.

12 Click on the OK button. The Named Pool Policy configuration form closes and the Manage Named Buffer Pool Policies form reappears.

13 Close the Manage Named Buffer Pool Policies form.

Procedure 44-27 To create an aggregation scheduler

You can create an aggregation scheduler when you have created two or more scheduler policies. See "Hierarchical schedulers" in this chapter for more information.

1 Create two or more scheduler policies, as described in Procedure 44-15.

2 Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.

3 Specify a filter to search for an existing customer and click on the Search button.

4 Select a customer in the list and click on the Properties button. The Customer (Edit) form opens.

5 Click on the Sites tab button.

6 Select a site in the list and click on the Properties button. The Site (Edit) form opens.

7 Click on the Aggregation tab button.

8 Click on the Add button. The Create Aggregation Scheduler wizard opens.

9 Select a site in the list and click on the Next button.

10 Configure the parameters:

- Scheduler Name
- Description

11 Click on the Next button. The Select Assignment Scope step is displayed.

12 Configure the Select Assignment Scope parameter.

13 Click on the Next button. The Select Card or the Select Port step is displayed, depending on the option chosen for the Select Assignment Scope parameter.

14 Click on the Select button to specify a card or port. The Select Card - Aggregation Scheduler form or the Select Site - Aggregation Scheduler form opens.

15 Select a card or port in the list and click on the OK button. The Select - Aggregation Scheduler form closes and the card or port information is displayed on the Select Card or Select Port form.

16 Click on the Next button. The Select Ingress and Egress Scheduler Policies step is displayed.

17 Click on the Select buttons to choose ingress and egress scheduler policies. The Select Policy - Aggregation Scheduler form opens.

18 Set the filter criteria, if required, and click on the Search button. A list of policies is displayed.

19 Select a policy in the list and click on the OK button. The Select Policy - Aggregation Scheduler form closes and the policy information is displayed in the Select Ingress and Egress Scheduler Policies form.

20 Click on the Next button. The Select Time Of Day Suite Policy step is displayed.

21 Click on the Select button to choose a time of day suite. The Select Time Of Day Suite - Aggregation Scheduler form opens.

22 Select a time of day suite entry and click on the OK button. The Select Time Of Day Suite - Aggregation Scheduler form closes and the policy information is displayed in the Select Time Of Day Suite Policy form.

23 Click on the Finish button. A dialog box appears.

24 Click on the OK button. The aggregation scheduler is listed in the Aggregation tab of the Site (Edit) form.

25 Close the Site (Edit) form. The Customer (Edit) form reappears.

26 Click on the OK button. A dialog box appears.

27 Click on the Yes button. The Customer (Edit) form closes and the Manage Customers form reappears.

28 Close the Manage Customers form.

Procedure 44-28 To configure an ANCP MSS static map

You can configure an ANCP MSS static map when you have created an ANCP policy and an aggregation scheduler.

1 Create an ANCP policy, as described in Procedure 64-16.

2 Create an aggregation scheduler, as described in Procedure 44-27.

3 Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.

4 Select a customer in the list and click on the Properties button. The Customer (Edit) form opens.

5 Click on the Aggregation tab button.

6 Select a site in the list and click on the Properties button. The Aggregation Scheduler (Edit) form opens.

7 Click on the ANCP Static Map button.

8 Select an ANCP policy in the list and click on the Add button. The ANCP MSS Static Map (Create) form opens.

9 Configure the parameters:

- ANCP String
- Displayed Name

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The ANCP Policy is listed in the ANCP Static Map tab of the Aggregation Scheduler (Edit) form.

12 Click on the OK button to close the Aggregation Scheduler (Edit) form. The Customer (Edit) form reappears.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button.

15 Close the Manage Customers form.

Procedure 44-29 To configure an ATM QoS policy

1 Choose Policies→QoS→SROS QoS→ATM QoS from the 5620 SAM main menu. The Manage ATM QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The ATM QoS Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Displayed Name
- Description

4 Click on the QoS tab button.

5 Configure the parameters:

- Service Category
- MIR (kbps)
- PIR (kbps)
- CDVT
- Shaping
- Policing
- Descriptor Type
- CLP Tagging

6 Click on the OK button to save the policy. The ATM QoS Policy (Create) form closes and the Manage ATM QoS Policies form reappears.

7 Click on the Search button to display the newly created policy or policies.

8 Choose a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

9 Close the Manage ATM QoS Policies form.

Procedure 44-30 To configure a 9500 MPR ATM QoS policy

1 Choose Policies→QoS→9500 MPR QoS→ 9500 ATM QoS from the 5620 SAM main menu. The 9500 ATM QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The 9500 ATM QoS Policy, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Displayed Name

4 Click on the QoS tab button.

5 Configure the parameters:

- Domain Name
- Service Category
- Policing
- PCR
- CDVT
- MDCR

6 Click on the OK button to save the policy. The ATM QoS Policy (Create) form closes and the 9500 ATM QoS Policies form reappears.

7 Click on the Search button to display the newly created policy or policies.

8 Choose a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

9 Close the 9500 ATM QoS Policies form.

Procedure 44-31 To configure a 7250 SAS or Telco QoS level policy

1 Choose Policies→QoS→7250 SAS and Telco QoS from the 5620 SAM main menu. The Manage 7250 SAS and Telco QoS Node Level Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The 7250 SAS and Telco Qos Node Level Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Displayed Name
- Description
- Queue Algorithm

4 If the Queue Algorithm parameter is set to Strict Priority, go to step 6.

5 Click on the Scheduling Tx Queue tab button.

i Configure the Txq 0 to Txq 7 parameters, depending on the number of queues. There is one Txq parameter for each queue. The number of queues and Txq parameters depends on the Queue Algorithm parameter value chosen in step 3.

ii Repeat step i for each Txq parameter on the Scheduling Tx Queue tab.

6 Click on the Traffic Class Entries tab button.

7 Click on the Add button. The QoSTrafficClassEntry (Create) form opens.

8 Configure the parameters:

- Traffic Class
- DSCP
- Priority
- Color
- DSCP Value

The DSCP Value parameter is configurable when the DSCP parameter is enabled.

9 To add more policy entries, repeat steps 7 to 8.

10 Click on the OK button. The QoSTrafficClassEntry (Create) form closes and the Manage 7250 SAS and Telco QoS Node Level Policies form reappears.

11 Click on the Search button to display the newly created policy or policies.

12 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

13 Close the Manage 7250 SAS and Telco QoS Node Level Policies form.

Procedure 44-32 To configure an OmniSwitch QoS policy condition

Note — OmniSwitch QoS policies consist of a condition and an action. You must configure at least one condition and one action before you can create a policy.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing condition. Select a condition in the filtered list and click on the Properties button.

b Click on the Create button and choose Create QoS Condition. The AOS QoS Condition, Global Policy (Create) form opens with the General tab displayed.

3 Configure the Displayed Name parameter.

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Filter Properties tab button. The Filter Properties form opens with the Port tab displayed.

5 Configure the parameters in the Port Match Criteria panel, if required:

- Match Source Port
- Source Slot
- Source Port
- Match Destination Port
- Destination Slot
- Destination Port

6 Click on the Layer 2 tab button.

7 Configure the parameters in the MAC Match Criteria panel, if required:

- Source MAC
- Source Mask
- Destination MAC
- Destination Mask

8 Configure the Source VLAN parameter in the Source VLAN Match Criteria panel, if required.

9 Configure the Priority parameter in the 802.1p Match Criteria panel, if required.

10 Click on the Layer 3 tab button.

11 Configure the parameters in the IP Match Criteria panel:

- Source IP
- Source Mask
- Source Net Mask
- Destination IP
- Destination Mask
- Destination Net Mask
- VRF Status
- VRF Name

12 Configure the parameters in the DSCP Match Criteria panel, if required:

- Differentiated Services Code Point
- Mask

13 Configure the parameters in the ToS Match Criteria panel, if required:

- ToS Precedence
- Mask

14 Configure the parameters in the ICMP Match Criteria panel, if required:

- ICMP Code
- ICMP Type

15 Click on the Layer 4 tab button.

16 Configure the IP Protocol parameter.

The following parameters are not displayed when the IP Protocol parameter is set to HOPOPT.

17 Configure the parameters in the IP Port Match Criteria panel, if required:

- Match Source IP Port Range
- Source IP Port (Start)
- Source IP Port (End)
- Match Destination IP Port Range
- Destination IP Port (Start)
- Destination IP Port (End)

18 Click on the OK button. The AOS QoS Condition, Global Policy (Create) form closes.

19 To create more QoS policy conditions, repeat steps 2b to 18.

20 Close the AOS QoS Policies form.

Procedure 44-33 To configure an OmniSwitch QoS policy action

Note — OmniSwitch QoS policies consist of a condition and an action. You must configure at least one condition and one action before you can create a policy.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing action. Select an action in the filtered list and click on the Properties button.

b Click on the Create button and choose Create QoS Action. The AOS QoS Action, Global Policy (Create) form opens with the General tab displayed.

Note — You cannot use DSCP and ToS parameters in the same action.

3 Configure the Displayed Name parameter.

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Configure the Action parameter in the Disposition panel.

5 Configure the parameters in the Priority and Bandwidth panel:

- Priority
- Maximum Bandwidth (Kbps)
- Share Resources

6 Configure the Priority parameter in the 802.1p panel.

7 Configure the Differentiated Services Code Point parameter in the DSCP panel.

8 Configure the Type of Service parameter in the ToS panel.

9 Configure the parameters in the Redirect panel, if required.

- Slot
- Port
- LAG Number

10 Click on the OK button. The AOS QoS Action, Global Policy (Create) form closes.

11 To create more actions, repeat steps 2b to 10.

12 Close the AOS QoS Policies form.

Procedure 44-34 To create an OmniSwitch QoS policy

Note — OmniSwitch QoS policies consist of a condition and an action. You must configure at least one condition and one action before you can create a policy.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button and choose Create QoS Policy. The AOS QoS Policy, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Policy Status
- Precedence

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Select button in the Action panel to choose an action for the policy. The Select Action - QoS Policy form opens with a list of available actions displayed.

5 Select an action and click the OK button. The Select Action - QoS Policy form closes and the AOS QoS Policy, Global Policy (Create) form refreshes.

6 Click on the Select button in the Condition panel to choose a condition for the policy. The Select Action - QoS Policy form opens with a list of available conditions displayed.

7 Select a condition and click the OK button. The Select Condition - QoS Policy form closes and the AOS QoS Policy, Global Policy (Create) form refreshes.

8 To create more policies, repeat steps 2b to 9.

9 Click on the OK button. The AOS QoS Policy, Global Policy (Create) form closes and the AoS QoS Policies form reappears.

10 Click on the Search button to display the newly created policy or policies.

11 Select a policy and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is dimmed and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

12 Close the AOS QoS Policies form.

Procedure 44-35 To create an OmniSwitch QoS list

This procedure is used to configure a QoS list, which is a collection of QoS polices. This QOS list includes support of egress policy configurations to perform last minute operations on the data traffic before it egresses through the port.

See Procedures 44-32, 44-33, and 44-34 to create AOS QoS policy actions, policy conditions, and policies.

1 Choose Policies→QoS→AOS QoS Policies from the 5620 SAM main menu. The AOS QoS Policies form opens.

2 Click on the Create button and choose Create QoS List. The AOS QoS Policy, Global Policy (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Displayed Name
- List Type
- Policy Status

Note — Do not use a colon to create the displayed name because the 5620 SAM uses colons as separators for the object full name.

4 To add an AOS QoS policy to the QoS list, click on the List Policies tab button.

5 Click on the Add button. The AOS QoS Policy List, AOS QoS List, Global Policy (Create) form opens.

6 Click on the Select button. The Select Policy Name - QoS Policy List- AOS QoS List, Global Policy form opens.

7 Select a policy entry. Click on the OK button. The Select Policy Name - QoS Policy List- AOS QoS List, Global Policy form closes.

8 The Select Policy Name - QoS Policy List- AOS QoS List, Global Policy form reappears, with the policy name selected in Step 7 displayed in the Displayed Name field.

9 Click on the Properties button. The AOS QoS Policy -<policy name>, Global Policy (Edit) form opens.

10 If required, configure the Precedence parameter.

11 Close the AOS QoS Policy -<policy name>, Global Policy (Edit) form

12 The AOS QoS Policy List, AOS QoS List, Global Policy (Create) form reappears. Click on the OK button. A dialog box appears.

13 Click on the OK button.

14 Close the AOS QoS Policy, Global Policy (Create) form.

Procedure 44-36 To create or configure a MC MLPPP ingress QoS profile

1 Choose Policies→QoS→SROS QoS→MLPPP→Ingress QoS Profile from the 5620 SAM main menu. The Manage MLPPP Ingress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.

Note — You can edit the properties of the default ingress MC profile, but you cannot delete the profile.

b Click on the Create button. The MLPPP Ingress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MLPPP Ingress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab button.

6 Select a class in the list and click on the Properties button. The MlpppIngressQosProfileClass (Edit) form opens.

7 Configure the Reassembly Timeout (msec) parameter.

8 Click on the OK button to save the values and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MLPPP Ingress QoS Profile (Edit) form closes.

12 Click on the Search button to display any newly created policy or policies in the bottom panel of the form.

13 Close the Manage MLPPP Ingress QoS Profile form.

Procedure 44-37 To create or configure a MC MLPPP egress QoS profile

1 Choose Policies→QoS→SROS QoS→MLPPP→Egress QoS Profile from the 5620 SAM main menu. The Manage MLPPP Egress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.

Note — You can edit the properties of the default egress MC profiles, but you cannot delete them.

b Click on the Create button. The MLPPP Egress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MLPPP Egress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab button.

6 Select a class in the list and click on the Properties button. The MlpppEgressQosProfileClass (Edit) form opens.

7 Configure the following parameters:

- MIR (%)
- Weight (%)
- Maximum Queue Size (msec)

8 Click on the OK button to save the changes and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the Forwarding Classes tab button.

11 Select a forwarding class in the list and click on the Properties button. The MlpppEgressQosProfileForwardingClass (Edit) form opens.

12 Configure the MLPPP Class parameter.

13 Click on the OK button to save the values and close the form.

14 Repeat steps 11 to 13 for each forwarding class that you need to configure.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The MLPPP Ingress QoS Profile (Edit) form closes.

17 Click on the Search button to display any newly created policies in the bottom panel of the form.

18 Close the Manage MLPPP Egress QoS Profile form.

Procedure 44-38 To create or configure an MCFR ingress QoS profile

1 Choose Policies→QoS→SROS QoS→MCFR→Ingress QoS Profile from the 5620 SAM main menu. The Manage MCFR Ingress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.

Note — You can edit the properties of the default ingress MC profile, but you cannot delete the profile.

b Click on the Create button. The MCFR Ingress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MCFR Ingress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab button.

6 Select a class in the list and click on the Properties button. The MCFR Ingress QoS Profile Class (Edit) form opens.

7 Configure the Reassembly Timeout (msec) parameter.

8 Click on the OK button to save the values and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MCFR Ingress QoS Profile (Edit) form closes.

12 Click on the Search button to display any newly created policies in the bottom panel of the form.

13 Close the Manage MCFR Ingress QoS Profile form.

Procedure 44-39 To create or configure an MCFR egress QoS profile

1 Choose Policies→QoS→SROS QoS→MCFR→Egress QoS Profile from the 5620 SAM main menu. The Manage MCFR Egress QoS Profile form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing profile. Use the filters to search for and open an existing profile by choosing a profile in the filtered list and clicking on the Properties button.

Note — You can edit the properties of the default egress MC profile, but you cannot delete the profile.

b Click on the Create button. The MCFR Egress QoS Profile (Create) form opens with the General tab displayed.

3 Configure the following parameters:

- Auto-Assign ID
- Profile ID
- Description

4 Click on the Apply button. The MCFR Egress QoS Profile (Edit) form opens with the General tab displayed.

5 Click on the Classes tab button.

6 Select a class in the list and click on the Properties button. The MCFR Egress QoS Profile Class (Edit) form opens.

7 Configure the following parameters:

- MIR (%)
- Weight (%)
- Maximum Queue Size (msec)

8 Click on the OK button to save the changes and close the form.

9 Repeat steps 6 to 8 for each class that you need to configure.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The MCFR Egress QoS Profile (Edit) form closes.

12 Click on the Search button to display any newly created policies in the bottom panel of the form.

13 Close the Manage MCFR Egress QoS Profile form.

Procedure 44-40 To configure QoS policy overrides on an L2 or L3 access interface

Use this procedure to override some or all settings associated with an access ingress, access egress, or scheduler policy on an L2 or L3 access interface configured for a service.

See the following procedures for information about overriding access ingress, access egress, or scheduler policies that are associated with residential subscribers:

- Procedure 64-3 for the overrides associated with SLA profiles
- Procedure 64-2 for the overrides associated with subscriber profiles

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens with Service (Service Management) selected in the filter list.

2 Choose Access Interface (Service Management) from the object drop-down list.

3 Click on one of the following icons listed below the Access Interface (Service Management) icon.

- L2 Access Interface (Service Management)
- L3 Access Interface (Service Management)

4 Set the filter criteria, if required, and click on the Search button. A list of L2 or L3 access interfaces is displayed.

5 Select an interface in the list and click on the Properties button. Based on the interface that you chose in step 3, the L2 Access Interface form or L3 Access Interface form opens.

6 Perform one of the following:

a Create an override for an access ingress or access egress policy queue. Go to step 7.

b Create an override for an access ingress or access egress policy HSMDA queue. Go to step 14.

c Create an override for an ingress or egress policy policer. Go to step 21.

d Create an override for an ingress or egress policer control policy. Go to step 29.

e Create an override for an ingress or egress scheduler policy. Go to step 40.

7 Click on the Override tab button. Perform one of the following actions.

a Click on the Access Ingress Queues tab button.

b Click on the Access Egress Queues tab button.

8 Click on the Add button.

Based on the tab that you selected in step 7, the Access Ingress Queue Override form or the Access Egress Queue Override form opens with the General tab displayed.

9 Choose the policy queue that you want to override.

i Click on the Select button. The policy queue form opens.

ii Choose the policy queue.

iii Click on the OK button. The queue override form reappears with the configured values for the policy queue.

10 Click on the Override tab button.

11 Configure the parameters:

- Override PIR
- Override CIR
- Override Maximum Burst Size
- Override Committed Burst Size
- Override High Priority Reserved
- Override PIR Adaptation
- Override CIR Adaptation
- Override Queue Weight
- Override Queue CIR Weight
- Override Port Average Overhead
- Default
- PIR (kbps)
- CIR (kbps)
- Maximum Burst Size (bytes)
- Committed Burst Size (KB)
- High Priority Reserved
- CIR Adaptation
- PIR Adaptation
- Queue Weight
- Queue CIR Weight
- Port Average Overhead (%)

The Override Port Average Overhead and Port Average Overhead (%) parameters are configurable only for access egress queues.

12 Click on the OK button. A dialog box appears.

13 Click on the OK button. The queue override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

14 Click on the Override tab button. Perform one of the following actions.

a Click on the Access Ingress HSMDA Queues tab button.

b Click on the Access Egress HSMDA Queues tab button.

15 Click on the Add button.

Based on the tab that you selected in step 14, the Access Ingress HSMDA Queue Override form or the Access Egress HSMDA Queue Override form opens with the General tab displayed.

16 Choose the policy queue that you want to override.

i Click on the Select button. The policy queue form opens.

ii Choose the policy queue.

iii Click on the OK button. The queue override form reappears with the configured values for the policy queue.

17 Click on the Override tab button.

18 Configure the parameters:

- Override PIR
- Override CIR
- PIR (kbps)
- CIR (kbps)

19 Click on the OK button. A dialog box appears.

20 Click on the OK button. The queue override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

21 Click on the Override tab button. Perform one of the following actions.

a Click on the Ingress Policer tab button.

b Click on the Egress Policer tab button.

22 Click on the Add... button. The policer override form opens.

23 Click on the Select button. The select policy policer form opens.

24 Select a policy policer and click on the OK button. The select policy policer form closes and the policer override form refreshes with the configured values for the policy policer.

Note — Policy policers must be applied to the L2 Access Interface or the L3 Access Interface in order to be selected.

25 Click on the Override tab button.

26 Enable the Override check box for any of the following parameters, and then configure the parameters:

- PIR (kbps)
- CIR (kbps)
- Maximum Burst Size (bytes)
- Committed Burst Size (KB)
- Packet Byte Offset
- Default
- Stats Mode

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The policer override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

29 Perform one of the following actions.

a Click on the Ingress Policer Control tab button.

b Click on the Egress Policer Control tab button.

Note — Policer control policies must be applied to the L2 Access Interface or the L3 Access Interface in order to enable the policer control tab buttons.

30 Click on the Add... button. The policer override form opens.

31 Enable the Override check box for any of the following parameters, and then configure the parameters:

- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space

32 Click on the Level Override tab button.

33 Select a Level Override from the list and click on the Properties button. The policy policer level override form opens with the General tab displayed.

34 Click on the Override tab button.

35 Enable the Override check box and then configure the Maximum Cumulative Buffer Space parameter.

36 Click on the OK button. A dialog box appears.

37 Click on the OK button. The policy policer level override form closes and the policer override form reappears.

38 Click on the OK button. A dialog box appears.

39 Click on the OK button. The policer override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

40 Click on the Schedulers tab button.

41 Choose the scheduler policy that you want to override.

i Click on the Select button to define the Ingress Scheduler and Egress Scheduler policy that you want to modify.

ii Choose the scheduler policy.

iii Click on the Apply button. A dialog box appears.

iv Click on the Yes button. The L2 Access Interface form or L3 Access Interface form reappears.

42 Click on the Overrides tab button.

43 Perform one of the following actions.

a Modify the Ingress Scheduler parameters.

i Click on the Ingress tab button.

ii Click on the Add button.

The Ingress policy scheduler override form opens with the General tab displayed.

b Modify the Egress Scheduler parameters.

i Click on the Egress tab button

ii Click on the Add button.

The Egress Policy Scheduler Override form opens with the General tab displayed.

44 Choose the scheduler policy that you want to override.

i Click on the Select button. The scheduler policy entry form opens.

ii Choose the policy entry.

iii Click on the OK button. The scheduler entry override form reappears with the configured values for the scheduler policy.

45 Click on the Override tab button.

46 Configure the parameters:

- Override Summed CIR
- Summed CIR
- Override PIR
- PIR (Kb/s)
- Override CIR
- CIR (Kb/s)

47 Click on the OK button. A dialog box appears.

48 Click on the OK button. The scheduler entry override form closes and the L2 Access Interface form or L3 Access Interface form reappears.

49 Click on the OK button to close the L2 Access Interface form or L3 Access Interface form.

45 — Filter policies

45.1 Filter policies overview

Filter policies specify a forward, drop, or HTTP redirect action for packets based on information specified as the match criteria. You can create up to 2000 IP and 2000 MAC filter policies per managed NE. You can create up to 131 071 entries in a filter policy.

Filter entry matching criteria are either general or specific, but all conditions must be met for the packet to be considered a match and the specified entry action performed. The process stops when the first complete match is found and the action defined in the entry is executed.

When an interface or circuit is not configured with a filter policy, all traffic is allowed. By default, there are no filters associated with services or interfaces.

The 5620 SAM supports the creation and management of the following filter policies:

- ACL IP filter policies—applied to network and access IP interfaces, and service tunnels
- ACL IPv6 filter policies—applied to access interfaces and service tunnels
- ACL MAC filter policies—applied to access interfaces and service tunnels
- ACL IGMP filter policies—applied to 7250 SAS and Telco interfaces

Note — The 7705 SAR does not support IPv6 and MAC ACL filters.

The 7705 SAR has the following configuration limits for ACL IP filter entries:

- For non-extended range filter entries, the match criteria cannot be defined to match more than 256 packets.
- For extended range filter entries, there is no limit on the number of packet matches for the defined criteria; however, the total number of unique match criteria in use across all extended range filter entries within the same ACL IP filter cannot exceed eight.

SAP and service tunnel forwarding

ACL IP and ACL MAC filters contain options for delivering packets to specific destination SAPs and service tunnels based on the match criteria. Because the forwarding action is specified separately from device configuration, the packet destination name must be entered directly in text form (for example, 1/1/2:500) and validated by the 5620 SAM. Consider the following before you create a SAP or service tunnel forwarding filter:

- Although you can configure them on other service types, you should only create these filters on a VPLS. On other service types, packets are dropped.
- You can apply these filters on an ingress, but not an egress, SAP or service tunnel.

- The destination SAP or service tunnel must be on the same service as the device on which the filter is applied.
- The encapsulation type of the destination SAP and the associated port must be the same. Supported encapsulations are Ethernet Null, Dot1 Q, Q in Q, BCP, bridged Ethernet, FR, and ATM.

Web portal redirect

ACL IP and ACL MAC filters contain options for redirecting hosts to a URL address. The 7710 SR, 7750 SR-7, and 7750 SR-12 open a new connection to the specified web portal. The host can use the web portal to create or modify a service profile. The web portal updates the ACL policy directly, or through another system such as the 5750 SSC, to remove the redirection policy.

Note — The 7750 SR-1 does not support web portal redirect.

45.2 Filter policies procedures

The following procedures describe how to configure filter policies.

Procedure 45-1 To configure an ACL IP filter policy

1 Choose Policies→Filter→ACL IP Filter from the 5620 SAM main menu. The Manage ACL IP Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button.

The ACL IP Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Auto-Assign ID
- Displayed Name
- Description
- Default Action

4 Click on the Insertion Blocks tab button.

5 Configure the parameters:

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- High WaterMark (%)
- Low WaterMark (%)

6 Perform the following steps to configure a filter entry.

i Click on the Filter Entries tab button.

ii Click on the Add button. The Entry, ACL IP Filter (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description
- Log ID
- Administrative State

iv To assign a time range to the filter entry, click on the Select button in the Time Range panel. The Select Time Range - Ipv6FilterEntry list form opens. Otherwise, go to step 6 vi.

v Select a time range entry and click on the OK button. The Select Time Range - Ipv6FilterEntry list form closes and the Entry, ACL IPv6 Filter (Create) form refreshes with the time range information.

Note — ACL filters that include ACL filter entries to which you have assigned a time range cannot be assigned to a time of day suite policy.

Time ranges with which you have associated a ACL filter within a time of day suite policy cannot be assigned to ACL filter entries of that ACL filter.

vi Click on the Filter Properties tab button.

vii Configure the Action parameter:

If you specify Forward, the Next Hop Routing tab appears. Perform the following:

- Click on the Next Hop Routing tab button.
- Configure the parameters:
  - Forward NH
  - Is Indirect
  - Forward NH Interface
  - Remark DSCP
  - Remark DSCP Mask
  - Remark Dot1p

If you specify forward (SAP), the Forwarding Destination tab appears. Perform the following:

- Click on the Forwarding Destination tab button.
- Configure the parameters:
  - Port Name
  - Outer Encap Value
  - Inner Encap Value

If you specify forward (SDP), the Forwarding Destination tab is configurable. Perform the following:

- Click on the Forwarding Destination tab button.
- Configure the parameters:
  - Path ID
  - VC ID

If you specify HTTP redirect, the Web Redirect tab appears. Perform the following:

- Click on the Web Redirect tab button.
- Configure the Redirect URL parameter.

viii Configure the parameters:

- Protocol
- DSCP
- Source IP
- Destination IP
- Src Mask
- Dst Mask
- Fragment
- IP Option
- IP Opt Mask
- Option Present
- Multiple Option
- Source Port
- Dest Port
- ICMP Code
- ICMP Type
- TCP Syn
- TCP Ack

The Source Port and Dest Port parameters are configurable only when the Protocol parameter value is TCP, UDP, or UDPTCP (*).

The TCP Syn and TCP Ack parameters are configurable when the Protocol parameter value is TCP.

The ICMP Code and ICMP Type parameters are configurable when the Protocol parameter value is ICMP.

ix Click on the Cflowd tab button.

x Configure the parameters:

- Cflowd Sample
- Cflowd If Sample

xi Click on the OK button. The Entry, ACL IP Filter (Create) form closes and a dialog box appears.

xii Click on the OK button. The ACL IP Filter (Create) form reappears with the newly created filter entry displayed.

7 To create an additional filter entry, repeat step 6.

8 To define the order in which the policy tries to match filter entries with packets, perform the following steps for each filter entry.

i Select a filter entry in the list.

ii Click on the Renumber ID button. The Renumber Entry ID form opens.

iii Configure the New Entry ID parameter.

iv Click on the OK button. The Renumber Entry ID form closes, and the Entry ID column displays the new identifier assigned to the entry.

9 Click on the OK button to save the policy. The ACL IP Filter form closes and the Manage ACL IP Filter Policies form reappears.

10 Click on the Search button to display the newly created policy or policies.

11 Select the newly created policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

12 Select the distributed policy in the list and click on the Properties button. The ACL IP Filter Global Policy (Edit) form opens.

13 Click on the Local Definitions tab button.

14 Select a local definition from the list and click on the Properties button. The ACL IP Filter Local Policy (Edit) form opens.

15 Click on the Insertion Blocks tab button.

16 Configure the parameters:

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- High WaterMark (%)
- Low WaterMark (%)

Note — The Group Entries Inserted panel displays the number of entries insterted on this filter range.

17 Configure the Application and Location parameters in the Group Insertion Sorting panel.

18 Click on the Sort Group Instertions button. A dialog box appears.

19 Click on the OK button.

20 Perform the following steps to view filter entry data.

i Click on the Filter Entries tab button.

ii Click on the Credit Control Entries tab button or the RADIUS Entries tab button.

iii Click on the Search button.

iv Select an entry from the list and click on the Properties button. A form opens.

v Close the form after viewing the filter entry data.

21 Close the ACL IP Filter Entry Local Policy (Edit) form.

22 Close the ACL IP Filter Entry Global Policy (Edit) form.

23 Close the Manage ACL IP Filter Policies form.

Procedure 45-2 To configure an ACL IPv6 filter policy

Note — The 7705 SAR does not support ACL IPv6 filters.

1 Choose Policies→Filter→ACL IPv6 Filter from the 5620 SAM main menu. The Manage ACL IPv6 Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button.

The ACL IPv6 Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Auto-Assign ID
- Displayed Name
- Description
- Default Action

4 Click on the Insertion Blocks tab button.

5 Configure the parameters:

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- High WaterMark (%)
- Low WaterMark (%)

6 Perform the following steps to configure a filter entry.

i Click on the Filter Entries tab button.

ii Click on the Add button. The Entry, ACL IPv6 Filter (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description
- Log ID
- Administrative State

iv To assign a time range to the ACL IPv6 filter entry, click on the Select button in the Time Range panel. The Select Time Range - Ipv6FilterEntry list form opens. Otherwise, go to step 6 vi.

v Select a time range entry and click on the OK button. The Select Time Range - Ipv6FilterEntry list form closes and the Entry, ACL IPv6 Filter (Create) form refreshes with the time range information.

Note — ACL filters that include ACL filter entries to which you have assigned a time range cannot be assigned to a time of day suite policy.

Time ranges with which you have associated a ACL filter within a time of day suite policy cannot be assigned to ACL filter entries of that ACL filter.

vi Click on the Filter Properties tab button.

vii Configure the parameters:

- Action
- Protocol
- DSCP
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- Source Port
- Dest Port
- ICMP Code
- ICMP Type
- TCP Syn
- TCP Ack

The Source Port and Dest Port parameters are configurable when the Protocol parameter value is TCP or UDP.

The TCP Syn and TCP Ack parameters are configurable when the Protocol parameter value is TCP.

The ICMP Code and ICMP Type parameters are configurable when the Protocol parameter value is IPv6_ICMP.

viii Click on the OK button. The Entry, ACL IPv6 Filter (Create) form closes and a dialog box appears.

ix Click on the OK button. The ACL IPv6 Filter (Create) form displays the new filter entry.

7 To create an additional filter entry, repeat steps 6.

8 To define the order in which the policy tries to match filter entries with packets, perform the following steps for each filter entry.

i Select a filter entry in the list.

ii Click on the Renumber ID button. The Renumber Entry ID form opens.

iii Configure the New Entry ID parameter.

iv Click on the OK button. The Renumber Entry ID form closes, and the Entry ID column displays the new identifier assigned to the entry.

9 Click on the OK button. The ACL IPv6 Filter (Create) form closes, and the Manage ACL IPv6 Filter Policies form reappears.

10 Click on the Search button to display the newly created policy.

11 Select the policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

12 Select the distributed policy in the list and click on the Properties button. The ACL IPv6 Filter Global Policy (Edit) form opens.

13 Click on the Local Definitions tab button.

14 Select a local definition from the list and click on the Properties button. The ACL IPv6 Filter Local Policy (Edit) form opens.

15 Click on the Insertion Blocks tab button.

16 Configure the parameters:

- Credit Control Start Entry
- Credit Control Count
- RADIUS Start Entry
- RADIUS Count
- High WaterMark (%)
- Low WaterMark (%)

Note — The Group Entries Inserted panel displays the number of entries insterted on this filter range.

17 Configure the Application and Location parameters in the Group Insertion Sorting panel.

18 Click on the Sort Group Instertions button. A dialog box appears.

19 Click on the OK button.

20 Perform the following steps to view filter entry data.

i Click on the Filter Entries tab button.

ii Click on the Credit Control Entries tab button or the RADIUS Entries tab button.

iii Click on the Search button.

iv Select an entry from the list and click on the Properties button. A form opens.

v Close the form after viewing the filter entry data.

21 Close the ACL IPv6 Filter Entry Local Policy (Edit) form.

22 Close the ACL IPv6 Filter Entry Global Policy (Edit) form.

23 Close the Manage ACL IPv6 Filter Policies form.

Procedure 45-3 To configure an ACL MAC filter policy

Note — ACL MAC filters are not supported for the 7705 SAR.

1 Choose Policies→Filter→ACL MAC Filter from the 5620 SAM main menu. The Manage ACL MAC Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The ACL MAC Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Auto-Assign ID
- Displayed Name
- Description
- Default Action
- MAC Filter Type

The Default Action parameter specifies the action to be applied to packets when no action is specified in the MAC filter entries or when the packets do not match the specified criteria.

4 Configure the filter entries. Perform the following:

i Click on the Filter Entries tab button.

ii Click on the Add button. The Entry, ACL MAC Filter (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Auto-Assign ID
- Entry ID
- Displayed Name
- Description
- Log ID
- Administrative State

iv Assign a time range to the ACL MAC filter entry by clicking on the Select button beside the Name parameter. The Select Time Range - MacFilterEntry list form opens.

v Select a time range entry and click on the OK button. The Select Time Range - MacFilterEntry list form closes and the Entry, ACL MAC Filter (Create) form refreshes with the time range information.

Note — ACL filters that include ACL filter entries to which you have assigned a time range cannot be assigned to a time of day suite policy.

Time ranges with which you have associated a ACL filter within a time of day suite policy cannot be assigned to ACL filter entries of that ACL filter.

vi Click on the Filter Properties tab button.

vii Configure the Action parameter:

If you specify forward (SAP), the Forwarding Destination tab is displayed. Perform the following:

- Click on the Forwarding Destination tab button.
- Configure the parameters:
  - Port Name
  - Outer Encap Value
  - Inner Encap Value

If you specify forward (SDP), the Forwarding Destination tab is displayed. Perform the following:

- Click on the Forwarding Destination tab button.
- Configure the parameters:
  - Path ID
  - VC ID

If you specify HTTP redirect, the Web Redirect tab is displayed. Perform the following:

- Click on the Web Redirect tab button.
- Configure the Redirect URL parameter.

viii Click on the Filter Properties tab button.

ix Configure the parameters:

- Frame Type
- Source MAC
- Src Mask
- Destination MAC
- Dst Mask
- Dot1p
- Dot1p Mask
- Low ISID
- High ISID
- DSAP
- DSAP Mask
- SSAP
- SSAP Mask
- SNAP OUI
- SNAP PID
- Ether Type

The Source MAC, Src Mask, Destination MAC, Dst Mask, Dot1p, Dot1p Mask, Low ISID and High ISID parameter pairs are configurable when the check box for each pair is selected.

The DSAP, DSAP Mask, SSAP, and SSAP Mask parameters are configurable when the Frame Type parameter value is set to e802dot2LLC and the MAC Filter Type parameter is set to Normal.

The SNAP OUI and SNAP PID parameters are configurable when the Frame Type parameter value is e802dot2SNAP and the MAC Filter Type parameter is set to Normal.

The Ether Type parameter is configurable only when the Frame Type parameter value is set to Ethernet II and the MAC Filter Type parameter is set to Normal.

The Low ISID and High ISID parameters are only configurable when the MAC Filter Type parameter is set to ISID.

x Click on the OK button. The Entry, ACL MAC Filter (Create) form closes and a dialog box appears.

xi Click on the OK button. The ACL MAC Filter (Create) form reappears with the newly created filter entry displayed.

5 By default, all IDs for filter entries are set to 0. Perform one of the following steps:

a Continue configuring the filter. Go to step 7.

b Reorder new or existing filter entries, using the New Entry ID parameter.

i Click on the Refresh button to find an existing filter entry. The list of filter entries is displayed.

ii Select a filter entry in the list.

iii Click on the Renumber ID button. The renumber entry ID form opens and displays the current filter ID.

iv Specify the New Entry ID parameter. The range is 1 to 65535.

v Click on the OK button. The renumber entry ID form closes and the list of filter entries is refreshed, based on the new ID number assigned to the filter.

6 To add an additional filter entry, repeat steps 4 and 5.

7 Click on the OK button to save the policy. The ACL MAC Filter (Create) form closes and the Manage ACL MAC Filter Policies form reappears.

8 Click on the Search button to display the newly created policy or policies.

9 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

10 Close the Manage ACL MAC Filter Policies form.

Procedure 45-4 To configure a 7250 SAS and Telco ACL standard IP filter policy

1 Choose Policies→Filter→7250 SAS and Telco ACL Standard IP Filter from the 5620 SAM main menu. The Manage 7250 SAS and Telco ACL Standard IP Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The 7250 SAS and Telco ACL Standard IP Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Displayed Name
- Description

4 Click on the Filter Entries tab button.

5 Click on the Add button. The 7250 SAS and Telco ACL Standard IP Filter entry form opens with the General tab displayed.

6 Configure the parameters:

- Displayed Name
- Description

7 Click on the Filter Properties tab button.

8 Configure the parameters:

- Action
- Source IP
- Src Mask
- VLAN Priority Tag

The VLAN Priority Tag parameter is configurable when its check box is selected. The parameter is configurable by default.

9 To add more filter entries, repeat steps 5 to 8.

10 Click on the OK button. The 7250 SAS and Telco ACL Standard IP Filter entry form closes and the Manage 7250 SAS and Telco ACL Standard IP Filter Policies form reappears.

11 Click on the Search button to display the newly created policy or policies.

12 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

13 Close the Manage 7250 SAS and Telco ACL Standard IP Filter Policies form.

Procedure 45-5 To configure a 7250 SAS and Telco ACL extended IP filter policy

1 Choose Policies→Filter→7250 SAS and Telco ACL Extended IP Filter from the 5620 SAM main menu. The Manage 7250 SAS and Telco ACL Extended IP Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The 7250 SAS and Telco ACL Extended IP Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Displayed Name
- Description

4 Click on the Filter Entries tab button.

5 Click on the Add button. The 7250 SAS and Telco ACL Extended IP Filter entry form opens.

6 Configure the parameters:

- Displayed Name
- Description

7 Click on the Filter Properties tab button.

8 Configure the parameters:

- Action
- Source IP
- Destination IP
- Source Port
- Dest Port
- TCP Ack
- Protocol
- Src Mask
- Dest Mask
- TOS
- Precedence
- VLAN Priority Tag
- ICMP Code
- ICMP Type

The Source Port and Dest Port parameters are configurable when the Protocol parameter value is TCP or UDP.

The TCP Ack parameter is configurable when the Protocol parameter value is TCP.

The ICMP Code and ICMP Type parameters are configurable when the Protocol parameter value is ICMP.

9 To add more filter entries, repeat steps 5 to 8.

10 Click on the OK button. The 7250 SAS and Telco ACL Extended IP Filter entry form closes and the Manage 7250 SAS and Telco ACL Extended IP Filter form reappears.

11 Click on the Search button to display the newly created policy or policies.

12 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

13 Close the Manage 7250 SAS and Telco ACL Extended IP Filter Policies form.

Procedure 45-6 To configure a 7250 SAS and Telco ACL IGMP filter policy

1 Choose Policies→Filter→7250 SAS and Telco ACL IGMP Filter from the 5620 SAM main menu. The Manage 7250 SAS and Telco ACL IGMP Filter Policies form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The 7250 SAS and Telco ACL IGMP Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Filter ID
- Displayed Name
- Description
- Name

4 Click on the Filter Entries tab button.

5 Click on the Add button. The Entry, 7250 SAS and Telco ACL IGMP Filter (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Displayed Name
- Description

7 Click on the Filter Properties tab button.

8 Configure the parameters:

- Action
- Source IP
- Src Mask
- Destination IP
- Dest Mask
- Loggable
- IGMP Option

9 Click on the OK button. A dialog box appears.

10 Click on the OK button. The 7250 SAS and Telco ACL IGMP Filter (Create) form reappears.

11 To add more filter entries, repeat steps 5 to 10.

12 Click on the OK button to close the 7250 SAS and Telco ACL IGMP Filter (Create) form and save the policy.

13 Click on the Distribute button to manually distribute the policy locally to 7250 SAS or Telco devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

14 Click on the Selected radio button to choose from the listed devices.

15 Choose one or more rows from the Available Nodes list.

16 Click on the right arrow button. The selected devices move to the list on the right side of the form.

17 Click on the Distribute button. The policy is distributed to the device or devices.

18 Close the Distribute form. The 7250 SAS and Telco ACL IGMP Filter Policy form reappears.

19 Close the 7250 SAS and Telco ACL IGMP Filter Policy form. The Manage 7250 SAS and Telco ACL IGMP Filter Policies form reappears.

20 Close the Manage 7250 SAS and Telco ACL IGMP Filter Policies form.

Procedure 45-7 To configure a 7250 SAS and Telco ACL MAC filter policy

1 Choose Policies→Filter→7250 SAS and Telco ACL MAC Filter from the 5620 SAM main menu. The Manage 7250 SAS and Telco ACL MAC Filter Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.
- **b** Click on the Create button. The 7250 SAS and Telco ACL MAC Filter (Create) form opens.

3 Configure the parameters:

- Filter ID
- Displayed Name
- Description

4 Click on the Filter Entries tab button.

5 Click on the Add button. The 7250 SAS and Telco ACL MAC Filter entry form opens with the General tab displayed.

6 Configure the parameters:

- Displayed Name
- Description

7 Click on the Filter Properties tab button.

8 Configure the parameters:

- Action
- Source MAC
- Destination MAC
- Pattern
- Src Mask
- Dst Mask
- Pattern Mask

The Pattern and Pattern Mask parameters are configurable when the check box is selected.

9 Click on the OK button.

10 To add more filter entries, repeat steps 5 to 11.

11 Click on the OK button. The 7250 SAS and Telco ACL MAC Filter (Create) form closes and the Manage 7250 SAS and Telco ACL MAC Filter Policies form reappears.

12 Click on the Search button to display the newly created policy or policies.

13 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

14 Close the Manage 7250 SAS and Telco ACL MAC Filter Policies form.

46 — Multicast policies

46.1 Multicast policies overview

You can use the 5620 SAM to create policies that regulate the flow of multicast traffic for more efficient multicast stream management, bandwidth management, and traffic forwarding.

Egress multicast groups

In VPLS standard multicasting, copies of the original packets are looped back to the SAP for transmission to each destination: an activity that consumes resources and makes the handling of congestion issues more difficult.

A more efficient method of forwarding multicast packets is to group destination SAPs in a set or "chain" that receives a single multicast packet from the egress forwarding plane with only a single pass. Adding SAPs to an EMG eliminates loopbacks by forwarding a multicast packet once to a group of shared definitions. As a result, an EMG makes multicasting more efficient and more scalable.

Creating an EMG in the 5620 SAM is similar to creating a policy, because it is first created globally and then distributed to NEs. The EMG is applied to an L2 access interface that has been created on an Ethernet port with null or Dot1 Q encapsulation. SAP membership in an EMG has the following requirements:

- The SAP must belong to an SHG.
- The L2 access interface egress ACL filter must match that of the EMG.
- The access port and the EMG must have the same encapsulation type.

When a SAP becomes a member of an EMG, the common parameters that it shares with other EMG members cannot be changed. On the other hand, a modification to an EMG common requirement changes that parameter in all SAPs in the chain. The same common required traits apply to egress filters: individual SAP filters cannot be changed, and any change to the EMG egress filter parameters affects the egress filters in all member SAPs. In addition, if an egress filter is not defined in the EMG common parameter requirements, a new member SAP cannot have an egress filter.

The following restrictions also apply to an EMG:

- only IPv4 egress filters can be applied to an EMG
- up to 30 EMGs can be created on a router
- an EMG can be deleted only if it has no SAP members
- the number of members in an EMG (the chain limit) is restricted to 30, with an optimal length of 10 to 16

Multicast package policies

Multicast package policies for Telco devices group together BTV multicast streams which can be applied to Telco ring groups for distribution to end users.

Multicast package policies are also used to assign a common set of multicast groups to all 7450 ESSs and 7750 SRs in an MVR VPLS. Multicast package policies ensure that the multicast groups on the devices of one or more MVR VPLS instances are consistent. See chapter 27 for information about configuring multicast groups on individual devices using a multicast routing policy.

When a multicast package policy is distributed to a 7450 ESS or 7750 SR, a multicast routing policy is configured with the appropriate multicast prefix list, which is based on the multicast groups in the multicast package policy. Multicast package policies are only used to distribute the policies to one of the two NEs. Policy discovery and synchronization are not supported.

A multicast package policy has zero or more multicast groups associated with it. The multicast groups are distributed to the 7450 ESS or 7750 SR as part of the policy. Only root catalog multicast packages can be distributed to the 7450 ESSs or 7750 SRs.

Distributing multicast package policies

When you distribute a multicast package policy to a 7450 ESS or 7750 SR, the 5620 SAM maps one multicast package policy to one routing policy statement. Each multicast policy group entry is mapped to one routing policy prefix list member.

For example, the ID of a multicast package policy is 2. When the policy is distributed to a 7450 ESS or 7750 SR, the 5620 SAM automatically creates a routing policy statement for the device. The name created for the routing policy statement is SAM_MPP_2, where 2 is the multicast package policy ID.

When the policy is distributed to the 7450 ESS or 7750 SR, the ID of the routing policy statement entry is always 1. A name is generated by the 5620 SAM to identify the prefix list in the routing policy statement entry. The name is SAM_MPG_2_1, where 2 is the multicast package policy ID and 1 is the routing policy statement entry ID. The prefix list name is referenced in the routing policy statement entry as the multicast group prefix list name.

In the same example, the multicast address for the multicast group of a multicast package policy is 224.0.0.0. When the multicast package policy is distributed to a 7450 ESS or 7750 SR, the 5620 SAM automatically creates a routing policy prefix list member for the device. The prefix list member address is 224.0.0.0.

Since the multicast package policy is not resynchronized, you must avoid duplicate names for routing policies.

For the 7450 ESS and 7750 SR, if a multicast group does not have a policy group entry, the multicast group is not distributed to the device as a prefix member.

If a multicast package policy is used by any MVR VPLS, it cannot be removed from the 5620 SAM.

Multicast CAC policies

Multicast CAC policies control the bandwidth consumed by BTV distribution services. Bandwidth control helps manage network congestion and maintain QoS standards. The multicast CAC function is supported on any IGMP and PIM interface, and in the case of BTV distribution, on VPLS SAPs and SDPs where IGMP snooping is enabled.

A multicast CAC policy manages the bandwidth consumed by BTV services on both the access node link and specific links in the aggregation network. Routers in the path are configured to maintain certain limits on broadcast bandwidth and can limit the number of channels simultaneously sent on both the second mile link and the network link.

Multicast CAC policies are supported for VPLS on the 7710 SR, 7750 SR, and 7450 ESS.

Ingress Multicast Bandwidth policy

Ingress Multicast Bandwidth policies are used to manage the ingress multicast path bandwidth of the multicast forwarding paths into the switching fabric. When Multicast Path Management is disabled (the default), two paths are available:

- a high-priority path, on which packets from queues classified as “expedited” are forwarded
- a low-priority path on which packets from queues classified as “non-expedited” are forwarded

When Multicast Path Management is enabled, an Ingress Multicast Bandwidth policy can be used to manage the flow of multicast traffic through an MDA (IOM or IOM 2) or the forwarding plane of an 2 x XP MDA IOM 3 or IMM.

The maximum number of bandwidth policies per NE is 32, including the default policy.

MDAs can be configured to use previously defined Ingress Multicast Bandwidth policies. However, any path limits specified in the selected policy can be overridden for each MDA, if required.

Ingress Multicast Info policy

Ingress Multicast Info policies are used to define how each multicast channel is handled by NEs. The policy is assigned to a VPLS/VPRN service site or default routing instance, but the policy is actually used by the Ingress Multicast Bandwidth Manager, the ECMP Path Manager, and the Egress Multicast CAC Manager to determine the path through the switch fabric and to make decisions on joins to multicast streams.

The maximum number of Info policies per NE is limited to 32, including the default policy.

MDAs can be configured to use previously-defined Ingress Multicast Bandwidth policies. However, any path limits specified in the selected policy can be overridden for each MDA, if required.

Ingress multicast forwarding on L2-snooped and L3-routed IP multicast traffic can be explicitly configured by applying an Ingress Multicast Path Management Info policy to a VPLS site (all types of VPLS are supported), a VPRN site, or the default routing instance.

An Info policy consists of one or multiple named Bundles, which in turn, contain Channel ranges with possible overrides for individual channels.

Bundles

A Bundle groups a set of explicit multicast channels (or channel ranges) into a common bandwidth context for CAC functions (such as join decisions) using common preferences. The channels in the bundle are managed as a defined percentage of the available bandwidth.

Bundles also simplify provisioning, since the default characteristics of the bundle channels are specified on the bundle level. These characteristics can be overridden at the Channel range level, or explicitly per channel.

Each Info policy has a default bundle named “default”. It cannot be edited or removed. Any multicast channel that fails to match a channel range within an explicit operator-defined bundle is associated with this default bundle.

Note — The maximum number of Bundles per Info policies is limited to 32. This limit includes the default bundle, leaving 31 operator-defined bundles per Info policy.

Channels and channel ranges

Channel ranges are used to define a set of multicast channels contained in a bundle and to override the default channel settings in the containing bundle.

A channel range is defined by a start destination multicast IP address and an end destination multicast IP address (both IP v4 and IPv6 are supported, but the start and end addresses must be of the same type). A channel in this context is a channel range where the start address and end address are identical.

Note — After you create a channel range, it is not possible to modify the start address or end address.

A channel range can contain multiple channel overrides. A channel override is used to specify an explicit setting for a channel within the range. The channel override is identified by a destination multicast IP address which falls between the start and end IP addresses of the channel range.

Note — The 7450 ESS does not support channel ranges and channel overrides having IPv6 addresses. Therefore, the 5620 SAM does not allow the creation of such channel ranges and channel overrides on local Ingress Multicast Info policies. In addition, the 5620 SAM removes any such channel ranges and channel overrides when synchronizing local Info policies with their respective global policies.

Dual stream selection

Dual stream selection support allows a single multicast stream to be duplicated into two different transmission paths. The two paths may have different transmission characteristics, such as latency and jitter. Rather than select one stream for retransmission to the client, the duplicate stream protection feature evaluates each stream packet-by-packet, selecting the packet that first arrives (and is valid) for retransmission.

Dual stream selection is supported on the 7710 SR and the 7750 SR.

Video quality monitoring

VQM to provides the functionality to analyze the quality of a video stream just prior to reaching the STB of client in a IPTV network. Statistics reports and alarms can be generated for VQM, providing operators with a view of multicast video quality at the last mile of distribution.

VQM is supported on the 7710 SR and the 7750 SR.

46.2 Multicast policies procedures

This section contains procedures relating to the configuration and maintenance of multicast policies.

Procedure 46-1 To create an egress multicast group policy

1 Choose Policies→Multicast→Egress Multicast Group. The Manage Egress Multicast Group Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Egress Multicast Group (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Destination Chain Limit

4 Click on the SAP Common Requirements tab button.

5 Configure the parameters:

- Encapsulation Type
- Dot1 Q Ethertype
- QinQ Ethertype
- QinQ Fixed Tag Value

6 Click on the Select button in the Egress Filter panel to choose an egress policy. The Select Egress Filter search form opens.

7 Select an egress policy in the list and click on the OK button. The Select Egress Filter form closes and the egress policy information appears on the Egress Multicast Group (Create) form.

Note — The egress policy that you choose for this EMG must be the same as the egress policy specified for a member SAP.

8 Click on the Apply button to save the policy. The Egress Multicast Group (Create) form reappears with the General tab displayed.

9 Click on the Distribute button to manually distribute the policy to local devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note 1 — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

Note 2 — To associate a SAP on the device with an EMG, the access port encapsulation type on the device must be the same as the encapsulation type that you specified in step 5.

10 Close the Egress Multicast Group form. The Manage Egress Multicast Group Policies form reappears.

11 Close the Manage Egress Multicast Group Policies form.

Procedure 46-2 To configure a multicast CAC policy

1 Choose Policies→Multicast→Multicast CAC. The Manage Multicast CAC Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Multicast CAC (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Default Action

4 Click on the Apply button. The Multicast CAC (Edit) form opens with the General tab displayed.

5 Click on the Bundles tab to associate a multicast bundle with the multicast CAC policy.

6 Click on the Add button. The Multicast CAC Bundle (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Name
- Description
- Max Bandwidth (kbps)
- Administrative State

8 Click on the Channels tab.

9 Click on the Add button. The Multicast CAC Channel (Create) form opens.

10 Configure the parameters:

- Start Address
- End Address
- Bandwidth (kbps)
- Class
- Type

11 Click on the OK button. The Multicast CAC Channel (Create) form closes and a dialog box appears.

12 Click on the OK button. The Multicast CAC Bundle (Create) form lists the newly configured channel.

13 To add additional channels to the bundle, repeat steps 9 to 12.

14 Click on the OK button. A dialog box appears.

15 Click on the OK button. The Multicast CAC Bundle (Create) form closes and the Multicast CAC (Edit) form reappears with the Bundles tab displayed.

16 Click on the OK button. A dialog box appears.

17 Click on the OK button. The Multicast CAC (Edit) form closes and the Manage Multicast CAC Policies form reappears.

18 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

19 Select a policy and click on the Distribute button to manually distribute the policy to local devices. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

20 Close the Manage Multicast CAC Policies form.

Procedure 46-3 To configure an Ingress Multicast Bandwidth policy

1 Choose Policies→Multicast→Ingress Multicast Path Management. The Manage Ingress Path Management Policies form opens.

2 Select the Multicast Bandwidth Policy (multicast) from the object drop-down list.

3 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button and select Create Multicast Bandwidth Policy from the contextual menu. The Multicast Bandwidth Policy (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description
- Falling Percent Reset (%)
- Admin BW Use Threshold (kbps)
- Percentage of Total pool (%)
- Reserved (CBS) (%)
- Displayed Name

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the T1 Paths tab button. A table displays the policy definitions for the primary, secondary, and ancillary paths. Each path definition contains configurable parameters.

6 Choose one of the paths and click on the Properties button. The Bandwidth Policy Path (Create) form opens.

7 Configure the parameters:

- Path limit (mbps)
- Committed Buffer Space (%)
- Maximum Buffer Space (%)
- High Priority Traffic (%)

8 Click on the Apply button. A dialog box appears.

9 Click on the OK button.

10 Repeat steps 6 to 9 for the remaining paths, if required.

11 Click on the T2 Paths tab button. A table displays the policy definitions for the primary and secondary paths. Each path definition contains configurable parameters.

12 Choose one of the paths and click on the Properties button. The Bandwidth Policy Path (Create) form opens.

13 Configure the parameters:

- Number of Secondary T2 Paths
- Committed Buffer Space (%)
- Maximum Buffer Space (%)
- High Priority Traffic (%)

14 Click on the Apply button. A dialog box appears.

15 Click on the OK button.

16 Repeat steps 12 to 15 for the remaining path, if required.

17 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

18 Close the Multicast Bandwidth Policy form. The Manage Ingress Path Management Policies form reappears.

19 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 46-4 To configure an Ingress Multicast Information policy

1 Choose Policies→Multicast→Ingress Multicast Path Management. The Manage Ingress Path Management Policies form opens.

2 Choose Multicast Info Policy (Multicast) from the object drop-down list.

3 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button and select Create Multicast Info Policy from the contextual menu. The Multicast Info Policy (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Bundles tab button. All defined bundles are displayed, including the default.

6 Click the Add button. The Info Policy Bundle, Multicast Info Policy (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Name
- Description
- Congestion Priority Threshold
- ECMP Optimization Threshold
- Administrative BW (kbps)
- Preference Level
- BW Decision
- Falling Delay (seconds)
- Black Hole Rate (kbps)
- Explicit Path

8 Click on the Video Defaults tab button.

9 Configure the parameters:

- Video Group Id
- Channel Type
- Re-order Audio Interval (msec)
- FCC Server
- Min Duration (msec)
- Buffer Size (msec)
- RT Server
- Local Server

10 Configure the stream selection parameters, if the Stream Selection parameter is enabled for the video group.

Note — Stream selection parameters are only available if you are performing the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the policy are retained. See chapter 43 for information on policy distribution modes.

i Enter a unicast IPv4 address for the Source Address parameter.

ii Click on the Select button next to the Primary Interface parameter. The Select - Multicast Path Management Bundle form opens.

iii Select an access interface and click on the OK button.

iv Click on the Select button next to the Secondary Interface parameter. The Select - Multicast Path Management Bundle form opens.

Note — The Primary Interface and Secondary Interface must be different.

v Select an access interface and click on the OK button.

11 Configure VQM if the Analyzer parameter is enabled for the video group.

Note — If VQM is not enabled for the video group, then parameters configured in the VQM Config tab will have no effect.

i Enable the Analyzer parameter in the VQM panel. The form refreshes with the additional VQM Config tab button.

ii Configure the Description parameter.

iii Click on the VQM Config tab button.

iv Configure the parameters:

- Continuity Counter Error
- Unreferenced PID Error
- SCTE35 Error
- TEI Error
- TS Sync Loss Error

v In the PAT (Program Association Table) Repetition panel, configure the PAT Syntax Error parameter.

vi Enable the PAT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

vii In the PCR (Program Clock Reference) Repetition panel, enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- POA (msec)

viii In the PMT (Program Map Table) Repetition panel, configure the PMT Syntax Error parameter.

ix Enable the PMT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- POA (msec)

x In the PID panel, configure the parameters:

- Video PID Absent Interval (msec)
- Non Video PID Absent Intv (msec)

12 Click on the Tunnel Interfaces tab button.

13 Click on the Select button next to the P2MP LSP Name parameter. The Select - Multicast Path Management Bundle form opens.

14 Select a Multicast Path Management Bundle and click on the OK button.

15 The Select - Multicast Path Management Bundle form closes and the information is displayed.

16 Click on the Select button next to the P2MP ID for LDP parameter. The Select LDP Tunnel Interface - Multicast Path Management Bundle form opens.

17 Select an LDP Tunnel Interface and click on the OK button.

18 The Select LDP Tunnel Interface - Multicast Path Management Bundle form closes and the information is displayed.

19 Configure the Ingress LER parameter.

Note 1 — You can configure either the P2MP LSP Name parameter or the P2MP ID for LDP parameter.

Note 2 — The Ingress LER parameter is automatically configured when the P2MP ID for LDP parameter is configured.

20 Click on the Channels tab button.

21 Click the Add button. The Info Policy Channel Range, Info Policy Bundle (Create) form opens with the General tab displayed.

22 Configure the channel range parameters:

- Start Address
- End Address

Note — The 7450 ESS does not support channel ranges and channel overrides having IPv6 addresses. Therefore, the 5620 SAM does not allow the creation of such channel ranges and channel overrides on local Ingress Multicast Info policies. In addition, the 5620 SAM removes any such channel ranges and channel overrides when synchronizing local Info policies with their respective global policies.

23 Configure any required overrides of the following parameters in the Channel Defaults block:

- Administrative BW (kbps)
- Preference Level
- BW Decision
- Falling Delay (seconds)
- Black Hole Rate (kbsp)
- Explicit Path

24 Click on the Video tab button.

25 Configure the parameters:

- Video Group Id
- Channel Type
- Re-order Audio Interval (msec)
- FCC Server
- Min Duration (msec)
- Buffer Size (msec)
- RT Server
- Local Server

26 Configure the stream selection parameters, if the Stream Selection parameter is enabled for the video group.

Note — Stream selection parameters are only available if you are performing the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the policy are retained. See chapter 43 for information on policy distribution modes.

i Enter a unicast IPv4 address for the Source Address parameter.

ii Click on the Select button next to the Primary Interface parameter. The Select - Multicast Path Management Bundle form opens.

iii Select an access interface and click on the OK button.

iv Click on the Select button next to the Secondary Interface parameter. The Select - Multicast Path Management Bundle form opens.

Note — The Primary Interface and Secondary Interface must be different.

v Select an access interface and click on the OK button.

27 Configure VQM if the Analyzer parameter is enabled for the video group.

Note — If VQM is not enabled for the video group, then parameters configured in the VQM Config tab will have no effect.

i Enable the Analyzer parameter in the VQM panel. The form refreshes with the additional VQM Config tab button.

ii Configure the Description parameter.

iii Click on the VQM Config tab button.

iv Configure the parameters:

- Continuity Counter Error
- Unreferenced PID Error
- SCTE35 Error
- TEI Error
- TS Sync Loss Error

v In the PAT (Program Association Table) Repetition panel, configure the PAT Syntax Error parameter.

vi Enable the PAT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

vii In the PCR (Program Clock Reference) Repetition panel, enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- POA (msec)

viii In the PMT (Program Map Table) Repetition panel, configure the PMT Syntax Error parameter.

ix Enable the PMT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- POA (msec)

x In the PID panel, configure the parameters:

- Video PID Absent Interval (msec)
- Non Video PID Absent Intv (msec)

28 Click on the Tunnel Interfaces tab button.

29 Click on the Select button next to the P2MP LSP Name parameter. The Select - Multicast Path Management Channel Range form opens.

30 Select a Multicast Path Management Channel Range and click on the OK button.

31 The Select - Multicast Path Management Channel Range form closes and the information is displayed.

32 Click on the Select button next to the P2MP ID for LDP parameter. The Select LDP Tunnel Interface - Multicast Path Management Channel Range form opens.

33 Select an LDP Tunnel Interface and click on the OK button.

34 The Select LDP Tunnel Interface - Multicast Path Management Channel Range form closes and the information is displayed.

35 Configure the Ingress LER parameter.

Note 1 — You can configure either the P2MP LSP Name parameter or the P2MP ID for LDP parameter, but not both.

Note 2 — The Ingress LER parameter is automatically configured when the P2MP ID for LDP parameter is configured.

36 Click on the Channel Override tab button if you need to specify overrides for explicit channels within the Channel Range.

37 Click on the Add button. The Info Policy Channel Override (Create) form opens, with the General tab displayed.

38 Enter the Source Address of the channel for which you want to specify overrides.

39 Configure any required overrides of the following parameters for the channel in the Overrides block:

- Administrative BW (kbps)
- Preference Level
- BW Decision
- Falling Delay (seconds)
- Black Hole Rate (kbsp)
- Explicit Path

40 Click on the OK button. A dialog box appears. Click OK. The channel to which you applied overrides is displayed.

41 Click on the Video tab button.

42 Configure the parameters:

- Video Group Id
- Channel Type
- Re-order Audio Interval (msec)
- FCC Server
- Min Duration (msec)
- Buffer Size (msec)
- RT Server
- Local Server

43 Configure the stream selection parameters, if the Stream Selection parameter is enabled for the video group.

Note — Stream selection parameters are only available if you are performing the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the policy are retained. See chapter 43 for information on policy distribution modes.

i Enter a unicast IPv4 address for the Source Address parameter.

ii Click on the Select button next to the Primary Interface parameter. The Select - Multicast Path Management Bundle form opens.

iii Select an access interface and click on the OK button.

iv Click on the Select button next to the Secondary Interface parameter. The Select - Multicast Path Management Bundle form opens.

Note — The Primary Interface and Secondary Interface must be different.

v Select an access interface and click on the OK button.

44 Configure VQM if the Analyzer parameter is enabled for the video group.

Note — If VQM is not enabled for the video group, then parameters configured in the VQM Config tab will have no effect.

i Enable the Analyzer parameter in the VQM panel. The form refreshes with the additional VQM Config tab button.

ii Configure the Description parameter.

iii Click on the VQM Config tab button.

iv Configure the parameters:

- Continuity Counter Error
- Unreferenced PID Error
- SCTE35 Error
- TEI Error
- TS Sync Loss Error

v In the PAT (Program Association Table) Repetition panel, configure the PAT Syntax Error parameter.

vi Enable the PAT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- TOA (msec)

vii In the PCR (Program Clock Reference) Repetition panel, enable the PCR Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- POA (msec)

viii In the PMT (Program Map Table) Repetition panel, configure the PMT Syntax Error parameter.

ix Enable the PMT Repetition Error parameter, if required, and configure the newly displayed parameters:

- TNC (msec)
- QoS (msec)
- POA (msec)

x In the PID panel, configure the parameters:

- Video PID Absent Interval (msec)
- Non Video PID Absent Intv (msec)

45 Click on the Tunnel Interfaces tab button.

46 Click on the Select button next to the P2MP LSP Name parameter. The Select - Multicast Path Management Channel Range form opens.

47 Select a Multicast Path Management Channel Range and click on the OK button.

48 The Select - Multicast Path Management Channel Range form closes and the information is displayed.

49 Click on the Select button next to the P2MP ID for LDP parameter. The Select LDP Tunnel Interface - Multicast Path Management Channel Range form opens.

50 Select an LDP Tunnel Interface and click on the OK button.

51 The Select LDP Tunnel Interface - Multicast Path Management Channel Range form closes and the information is displayed.

52 Configure the Ingress LER parameter.

Note 1 — You can configure either the P2MP LSP Name parameter or the P2MP ID for LDP parameter, but not both.

Note 2 — The Ingress LER parameter is automatically configured when the P2MP ID for LDP parameter is configured.

53 Click on the Video Interfaces tab button if you need to configure a video interface.

Note — If you are configuring a video interface you must perform the configuration in the local policy definition. After the changes are applied to the local policy, the policy can be switched back to Sync With Global mode and the local changes made to the video interface are retained. See chapter 43 for information on policy distribution modes. See chapter 33 for more information about IPTV video features and configuration.

54 Click on the Add button. The Multicast Video Interface (Create) form opens with the General tab displayed.

55 Configure the Address parameter.

56 Click on the Channel Config tab button.

57 Select a channel in the list and click on the Properties button. The Multicast Video Interface Channel Config (Create) form opens.

58 Configure the parameters:

- RT Rate
- Local RT Server
- RT Payload Type
- FCC Server Mode
- FCC Burst
- FCC MC Handover Rate
- Max IGMP Latency
- Max Number of Sessions

59 Click on the OK button. The Multicast Video Interface Channel Config (Create) form closes and a dialog box appears.

60 Click on the OK button. The configured channels are displayed in the list.

61 Repeat steps 56 to 60 to configure additional channels, if required.

62 Click on the OK button. The Multicast Video Interface (Create) form closes and a dialog box appears.

63 Click on the OK button.

64 Click on the Apply button.

65 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

66 You can view information on VPLS sites (regular sites and I-Sites), VPRN sites, and Default Routing Instances affected by the Multicast Info Policy by clicking the appropriate tab. Run a search and view the properties for the desired item.

67 Close the Multicast Info Policy form. The Manage Ingress Path Management Policies form reappears.

68 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

Procedure 46-5 To view multicast CAC channel statistics

Perform this procedure to view multicast CAC channel statistics and identify the status of BTV channels on a managed NE. This procedure allows you to display useful information including which channels are blocked and their location, bandwidth availability, the number of times channel requests are dropped on an interface, and the cause of the action based on the multicast CAC policy.

1 Choose Tools→BTV Channel Monitor. The Select Site form opens.

2 Select a site in the list and click on the OK button. The BTV Channel Monitor form opens.

3 Perform one of the following:

- **a** Choose Multicast CAC Channel Statistics (multicast) from the object drop-down list to list network protocol statistics.
- **b** Choose Multicast CAC Channel Statistics on Services (multicast) from the object drop-down list to list service statistics.

4 Configure the filter criteria and click on the Search button. A list of multicast CAC channel statistics is displayed at the bottom of the form.

Note — To get the most recent channel information on a managed NE, perform a resynchronization by clicking on the Resync button before clicking on the Search button.

5 Close the BTV Channel Monitor form.

Procedure 46-6 To configure a multicast package policy

Use multicast package policies to:

- define a set of broadcast channels that are multicast across a ring group in a BTV VLAN
- assign a common set of multicast groups to all 7450 ESSs or 7750 SRs in an MVR VPLS to ensure accuracy and consistency

Consider the following when creating multicast package policies:

- one root multicast package policy should be created for a ring or multiple rings, which contains the multicast addresses of all BTV channels distributed in the ring
- specify this root multicast package policy for the BTV (MVR) VLAN
- create other multicast package policies from the root package using the Copy button on the configuration form
- use the child policies to differentiate the types of broadcast TV services offered, for example, basic service and premium service
- when you create 7250 SAS and Telco IGMP ACL filter policies, use these child policies to limit access for end users to specific types of services, for example, access to basic service, premium service, or both services

1 Choose Policies→Multicast→Multicast Package from the 5620 SAM main menu. The Multicast Package Policy Manager form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The Multicast Package Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Auto-Assign ID
- Name
- Description
- Is Root Catalogue
- IGMP Option
- Loggable

4 Click on the Multicast Groups tab button.

5 Click on the Add button. The Multicast Group (Create) form opens.

Note — Each multicast group that is specified must be preconfigured in the PIM configuration. See the PIM configuration procedures in chapter 28.

6 Configure the parameters:

- Multicast Address
- Name
- Description
- Channel
- Cost

7 Click on the Apply button to save the policy. The Multicast Package Policy (Create) form is refreshed with additional buttons.

8 Click on the Definitions tab, if applicable.

9 Click on the Distribute button to manually distribute the policy locally to devices in the ring. You can use the Distribute button when the Is Root Catalogue parameter is set to root. The Distribute form opens. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

When any new devices are added to the ring, the policy is automatically distributed to any new MVR VLAN service or to any new MVR VLAN service sites in the ring.

10 Click on the Selected radio button to choose from the listed devices.

11 Choose one or more rows from the Available Nodes list.

12 Click on the right arrow button. The selected devices move to the list on the right side of the form.

13 Click on the Distribute button. The policy is distributed to the device or devices.

14 Close the Distribute form. The Multicast Package Policy form reappears.

15 Close the Multicast Package Policy form.

Create other multicast package policies from the root policy using the Copy button, as required. These child policies of the root policy can be used to help differentiate the types of BTV services being created, for example, basic services and premium services.

47 — Time of day policies

47.1 Time of day policies overview

The 5620 SAM supports the creation of time of day policies that allow you to configure time-based QoS policies, ACL filters, and schedulers that are applied to aggregation schedulers and L2 and L3 access interfaces. For example, a time of day policy allows you to manage peer-to-peer traffic by limiting access during peak hours, such as evenings and weekends.

A time range policy consists of one or more schedules, which include a start and end day and time and a priority.

A time of day suite policy is a collection of ingress and egress policies, filter policies, and schedulers, to which time range policies have been assigned. You can apply time of day suite policies to aggregation schedulers and L2 and L3 access interfaces.

You can create a time of day suite policy by assigning time range policies to the following objects to apply time and day restrictions to their deployment and access:

- ACL MAC filters and filter entries
- ACL IP filters and filter entries
- ACL IPv6 filters and filter entries
- access ingress and egress QoS policies
- scheduler policies

The default time range policy is the NO-TIME-RANGE policy, which means that no time and day restrictions apply. There can be only one NO-TIME-RANGE entry in each type of time of day suite policy entry.

Time range policies are first created globally and then distributed to NEs. You can distribute time range policies to the 7750 SR, 7710 SR, 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, and 7450 ESS.

Time range assignment analysis tool

The time range assignment analysis tool allows you to view the time range policies that have been assigned over a specific time period to the following objects:

- L2 access interfaces
- L3 access interfaces
- aggregation schedulers
- time of day suite policies

You can use the time range assignment analysis tool to verify the configuration of multiple schedules and the adequacy of a time of day suite policy on a specific NE. For example, you can use this tool to verify that multiple time ranges that are assigned to IP filters in a time of day suite policy cover an entire month.

47.2 Time of day policies procedures

The following procedures describe how to configure and manage time of day policies.

Procedure 47-1 To configure a time range policy

1 Choose Policies→Time of Day→Time Range from the 5620 SAM main menu. The Manage Time Range form opens.

2 Perform one of the following:

a Specify a filter to search for an existing time range policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The Time Range (Create) form opens.

3 Configure the parameters:

- Name
- Description

4 Click on the Time Range Entries tab button.

5 Click on the Add button. The Time Range Entries (Create) form opens.

6 Configure the parameters:

- Start Time
- End Time
- Ongoing
- Frequency
- Start Run Day
- End Run Day

The Frequency parameter is configurable when the Ongoing parameter is enabled.

The Start Run Day and End Run Day parameters are configurable when the Frequency parameter is set to Weekly.

7 Click on the OK button. The Time Range Entries (Create) closes. The Manage Time Range form opens.

8 Click on the Search button to display the newly created policy or policies.

9 Select a policy and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

10 Close the Manage Time Range form.

Procedure 47-2 To configure a time of day suite

Consider the following when you create a time of day suite policy:

- when there are overlapping time range policy entries within a time of day suite policy, the time range policy entry with the highest priority is applied first
- only one time of day suite policy entry without a time range (default NO-TIME-RANGE) is allowed for each type of policy
- you cannot modify a time of day suite policy entry after you create the entry
- you cannot assign the same priority of a global policy within the same policy type
- you cannot assign the same priority of a local policy within the same policy type
- you cannot assign the same time range of a global policy within the same policy type
- you cannot assign the same time range a local policy within the same policy type
- you cannot distribute a time of day suite policy entry to a local policy if the local policy already has been assigned the same time range as the global policy
- you cannot distribute a time of day suite policy entry to a local policy if the local policy already has been assigned the same priority as the global policy
- all time of day suite policy entries of a local policy are replaced by the time of day suite policy entries of a global policy if none of the entries from the local policy have the same priority or time ranges as the global policy

1 Choose Policies→Time of Day→Time Of Day Suite from the 5620 SAM main menu. The Manage Time-of-day suite form opens.

2 Perform one of the following:

a Specify a filter to search for an existing suite. Select a suite in the filtered list and click on the Properties button.

b Click on the Create button. The Time of Day Suite (Create) form opens.

3 Configure the parameters:

- Name
- Description

4 Click on the TOD Suite Entries tab button.

5 Click on the Ingress tab button.

6 Assign a time range to ingress filter policies, if required. Perform the following steps:

i Click on the Add button. The Ingress *type_of_filter* (Create) form opens.

ii Configure the Priority parameter.

iii Click on the Select button beside the Name parameter. The Select Time Range - Ingress *filter* list form opens.

iv Select a time range in the list and click on the OK button. The Select Time Range - Ingress *filter* list form closes.

v Click on the Select button beside the Filter ID parameter. The ingress filter list form opens.

vi Select a filter in the list and click on the OK button. The ingress filter list form closes.

vii Click on the OK button to save the configuration and close the form. The Time of Day Suite (Create) form reappears with the time of day suite entry displayed in the list.

7 Assign a time range to ingress QoS policies, if required. Perform the following:

i Click on the QoS tab button.

ii Click on the Add button. The Ingress QoS (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button in the Time Range panel. The Select Time Range - Ingress QoS list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Ingress QoS list form closes.

vi Click on the Select button in the Policy panel. The Select Policy - Ingress QoS list form opens.

vii Select an entry in the list and click on the OK button. The Select Policy - Ingress QoS list form closes.

viii Click on the Select button in the 7210 Policy panel. The Select 7210 Policy - Ingress QoS list form opens.

ix Select an entry in the list and click on the OK button. The Select 7210 Policy - Ingress QoS list form closes.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The Time of Day Suite (Create) form reappears.

8 Assign a time range to ingress scheduler policies, if required. Perform the following:

i Click on the Scheduler tab button.

ii Click on the Add button. The Ingress Scheduler (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button beside the Name parameter. The Select Time Range - Ingress Scheduler list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Ingress Scheduler list form closes.

vi Click on the Select button beside the Displayed Name parameter. The Select Policy Name - Ingress Scheduler list form opens.

vii Select a filter in the list and click on the OK button. The Select Policy Name - Ingress Scheduler list form closes.

viii Click on the OK button to save the configuration and close the form. The Time of Day Suite (Create) form reappears with the time of day suite entry displayed in the list.

9 Click on the Egress tab button.

10 Assign a time range to egress filter policies, if required. Perform the following steps:

i Click on the Add button. The Egress *type_of_filter* (Create) form opens.

ii Configure the Priority parameter.

iii Click on the Select button beside the Name parameter. The Select Time Range - Egress *filter* list form opens.

iv Select a time range in the list and click on the OK button. The Select Time Range - Egress *type_of_filter* list form closes.

v Click on the Select button beside the Filter ID parameter. The egress filter list form opens.

vi Select a filter in the list and click on the OK button. The egress filter list form closes.

11 Assign a time range to egress QoS policies, if required. Perform the following:

i Click on the QoS tab button.

ii Click on the Add button. The Egress QoS (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button in the Time Range panel. The Select Time Range - Egress QoS list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Egress QoS list form closes.

vi Click on the Select button in the Policy panel. The Select Policy - Egress QoS list form opens.

vii Select an entry in the list and click on the OK button. The Select Policy - Egress QoS list form closes.

12 Assign a time range to egress scheduler policies, if required. Perform the following:

i Click on the Scheduler tab button.

ii Click on the Add button. The Egress Scheduler (Create) form opens.

iii Configure the Priority parameter.

iv Click on the Select button beside the Name parameter. The Select Time Range - Egress Scheduler list form opens.

v Select a time range in the list and click on the OK button. The Select Time Range - Egress Scheduler list form closes.

vi Click on the Select button beside the Displayed Name parameter. The Select Policy Name - Egress Scheduler list form opens.

vii Select a filter in the list and click on the OK button. The Select Policy Name - Egress Scheduler list form closes.

13 Click on the OK button. The Time of Day Suite (Create) form closes and the Manage Time-of-day suite form reappears.

14 Close the Manage Time-of-day suite form.

Procedure 47-3 To perform a time range entry assignment analysis

1 Choose Tools→Time Range Entry Assignment from the 5620 SAM main menu. The List Time Range Entry Assignment form opens.

2 Click on the Select button to choose a site for the analysis. The Select Site to Analyze form opens.

3 Select a site in the list and click on the OK button.

4 Configure the Time Range Entry Container Type parameter.

5 Click on the Select button beside the Time Range Entry Container Type to choose a specific object of the container type you chose in step 4. The appropriate list form opens.

6 Configure the filter criteria.

7 Click on the Search button.

8 Double-click on an entry in the list, or select an entry and click on the OK button. The list form closes and the List Time Range Entry Assignment form refreshes.

9 Configure the Search by Time Of Day Entry Type and Time Of Day Entry Policy Type parameters.

10 Configure the Start Date and End Date parameters.

11 Click on the Search button. A list of time range entries that meet the defined criteria is displayed.

12 Double-click on an entry to view information about the time range policy and time of day suite policy. The Time Range Entry Assignment: *Start Date End Date* form opens.

13 Click on the Cancel button to close the Time Range Entry Assignment: *Start Date End Date* form.

14 Close the List Time Range Entry Assignment form.

48 — Ethernet service policies

48.1 Ethernet service policies overview

This chapter describes how to configure the UNI and SAP profiles associated with OmniSwitch Ethernet services.

48.2 Ethernet service policies procedures

The following procedures describe how to configure Ethernet service policies.

Procedure 48-1 To configure an OmniSwitch Ethernet service UNI profile

1 Choose Policies→Layer 2→AOS Ethernet Service from the 5620 SAM main menu. The Manage Ethernet Service Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing UNI profile. Select a profile in the filtered list and click on the Properties button.

b Click on the Create button and choose Create UNI Profile. The Ethernet Service UNI Profile, Global Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- STP
- GVRP
- 802.1x
- 802.3ad
- MVRP
- OAM
- UDLD
- VTP
- PVST
- UPLINK
- 802.1AB
- AMAP
- LACPMARKER
- PAGP
- CDP
- DTP
- VLAN
- Tunnel MAC

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button. The Ethernet Service UNI Profile, Global Policy (Create) form closes.

5 To create more UNI profiles repeat steps 2b to 4.

6 Close the Manage Ethernet Service Policies form.

Procedure 48-2 To configure an OmniSwitch Ethernet SAP profile

1 Choose Policies→Layer 2→AOS Ethernet Service from the 5620 SAM main menu. The Manage Ethernet Service Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing SAP profile. Select a profile in the filtered list and click on the Properties button.

b Click on the Create button and choose Create SAP Profile. The Ethernet Service SAP Profile (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Ingress Bandwidth (Mb)
- Bandwidth Sharing
- CVLAN Treatment
- Priority Mapping
- Priority

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the OK button. The Ethernet Service SAP Profile, Global Policy (Create) form closes.

5 To create more SAP profiles repeat steps 2b to 4.

6 Close the Manage Ethernet Service Policies form.

49 — Service PW template policies

49.1 Service PW template policies overview

Service PW templates are policies that enable PE routers to discover the other participating PE routers in an LDP or BGP VPLS.

49.2 Service PW template policies procedures

The following procedure describes how to configure service PW templates.

Procedure 49-1 To create or configure a PW Template

1 Choose Manage→Service→Service PW Template from the 5620 SAM main menu. The Service PW Template Manager form opens.

2 Perform one of the following:

- **a** Click on the Create button. The Service PW Template (Create) form opens with the General tab displayed.
- **b** Search for an existing policy you want to modify.
  - **i** Click on the Search button.
  - **ii** Select a policy from the displayed list.
  - **iii** Click on the Properties button. The Service PW Template (Edit) form opens with the General tab displayed.

3 Perform one of the following:

- **a** Click on the Populate from Pseudowire button.

  This allows you to populate the Service PW Template form using an existing pseudowire (SDP Binding) as a base.
  - **i** After clicking the Populate from Pseudowire button, the Select a Pseudowire form opens.
  - **ii** Click on the Search button.
  - **iii** Choose the required pseudowire from the displayed list.

iv Click on OK. All of the relevant values are copied into the Service PW Template form.

v Go to step 19.

b Populate the form manually.

i Configure the following parameters:

- Policy ID
- Auto-Assign ID
- Description
- Enable Hash Label
- Use Provisioned SDP
- Enable Force-Vlan-VC Forwarding
- Enable Control Word
- VC Type
- Collect Stats

ii Select an Accounting Policy, if required, by clicking on the Select button. The Select Accounting Policy form opens.

iii Select an accounting policy and click OK, or create a new one by clicking on the Create button.

4 Click on the MAC tab button.

5 Configure the following parameters, as required:

- MAC Learning
- MAC Aging
- Discard Unknown Source
- Limit MAC Move
- MAC Pinning
- VLAN VC Tag
- MAC Address Limit

6 Click on the Split Horizon Group tab button.

7 Configure the following parameters, as required:

- Name
- Description
- Restrict Protected Source
- Restrict Unprotected Destination

8 Click on the Ingress Filters tab button.

9 Configure the Ingress Filter Type parameter, if required.

10 Click on the Egress Filters tab button.

11 Configure the Egress Filter Type parameter, if required.

12 Click on the IGMP tab button.

13 Configure the following parameters, as required:

- IGMP Version
- IGMP Fast Leave
- IGMP Import Policy
- IGMP Last Member Interval (deciseconds)
- IGMP Max Number Groups
- IGMP Max Number Sources Per Group
- IGMP General Query Interval (seconds)
- IGMP Query Response Interval (seconds)
- IGMP Robust Count
- IGMP Sent Queries

14 If you need to re-configure an existing, distributed local PW Template, go to step 15. Otherwise go to step 19.

15 Click on the Local Definitions tab button.

16 Select the required entry from the list and click the Properties button. The Service PW Template - Local Policy - (Edit) form opens with the General tab displayed.

17 Make any required changes here - the tabbed pages are essentially the same as for the global definition of the PW Template covered in steps 3 through 13.

18 Click the Re-evaluate PW Template button to run an evaluation of the modified template. A pop-up window appears indicating if the re-evaluation was successful. If it was not, the reason for the failure is displayed. If you make any subsequent modifications, you can re-evaluate the template again.

19 Click on the OK button to confirm your changes. The Service PW Template - Local Policy - (Edit) form closes.

20 Click on the OK button to close the Service PW Template - Global Policy form.

50 — Auto tunnels policies

50.1 Auto tunnels policies overview

The 5620 SAM supports the creation of service tunnels for groups of NEs based on mesh, hub-and-spoke, or ring network topology. The 5620 SAM uses tunnel management policies to define the conditions for service tunnel creation. A tunnel management policy has four components:

- the group of NEs to which the policy applies and their collective role
- the tunnel specifications, for example, the tunnel type and underlying transport
- the topology specification, for example, mesh
- a tunnel template must be applied

You can specify a system-generated naming format, or you can also specify a naming prefix. The resulting name is a combination of the user-specified prefix and the ID of the tunnel.

Tunnel templates

You must create a tunnel policy using a tunnel template. You can view, but not save or reapply, a tunnel policy created using 5620 SAM releases earlier than 7.0. For example, if a new tunnel is required as a result of group member changes, the tunnel cannot be created if the policy was created using a 5620 SAM release earlier than 7.0. If such a tunnel must be deleted as a result of group member changes, the tunnel can be deleted regardless of the state of the policy.

Depending on the tunnel type selected for an auto tunnel, an SDP or LSP tunnel template can be selected. For an RSVP LSP tunnel type, one LSP template must be selected. For an RSVP SDP tunnel type, 16 LSP templates can be selected. When an LSP parent template with more than one LSP path child templates is specified, more than one LSP path is created.

A template should be configured to be deployed to a majority of the NE types. The user must validate the template and enter appropriate changes to the script before the template can be deployed in an auto tunnel policy. The parameters that can be modified, depend on the template type.

The following parameters can be modified for an SDP template:

- name
- source NE ID
- destination NE ID
- displayed name
- LDP enabled
- underlying transport
- path ID

The following parameters can be modified for an LSP template:

- name
- source NE ID
- path ID
- displayed name

- destination IP address
- destination NE ID

Note — If the policy ID value is specified by a format policy in the template, the path ID value must be set to 0.

When you execute an LSP path template in an auto tunnel policy, the following parameters are substituted with the values from the original tunnel policy:

- name
- resource ID

You can create templates from examples. Use an example as a starting point to create service or tunnel templates with or without format and range policies. When a template with format and range policies is associated with an auto tunnel rule, the format and range policies defined in the template override the name defined in the auto tunnel rule.

Class of Service

When you implement CoS, consider the following:

- To create a CoS-based SDP using RSVP, a user must apply a combination of SDP and LSP templates. An SDP tunnel template can use up to 16 LSPs. For CoS routing, 10 LSP s are required for the following: 1 for default, 1 for multicast, and 8 LSPs for different CoS routes.
- For CoS-based forwarding, at least one LSP template must be associated with the SDP. The LSP template must be specified as the default LSP template for CoS forwarding.
- When LSP templates are not specified, during non-CoS-based forwarding, the SDPs are created without LSPs attached.

Tunnel groups

A tunnel group is defined as collection of network resources, such as NEs, that perform the same role in the network; for example, the way that the designation of a port as an access or network port defines the role of the port in the network.

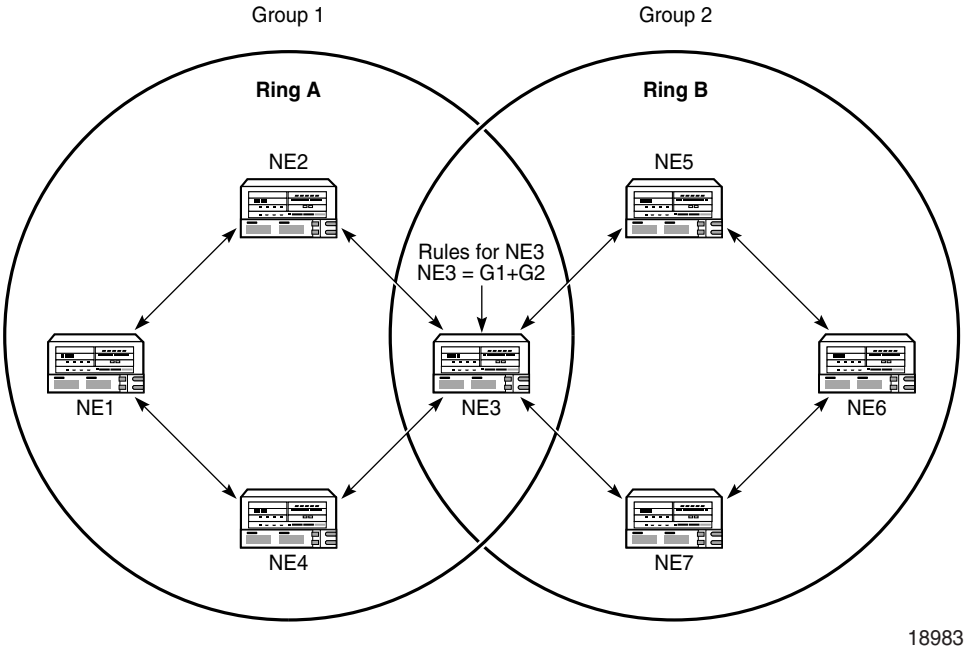
By grouping resources by role, a common policy-based management framework can be used to ensure the appropriate configuration of resources, for example, create service tunnels for different topologies.

The following conditions apply to tunnel groups.

- An NE can belong to multiple groups.
- A group is ordered or unordered depending on the requirements. The members in a group must be ordered when you create some topologies; for example, a ring topology. Topologies such as mesh or hub-and-spoke, in which NEs are not linearly arranged, do not need an ordered group.

- A non-5620 SAM-managed NE can belong to the tunnel group to which it was added, however, it is not active as a destination NE during rule execution.
- When two or more tunnel groups share an NE, the shared NE performs the roles defined for each group. In Figure 50-1, Group 1 contains routers NE1, NE2, NE3, and NE4, and Group 2 contains routers NE3, NE5, NE6, and NE7. NE3 is the intersection set of Groups 1 and 2, therefore NE3 assumes the roles defined for Groups 1 and 2.

Figure 50-1 NE shared by two tunnel groups



Tunnel policy creation requires the configuration of the following:

- one or more group conditions to specify the NEs that are included in the topology
- a least one tunnel template configuration
- one or more tunnel definitions that specify the service-tunnel characteristics, such as the type of tunnel and the underlying transport

Tunnel policy rules

The following conditions apply to tunnel policies.

- A 5620 SAM operator requires topology-management privileges to create or modify a tunnel policy.
- A tunnel can originate and terminate on 5620 SAM-managed NEs. Tunnels cannot originate on non-SAM-managed NEs, however, tunnels can terminate on non-SAM-managed NEs.
- When an NE, that is in a rule-based group, is unmanaged or delete, it is identified as unmanaged in the rule-based group. Tunnels to the NE are not removed, however tunnels from the NE are removed from 5620 SAM.

- When an auto-tunnel rule is created for a group that contains non-SAM-managed NEs, tunnels cannot be created to and from the NE using that rule.
- When you add NEs to a tunnel group that is in use, new tunnels are created according to the policy definition.
- A group condition must contain at least one group of NEs.
- Tunnel elements are not updated dynamically.
- An unmanaged NE is removed from the tunnel groups to which the NE belongs. The associated service tunnels are also removed if they originate from a managed NE. A service tunnel that originates on an unmanaged NE is retained, but is not included in the tunnel group after reconfiguration.
- When a service tunnel created by a tunnel policy is removed, the policy does not attempt to recreate the tunnel.
- You can modify the tunnel definition in a tunnel policy when the tunnel policy has not yet created a service tunnel.

Not all NEs that are assigned to a topology rule share the same functionality. The topology rule runs capability checks on the source NEs to determine whether specific tunnels or tunnel configurations can be applied. Table 50-1 lists the auto tunnel rules that are supported by each NE.

Table 50-1 Auto tunnel rules and NE support

Auto tunnel rule	7710 SR 7450 ESS 7750 SR	7705 SAR			7250 SAS-ES
		1.0	1.1	2.0	
SDP LDP	X	X	X	X	–
SDP GRE	X	–	X	X	–
SDP LSP	X	X	X	X	X
Dynamic LSP	X	–	–	X	X
CoS-based SDP	X	–	–	–	–
LDP-over-RSVP	X	–	–	–	–

50.2 Workflow to configure auto tunnel creation

The following list describes the step required to setup an auto tunnel:

1 Configure a tunnel template from one of the following:

- template creation form
- network or service object properties form
- pre-configured tunnel template

See the *5620 SAM Scripts and Templates Developer Guide* for more information.

2 Configure rule-based groups. See Procedure 50-1 for more information.

3 Convert an auto tunnel rule created using a 5620 SAM release earlier than 7.0 to a template-based auto tunnel rule. See Procedure 50-2 for more information.

4 Configure mesh or ring topology rules, if required. See Procedure 50-3 for more information.

5 Configure hub and spoke topology rules, if required. See Procedure 50-4 for more information.

6 Create a service and specify Automatic Mesh SDP Binding Creation.

50.3 Auto tunnels policies procedures

The following procedures describe how to configure and manage auto tunnel elements.

Procedure 50-1 To create a rule-based group

1 Choose Policies→Auto Tunnels→Rule-Based Groups from the 5620 SAM main menu. The Manage Rule-Based Groups form opens.

2 Click on the Create button and choose Create Rule-Based NE Group from the menu. The Rule-Based NE Group (Create) form opens.

3 Configure the parameters.

- Group Name
- Description
- Order

4 Click on the Apply button to save the changes. The Group Members tab becomes configurable.

5 Click on the Group Members tab button.

6 Depending on the value specified for the Order parameter, perform one of the following:

a Add members to an unordered group.

i Click on the Add button. The Select Network Elements form opens.

ii Select an NE and click on the OK button. A dialog box appears.

iii Click on the OK button. The Rule-Based NE Group (Edit) form reappears with the member NE displayed.

iv Repeat steps 6i to iii to add another member to the unordered group, if required or go to step 7.

b Add members to an ordered group.

i Click on the Add button. The Select Network Elements form opens.

ii Select an NE and click on the OK button. A dialog box appears.

iii Click on the OK button. The Rule-Based NE Group (Edit) form reappears with the member NE displayed.

iv Repeat steps 6i to iii to add a member to the end of the ordered group list, if required.

v To insert an NE between two NEs in the ordered group list, click on the Insert button and perform steps 6ii to iii.

7 Click the OK button. A dialog box appears.

8 Click the Yes button. The Rule-based NE Group (Edit) form closes and the Manage Rule-Based Groups form reappears.

9 Close the Manage Rule-Based Groups form.

Procedure 50-2 To convert old auto tunnel rules to template-based auto tunnel rules

Perform this procedure to convert tunnel policies created using a 5620 SAM Release earlier than 7.0 to template-based auto tunnel rules.

The number and type of templates that are displayed depend on the policy type. For example, a mesh SDP policy with GRE as the underlying transport requires 1 SDP template. A hub-and-spoke SDP policy with LSP as the underlying transport requires two SDP and two LSP templates.

When you apply a new template to an old auto tunnel rule, you must ensure that the parameter values defined in the template are consistent with the values that you defined in the original auto tunnel rule. For example, if you convert an auto tunnel rule that requires you to apply an LSP template, you must choose a template in which the LSP Bandwidth and Fast Re-Route parameter values in the template match the values defined in the old auto tunnel rule.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Click on the Search button. A list of old and new auto tunnel rules is displayed.

3 Select an old auto tunnel rule in the list.

4 Click on the Properties button. An *Auto Rule_type* (Edit) form opens.

5 Click on the Convert button. The Convert Old Rule form opens.

Note — The Convert button is displayed only if the selected policy has been created using a 5620 SAM Release earlier than 7.0.

6 Perform one or both of the following, depending on the type of tunnel and the underlying transport value.

When the tunnel type value is SDP and the underlying transport value is RSVP-LSP, you must choose a SDP and an LSP template. When the tunnel type value is LSP, you must choose an LSP template only.

a Click on the Select button beside the Name parameter in the SDP Template panel. The Select Template form opens.

b Click on the Select button beside the Name parameter in the LSP Template panel. The Select Template form opens.

7 Select a template in the list and click on the Execute button. The Convert Old Rule form is refreshed with the template information and the Execute button is replaced with a Done button.

Note — After an auto tunnel rule is converted, the Convert button is not displayed when the *Auto Rule_type* (Edit) form is opened.

8 Click on the Tunnel Definition tab in the *Auto Rule_type* (Edit) form. The Template panel is refreshed with the template information.

9 Close the Convert Old Rule form and close the *Auto Rule_type* (Edit) form.

Procedure 50-3 To create a mesh or ring topology rule

Perform this procedure to create a mesh topology rule for service-tunnel creation. A template must be applied to an auto-tunnel policy. You must configure an LSP or SDP tunnel template before you can deploy a template to an LSP or SDP tunnel. See the *5620 SAM Scripts and Templates Developer Guide* for information about creating tunnel templates.

Note — You must convert auto tunnels created using the 5620 SAM, Release 6.1 or earlier, that are not associated with a tunnel template. See Procedure 50-2 for more information.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Click on the Create button and choose one of the following:

a Create Mesh Topology Rule. The Mesh Topology Rule (Create) form opens with the General tab displayed.

b Create Ring Topology Rule. The Ring Topology Rule (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Naming Format
- User Specified Naming Prefix
- Template Versions
- Tunnel Creation Pacing Interval (seconds)
- Auto-Rule Execution

4 Click on the LERs Definition tab button.

5 Click on the Add button. The Select Rule-Based Group form opens.

6 Click on the Search button.

7 Select a rule-based group in the list and click on the OK button. The Select Rule-Based Group form closes and the group is displayed on the Topology Rule (Create) form.

8 Click on the Tunnel Definition tab button.

9 Perform one of the following to configure the Tunnel Type parameter:

a Choose SDP.

b Choose RSVP-LSP; go to step 19.

10 Click on the SDP tab button.

11 Click on the Select button beside the Script ID parameter. The Select SDP Template form opens with a list of configured templates.

12 Select a template in the list. See Procedure 5-2 for information about creating a tunnel template.

13 Click on the OK button. The Select SDP Template form closes and the SDP template information is displayed on the Topology Rule (Create) form.

14 Configure the parameters:

- Underlying Transport
- Class Forwarding Capability
- Administrative State

  The Class Forwarding Capability and Administrative State parameters are configurable when the Underlying Transport parameter is set to RSVP-LSP.

  The Administrative State parameter is not configurable when the Class Forwarding Capability parameter is disabled.

15 If you set the Underlying Transport parameter to RSVP-LSP, the LSPs tab is displayed. Click on the LSPs tab button; otherwise, go to step 22.

16 Click on the Add button. The Select LSP Template form opens.

17 Select a template in the list and click on the OK button. The Select LSP Template form closes and the Topology Rule (Create) form displays the LSP template information.

18 Go to step 22.

19 Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

20 Select a template in the list and click on the OK button. The Select LSP Template form closes and the LSP template information is displayed on the Topology Rule (Create) form.

21 Configure the Enable LDP-over-RSVP parameter.

22 Click the OK button. The Topology Rule (Create) form closes and the Manage Auto Tunnel Rules form reappears.

23 Close the Manage Auto Tunnel Rules form.

Procedure 50-4 To create a hub-and-spoke topology rule

Note — You must convert auto tunnels created using the 5620 SAM, Release 6.1 or earlier, that are not associated with a tunnel template. See Procedure 50-2 for more information.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Click on the Create button and choose Create Hub and Spoke Topology Rule from the contextual menu. The Hub and Spoke Topology Rule (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Naming Format
- User Specified Naming Prefix
- Template Versions
- Tunnel Creation Pacing Interval (seconds)
- Auto-Rule Execution

4 Click on the Hub LERs Definition tab button.

5 Click on the Add button. The Select form opens.

6 Click on the Search button. A list of rule-based groups is displayed.

7 Select a group in the list and click on the OK button. The Select form closes and the group is displayed on the Hub and Spoke Topology Rule (Create) form.

8 Click on the Spoke LERs Definition tab button.

9 Click on the Add button. The Select form opens.

10 Click on the Search button. A list of rule-based groups is displayed.

11 Select a group and click on the OK button. The Select form closes and the group is displayed on the Hub and Spoke Topology Rule (Create) form.

12 Click on the Hub Tunnel Definition tab button.

13 Perform one of the following to configure the Tunnel Type parameter:

a Choose SDP.

b Choose RSVP-LSP; go to step 16.

14 Click on the SDP tab button.

15 Click on the Select button beside the Script ID parameter. The Select SDP Template form opens with a list of configured templates.

i Select a template in the list.

ii Click on the OK button. The Select SDP Template form closes and the SDP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

iii Configure the parameters:

- Underlying Transport
- Class Forwarding Capability
- Administrative State

  The Class Forwarding Capability and Administrative State parameters are displayed when the Underlying Transport parameter is set to RSVP-LSP.

  The Administrative State parameter is configurable when the Class Forwarding Capability parameter is enabled.

iv If you set the Underlying Transport parameter to RSVP-LSP, the LSPs tab is displayed. Click on the LSPs tab button; otherwise go to step 18.

v Click on the Add button. The Select LSP Templates form opens.

vi Select a template in the list and click on the OK button. The Select LSP Templates form closes and the Associated LSP Templates panel displays the LSP template information.

vii Select the LSP template in the Associated LSP Templates panel. If the Class Forwarding Capability parameter in step 15 is enabled, the buttons in the Class Forwarding panel become enabled; otherwise, go to step 18.

viii Click on the Set as Default LSP button to specify the LSP as the default, if required.

ix Click on the Set as Multicast LSP button to specify that the LSP is a multicast LSP, if required.

x Click on the Choose a Forwarding Class button and choose a forwarding class from the contextual menu, if required.

16 Click on the LSP tab button.

17 Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

i Select a template in the list and click on the OK button. The Select LSP Template form closes and the LSP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

ii Configure the Enable LDP-over-RSVP parameter.

18 Click on the Spoke Tunnel Definition tab button.

19 Perform one of the following to configure the Tunnel Type parameter:

a Choose SDP.

b Choose RSVP-LSP; go to step 21.

20 Perform the following steps.

i Click on the SDP tab button.

ii Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

iii Select a template in the list and click on the OK button. The Select LSP Template form closes and the LSP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

iv Configure the Underlying Transport parameter.

21 Perform the following steps.

i Click on the LSP tab button.

ii Click on the Select button beside the Script ID parameter. The Select LSP Template form opens.

iii Select a template in the list and click on the OK button. The Select SDP Template form closes and the SDP template information is displayed on the Hub and Spoke Topology Rule (Create) form.

iv Configure the Enable LDP-over-RSVP parameter.

22 Click the OK button. The Hub and Spoke Topology Rule (Create) form closes and the Manage Auto Tunnel Rules form reappears.

23 Close the Manage Auto Tunnel Rules form.

Procedure 50-5 To modify a topology rule

Use this procedure to change the parameter settings for a topology rule.

Note — You can modify group conditions and tunnel definitions only when a topology rule is not active.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button.

3 Select a rule and click on Properties. The system displays the rule properties form.

4 Make the required changes to the rule.

5 Click on OK button. A dialog box appears.

6 Click the Yes button. The rule properties form closes and the Manage Auto Tunnel Rules form reappears.

7 Close the Manage Auto Tunnel Rules form.

Procedure 50-6 To reapply a topology rule

Use this procedure to force a rule to be re-evaluated. Missing or changed configurations are corrected. A rule can be re-evaluated at any time after the rule is created.

Note — When a hopless path rule is changed by the user, the rule cannot be corrected by the reapply operation.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button.

3 Select a rule and click on Properties. The system displays the rule properties form.

4 Click on the Execute button.

5 Close the Manage Auto Tunnel Rules form.

Procedure 50-7 To import tunnels not managed by topology rules

Use this procedure to import a tunnel that is not managed by a topology rule. After you import the tunnel, the tunnel is manage by the rule. However, the rule does not enforce the source and destination IDs to match the rule group. If the imported tunnel is not part of the group, the execute button or change notifications by the group members do not apply, even though the imported tunnel is part of the rule.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button. A list of auto tunnel rules is displayed.

3 Select a rule in the list and click on the Properties button. The system displays the *Topology_Rules* (Edit) form.

4 Click on the Created/Imported Tunnel Elements tab button.

5 Click on the Import Tunnels button. An Import Tunnels form opens.

6 Perform one of the following:

   a Click on the Add SDPs button. The Select SDPs form opens. Go to step 8.

   b Click on the Add LSPs button. The Select LSPs form opens.

7 Click on the Search button. A list of LSPs is displayed.

   i Choose one or more LSPs in the list.

   ii Click on the OK button. The Select LSPs form closes and the Import Tunnels form is refreshed with the chosen LSPs. Go to step 9.

8 Click on the Search button. A list of SDPs is displayed.

   i Choose one or more SDPs in the list.

   ii Click on the OK button. The Select SDPs form closes and the Import Tunnels form is refreshed with the chosen SDPs.

9 Click on the Import button. The Import Tunnels form closes.

10 Click on the Created/Managed Tunnel Elements tab button to view the imported networks.

11 Close the *Topology_Rules* (Edit) form.

12 Close the Manage Auto Tunnel Rules form.

Procedure 50-8 To display and delete tunnel elements

1 Choose policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button. A list of service-tunnel topology rules is displayed.

3 Select a rule and click on the Properties button. The rule properties form is displayed.

4 Click on the Created/Imported Tunnel Elements tab button.

5 Click on the Search button.

6 Perform one of the following actions to delete tunnel elements, as required:

   a Click on the Delete Unused button to delete tunnels that are no longer applied to a group. A dialog box appears.

   b Click on the Delete All button to delete all tunnels that are not associated with a service. A dialog box appears.

7 Click on the Yes button. The 5620 SAM deletes the elements and removes them from the list.

8 Close the rule properties form. The Manage Auto Tunnel Rules form reappears.

9 Close the Manage Auto Tunnel Rules form.

Procedure 50-9 To execute a topology rule

Use this procedure at any time after a rule is created. The execute button forces the topology rule to be evaluated; any missing or configuration changes are corrected.

Note — The 5620 SAM supports the reapply function, except in reference to hop-less path changes. If a hop-less path changes, it may not be corrected by a reapply operation.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button. A list of service-tunnel topology rules is displayed.

3 Select a rule and click on the Properties button. The rule properties form is displayed.

4 Click on the Execute button.

5 Close the topology map.

Procedure 50-10 To display missing tunnel elements

Perform this procedure to display the missing tunnel elements. A missing tunnel element is one that the 5620 SAM is unable to create based on the specified tunnel rules, or a tunnel element that is deleted.

1 Choose Policies→Auto Tunnels→Auto Tunnel Rules from the 5620 SAM main menu. The Manage Auto Tunnel Rules form opens.

2 Configure the filter criteria and click on the Search button. A list of service-tunnel topology rules is displayed.

3 Select a rule and click on the Properties button. The rule properties form is displayed.

4 Click on the Missing Tunnel Elements tab button.

5 Click on the Search button.

6 Select a missing tunnel element and click on the Properties button. The element properties form opens.

7 View the element properties.

8 Close the element properties form. The rule properties form reappears.

9 Close the rule properties form. The Manage Auto Tunnel Rules form reappears.

10 Close the Manage Auto Tunnel Rules form.

51 — VRRP policies

51.1 VRRP policies overview

VRRP priority control-policies manage VR backup router priorities. The policies override the base priority value, depending on NE events or conditions. You can configure a VRRP policy only for the non-owner VRRP instance; the same policy can be applied to IPv4 and IPv6 VRRP instances.

The main function of a VRRP priority-control policy is to define the conditions or events that affect the VR ability to communicate with outside hosts or portions of the network. When at least one of these events is true, the base priority for the VR instance is affected in one of two ways:

- an explicit value is overridden
- a value is subtracted from the sum of delta priorities

The result is the actual in-use priority for the VR instance. Any priority event may be configured as an explicit event or a delta event.

Table 51-1 describes the policy events that you can configure using the 5620 SAM.

Table 51-1 VRRP policy events

Policy Event	Description
Host unreachable	Configures a host unreachable priority-control event that monitors the ability of a host to receive an ICMP echo reply packet from a specific IP host address. A host unreachable priority-control event creates a continuous ICMP echo request (ping) probe to the specified IP address. During ping failure, the event is considered to be set. During ping success, the event is considered to be cleared.
IPv6 Host unreachable	Configures an IPv6 host unreachable priority-control event that monitors the ability of a host to receive an ICMP echo reply packet from a specific IPv6 host address. An IPv6 host unreachable priority-control event creates a continuous ICMP echo request (ping) probe to the specified IPv6 address. During ping failure, the event is considered to be set. During ping success, the event is considered to be cleared.
LAG port down	Configures a LAG priority-control event that monitors the operational state of the links and each port in the LAG. When one or more of the ports enters the operational down state, the event is considered to be set. When all ports enter an operational up state, the event is considered to be clear.
Route unknown	Configures a route unknown priority-control event that monitors the existence of a specific active IP route prefix in the routing table. Route unknown defines a link between the VRRP priority-control policy and the RTM. The RTM registers the specified route prefix as monitored by the policy. If any change (add, delete, new next hop) occurs relative to the prefix, the policy is notified and takes action according to the priority event definition.
Port Down Events	Configures an override or adjustment to the base priority value of a VRRP VR instance depending on the operational state of the event. Port Down events can only be configured on the local definitions of VRRP policies.

As priority events clear in the policy, the in-use priority can eventually be restored to the base priority value.

51.2 VRRP policies procedures

The following procedures describe how to configure and manage VRRP policies.

Procedure 51-1 To configure a VRRP priority-control policy

1 Choose Policies→VRRP from the 5620 SAM main menu. The Manage VRRP Policies form opens.

2 Perform one of the following:

- **a** Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.
- **b** Click on the Create button. The VRRP Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- ID
- Displayed Name
- Description
- Delta in Use Limit

4 Click on the Apply button.

5 Perform one of the following steps:

- **a** For IPv4 hosts, click on the Host Unreachable tab button.
  - **i** Click on the Add button. The Host Unreachable Event (Create) form opens.
  - **ii** Configure the parameters:
    - IP Address
    - Hold Clear (seconds)
    - Hold Set (seconds)
    - Priority Type
    - Priority
    - Limit of Echo Request Failures
    - Interval For Echo Request (seconds)
    - Timeout For Echo Request (seconds)
  - **iii** Click on the OK button. A dialog box appears.

iv Click on the OK button. The Host Unreachable Event form reappears with the newly created filter entries displayed.

v Go to step 6.

b For IPv6 hosts, click on the IPv6 Host Unreachable tab button.

i Click on the Add button. The IPv6 Host Unreachable Event (Create) form opens.

ii Configure the parameters:

- IP Address
- Interface Name
- Hold Clear (seconds)
- Hold Set (seconds)
- Priority Type
- Priority
- Limit of Echo Request Failures
- Interval For Echo Request (seconds)
- Timeout For Echo Request (seconds)

The Interface Name parameter is only configurable when the host IP Address parameter is a Link Local Address.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The IPv6 Host Unreachable Event form reappears with the newly-created filter entries displayed.

v Go to step 6.

6 Click on the Lag Port Down tab button.

7 Click on the Add button. The Lag Port Down Event (Create) form opens with the General tab displayed.

8 Configure the parameters:

- LAG ID
- Hold Clear (seconds)
- Hold Set (seconds)

9 Click on the Number Down tab button.

10 Click on the Add button. The Number Down (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Number of Ports Down
- Priority
- Priority Type

12 Close the Number Down (Create) form. A dialog box appears.

13 Click on the OK button.

14 Click on the OK button. A dialog box appears.

15 Click on the OK button. The Lag Port Down Event form reappears with the newly created filter entries displayed.

16 Click on the Route Unknown tab button.

17 Click on the Add button. The Route Unknown (Create) form opens with the General tab displayed.

18 Configure the parameters:

- IP Address
- Mask
- Hold Clear (seconds)
- Hold Set (seconds)
- Priority
- Priority Type
- Protocol
- Less Specific

19 Click on the Next Hop tab button.

20 Click on the Add button.

If the IP Address you specify on the General tab is an IPv4 address, the NextHop (Create) form opens; if it is an IPv6 address, the NextHopV6 (Create) form opens.

21 Configure the Hop Address parameter.

22 Configure the Interface Name parameter if the IPv6 Next Hop Address is a Link Local Address.

23 Click on the OK button. A dialog box appears.

24 Click on the OK button.

25 Click on the OK button.The Manage VRRP Policies form reappears.

26 Click on the Search button to display the newly created policy or policies.

27 Select a policy in the list and click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

28 Close the Manage VRRP Policies form.

52 — 802.1x policies

52.1 802.1x policies overview

The 5620 SAM implementation of the 802.1X protocol provides 802.1X authentication on an individual port basis.

In an 802.1X environment, a user called the supplicant requests access to an access point, called the authenticator. The authenticator forces the supplicant into an unauthorized state, forcing them to send an EAP start message.

The authenticator returns an EAP message to request the user identity. The user returns the identity, which is forwarded by the authenticator to the authentication server. The server authenticates the user and returns an accept or reject message to the authenticator.

If an accept message is received, the authenticator changes the user state to authorized and user traffic is processed.

52.2 802.1x policies procedures

The following procedures describe how to configure and manage 802.1x policies.

Procedure 52-1 To configure an 802.1X policy

Note — Before you can create an 802.1X policy, 802.1X must be enabled on the device. See Procedure 17-13 for information about enabling 802.1X.

1 Choose Policies→Layer 2→802_1x from the 5620 SAM main menu. The Manage 802_1x Policies form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The 802_1x Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Source Address
- Administrative Status
- Description
- Retry Attempts
- Request Timeout

Note — Do not use a colon in the policy name. The 5620 SAM uses colons as separators for the object full name.

4 Click on the RADIUS Servers tab button, if required. Otherwise, go to step 8.

5 Click on the Add button. The RADIUS Server (Create) form opens.

6 Configure the parameters:

- Server Index
- IP Address
- Password
- Authorization Port
- Accounting Port
- Server Type

7 Click on the OK button. The Radius Server (Create) from closes and the 802_1x Policy (Edit) form refreshes with the server information displayed in the Radius Servers tab.

8 Click on the Apply button to save the policy. The 802_1x Policy form is refreshed with additional buttons and tab buttons.

9 Click on the Distribute button to manually distribute the policy locally to devices.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

Policies are also automatically distributed to devices when they are used by resources on the device.

10 Close the 802_1x Policies form.

11 Close the Manage 802_1x Policies form.

53 — PBB MRP policies

53.1 PBB MRP policies overview

This chapter describes how to configure and manage PBB MRP policies.

53.2 PBB MRP policies procedures

The following procedures describe how to configure and manage PBB MRP policies.

Procedure 53-1 To configure a PBB MRP policy

The PBB MRP policy limits the scope of MMRP advertisements to a specific network domain using ISID-based filters for both the MMRP control plane and the B-VPLS data plane. The policy contains a configurable option to instantiate an MMRP tree and related entry only when both an MMRP declaration and registration are received on a port.

1 Choose Policies→Layer 2→PBB MRP from the 5620 SAM main menu. The PBB MRP Policy Manager form opens.

2 Perform one of the following:

a Specify a filter to search for and edit an existing policy. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The PBB MRP Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- Scope
- Default Action

4 Click on the Entries tab.

5 Click on the Add button to create entries for the policy. The PBB MRP Policy Entry (Create) form opens.

6 Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description
- Action

7 Click on the ISID Match Criteria tab.

8 Click on the Add button to specify ISID matching criteria for an entry in the policy. Multiple ISID matching criteria can be specified for each entry. The ISID Match Criteria (Create) form opens.

9 Configure the parameters:

- Low ISID
- High ISID

10 Click on the OK button. A dialog box appears.

11 Click on the OK button. The ISID Match Criteria you specified appears in the list.

12 Perform one of the following:

a Add another set of criteria. Go to step 8.

b Click on the OK button. A dialog box appears.

13 Click on the OK button. The Entries tab page reappears.

14 Click on the OK button. The Entries tab page closes.

15 Close the PBB MRP Policy Manager form.

54 — RADIUS-based accounting policies

54.1 RADIUS-based accounting policies overview

A RADIUS-based accounting policy is used to send accounting information to a RADIUS server whenever a subscriber initiates or terminates a session. The 7710 SR, 7450 ESS, and 7750 SR support the use of RADIUS-based accounting policies.

When a subscriber host is created on a device that uses a RADIUS-based accounting policy, the device generates an accounting-start packet that includes the RADIUS policy parameters. The packet is sent to the RADIUS server. When the subscriber host session ends, the device generates an accounting-stop packet that includes the accounting statistics for the subscriber host.

See chapter 64 for information about configuring RADIUS-based accounting policies for subscriber profiles.

54.2 RADIUS-based accounting policies procedures

The following procedures describe how to configure and manage RADIUS-based accounting policies.

Procedure 54-1 To configure RADIUS-based accounting policies

Perform the following procedure to create a RADIUS-based accounting policy to send subscriber session accounting information to the RADIUS server.

1. Choose Policies→RADIUS Based Accounting from the 5620 SAM main menu. The RADIUS Based Accounting Policies form opens.
2. Click on the Create button. The Radius Accounting Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Session ID Format
- Source Address
- Retry Attempts
- Timeout (seconds)
- Access Algorithm
- RADIUS Attributes
- Use Standard Account Attribute
- Enable Host Accounting
- Enable
- Value (minutes)
- Port Prefix Type
- Port Prefix String
- Port Suffix Type
- Port Type
- Port Type Value
- Calling Station ID Type
- Port Binary Specification

Note — The Port Prefix Type, Port Prefix String, and Port Suffix Type parameters are configurable when the NAS Port ID option is enabled for the RADIUS Attributes parameter.

The Port Type parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter.

The Port Type Value parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter, and the value of Port Type is set to Config.

The Calling Station ID Type parameter is configurable when the Calling Station ID option is enabled for the RADIUS Attributes parameter.

The Port Binary Specification parameter is configurable when the NAS Port option is enabled for the RADIUS Attributes parameter.

4 Configure the Router Instance parameter. If you set the Router Instance parameter to VPRN, perform step 5. Otherwise, go to step 6

Note — The Router Instance parameter is configurable on the 7710 SR and 7750 SR, and on the 7450 ESS, Release 6.0 or later.

5 Configure a VPRN service as a virtual router instance for the RADIUS-based accounting policy. Perform the following:

i Click on the Select button in the VPRN ID panel. The Select VPRN ID - Radius Accounting Policy list form opens.

ii Select a VPRN site in the list and click on the OK button. The Select VPRN ID - Radius Accounting Policy list form closes and the Radius Accounting Policy (Create) form refreshes with the VPRN service information.

6 Configure the RADIUS servers for the policy. Perform the following:

i Click on the RADIUS Servers tab button.

ii Click on the Add button. The RADIUS Server (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Description
- Server IP Address
- Port
- Secret Name

iv Click on the OK button. A dialog box appears.

v Click on the OK button.

vi Repeat steps ii and v to add additional RADIUS servers, as required.

7 Click on the OK button.

8 Perform the following steps.

i Click on the Custom Record tab button. The Significant Change Criteria tab is displayed.

ii Configure the Significant Change Delta parameters.

iii Configure the parameters in the Reference Queue panel:

Note 1 — You can select all options for a parameter by clicking on the Select All button beside the counters.

Note 2 — You can deselect all options for a parameter by clicking on the Deselect All button beside the counters.

- All Queues
- Ingress Counters
- Egress Counters

iv If the All Queues parameter is enabled, go to step vii.

v Click on the Select button below the All Queues parameter to choose a queue to monitor for the significant change. The Select Queue form opens.

vi Select a queue in the list and click on the OK button. The Select Queues form closes and the queue ID is displayed on the form.

vii Configure the parameters in the Reference Override panel:

Note 1 — You can select all options for a parameter by clicking on the Select All button beside the counters.

Note 2 — You can deselect all options for a parameter by clicking on the Deselect All button beside the counters.

- All Overrides
- Ingress Counters
- Egress Counters

viii If you do not enable the All Overrides parameter, go to step 9.

ix Click on the Select button below the All Overrides parameter to choose an override counter to monitor for the significant change. The Select Override form opens.

x Select an override in the list and click on the OK button. The Select Override form closes and the override ID is displayed on the form.

9 Perform the following steps.

i Click on the Queue Counter Config tab button.

ii Click on the Add button. The CustomQueueConfig (Create) form opens.

iii Configure the ID parameter.

iv Configure the Counters parameter in the Ingress panel.

v Configure the Counters parameter in the Egress panel.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The Accounting Policy (Edit) form reappears.

10 Perform the following steps.

i Click on the Override Counter Config tab button.

ii Click on the Add button. The CustomOverrideConfig (Create) form opens.

iii Configure the ID parameter.

iv Configure the Counters parameter in the Ingress panel.

v Configure the Counters parameter in the Egress panel.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The Accounting Policy (Edit) form reappears.

11 Close the Radius Accounting Policy (Create) form. The Manage Radius Based Accounting Policies form reappears.

12 Click on the Search button to display the newly created policy or policies. Select a policy.

13 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

14 Close the Manage Radius Based Accounting Policies form.

55 — Residential subscriber policies

55.1 Residential subscriber policies overview

Residential subscriber management requires the use of policies and profiles that include the following:

- subscriber identification policies
- subscriber profiles
- SLA profiles

A subscriber identification policy is a component of residential subscriber management. It associates dynamic residential subscriber hosts with NE subscriber instances for the purpose of applying SLA profiles and subscriber profiles that act as templates for defining QoS, security and accounting attributes. There is no default subscriber identification policy in the 5620 SAM, but an operator can create a subscriber identification policy and designate it as the default.

A subscriber identification policy uses a parsing script to extract a subscriber identifier from a host DHCP packet. A common subscriber identifier indicates that hosts belong to the same subscriber and receive common HQoS and accounting treatment. A subscriber identification policy also assigns SLA profiles to hosts of a specific subscriber based on the type and class of service offering.

See chapter 64 for information about configuring and using subscriber identification policies, subscriber profiles, SLA profiles, and other residential subscriber management components.

56 — Remote network monitoring policies

56.1 Remote network monitoring policies overview

You can create remote network monitoring (RMON) policies that allow you to perform the following tasks.

- Use the policy framework to configure RMON that allows 5620 SAM users to deploy configurations to multiple devices.
- Map RMON events to information alarms in the 5620 SAM GUI.

Remote network monitoring allows you to monitor the behavior of functions that are not typically supported by the 5620 SAM. For example, events may be configured on generic NEs to monitor system temperature or CPU usage. The 5620 SAM can raise informational alarms for the exceeded thresholds. You can also configure custom values to supersede the hard-coded threshold values associated with a specific function on an NE.

The 5620 SAM maps RMON SNMP traps to alarms in the GUI.

Policy distribution and event mapping are supported for the following NE types:

- 7210 SAS-M24F
- 7210 SAS-M24F2XFP
- 7210 SAS-M24F2XFP [ETR]
- 7210 SAS-X24F2XFP
- 7250 SAS, Release 2.0 or later
- 7250 SAS-ES, Release 2.0 or later
- 7450 ESS
- 7710 SR
- 7750 SR

56.2 Remote network monitoring policies procedures

The following procedures describe how to configure and manage RMON policies.

Procedure 56-1 To configure a remote network monitoring policy

1 Choose Tools→Remote Network Monitoring (RMON) from the 5620 SAM main menu. The Remote Network Monitoring (RMON) form opens.

2 Perform one of the following:

a Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.

b Click on the Create button. The RMON (Create) form opens.

3 Configure the parameters:

- Displayed Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Create events to associate with the rising and falling thresholds on the remote NE.

i Click on the Events tab button.

ii Click on the Add button. The Event RMON (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Displayed Name
- Description
- Type
- Owner
- Community

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Event RMON (Create) form closes and the RMON (Create) form reappears.

vi Repeat steps 4ii to v to create another event, if required.

5 Configure the alarm information that is associated with the remote event.

i Click on the Alarms tab button.

ii Click on the Add button. The Alarm RMON form opens.

iii Configure the parameters:

- Auto-Assign ID
- ID
- Displayed Name
- Description
- Monitored Object OID
- Interval (seconds)
- Sample Type
- Start Up Alarm
- Owner

6 Configure the properties for the rising threshold crossing alarm.

i Click on the Select button in the Rising TCA Properties panel. The Select Rising Event - Alarm form opens.

ii Select the event and click on the OK button. The Select Rising Event - Alarm form closes and the Alarm RMON form reappears.

iii Configure the Rising Threshold parameter.

7 Configure the properties for the falling threshold crossing alarm.

i Click on the Select button in the Falling TCA Properties panel. The Select Falling Event - Alarm form opens.

ii Select the event and click on the OK button. The Select Falling Event - Alarm form closes and the Alarm RMON form reappears.

iii Configure the Falling Threshold parameter.

8 Click on the OK button. A dialog box appears.

9 Click on the OK button. The Alarm RMON form closes and the RMON (Create) form reappears.

10 Click on the Apply button.

11 Click on the Distribute button to manually distribute the policy locally to devices. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribution button is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

12 Close the RMON (Create) form. The Remote Network Monitoring (RMON) form reappears.

13 Click on the Search button to display the newly created policy or policies in the bottom panel of the form.

14 Close the Remote Network Monitoring (RMON) form.

57 — Size constraint policies

57.1 Size constraint policies overview

Size constraint policies regulate the number of historical records that the 5620 SAM database retains. The scheduling of tasks through the 5620 SAM can generate a great deal of archived result information if left unchecked. Size constraint policies control this volume by defining thresholds for various record classes. When the number of records for a specific class or group of classes reaches a threshold specified in the policy, the 5620 SAM deletes a specified number of the oldest objects that are associated with the class or group of classes.

57.2 Size constraint policies procedures

The following procedures describe how to configure and manage size constraint policies.

Procedure 57-1 To configure a size constraint policy

1 Choose Administration→Size Constraint from the 5620 SAM main menu. The Size Constraint Policy Manager form opens.

2 Perform one of the following:

- **a** Specify a filter to search for an existing policy. Select a policy in the filtered list and click on the Properties button.
- **b** Click on the Create button. The Size Constraint Policy (Create) form opens.

3 Configure the parameters:

- Auto-Assign ID
- Policy Id
- Description
- Threshold (# of objects)
- Objects To Be Deleted When Threshold Exceeded (# of objects)
- Apply Threshold To

4 Click on the Constrained Packages tab button.

5 Right-click on the Size Constraint Policy icon and choose Select Packages from the contextual menu. The Select Size Constrained Packages form opens with a list of packages displayed.

6 Choose the packages to include in the size constraint policy and click on the OK button. The packages appear in the navigation tree under Constrained Packages.

7 From a package icon below the Size Constraint Policy icon, choose Select Classes from the right-click contextual menu to include in the size constraint policy.

- **i** Right-click on a package and choose Select Classes from the contextual menu. The Select Size Constrained Classes form opens.
- **ii** Choose the required classes in the list and click on the OK button. The classes appear in the navigation tree under the associated package.

8 Repeat step 7 for each package icon in the list.

9 Click on the OK button. The Size Constraint Policy Manager form reappears with the new size constraint policy displayed in the list.

10 Close the Size Constraint Policy Manager form.

58 — NAT policies

58.1 NAT policies overview

A Network Address Translation, or NAT, policy, defines general NAT properties and associates a NAT address pool with an ISA-NAT group on the same NE. A NAT policy is associated with a subscriber profile for L2-aware NAT in an IES or VPRN service, or for large-scale NAT in a VPRN service.

See chapter 15 for information about ISA-NAT groups. See chapter 27 for information about configuring and deploying NAT in a network. See Procedure 58-1 for NAT policy configuration information. See chapter 70 for information about configuring and using NAT in an IES. See chapter 71 for information about configuring and using NAT in a VPRN service.

58.2 NAT policies procedures

The following procedures describe how to configure and manage NAT policies.

Procedure 58-1 To create a NAT policy

Perform this procedure to create a NAT policy for a large-scale or L2-aware NAT implementation.

1 Choose Policies→ISA Policies→NAT Policy from the 5620 SAM main menu. The NAT Policy Manager form opens.

2 Click on the Create button. The NAT Policy (Create) form opens.

3 Configure the following parameters:

- Displayed Name
- Description

4 Click on the Select button in the NAT Pool panel to choose a NAT pool. The Select NAT Pool form opens.

5 Choose a NAT pool in the list and click on the OK button. The Select NAT Pool form closes and the NAT pool name is displayed on the NAT Policy (Create) form.

6 Configure the remaining parameters:

- Filtering
- Port Reservation Count
- High Watermark
- Low Watermark
- Session Limit
- Reservation Count
- Session High Watermark
- Session Low Watermark
- Priority Session Forwarding Class Set
- TCP Established (sec)
- TCP Transitory (sec)
- TCP Syn (sec)
- TCP Time Wait (sec)
- ICMP Query (sec)
- UDP (sec)
- UDP Initial (sec)
- UDP DNS (sec)

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The NAT Policy (Create) form closes.

9 Close the NAT Policy Manager form.

59 — Format and range policies

59.1 Format and range policies overview

The 5620 SAM supports format and range policies. Format policies manage how services, LSPs, L2 and L3 access interfaces are named and described. Range policies manage the ID numbers that are assigned to services, LSPs, L2 and L3 access interfaces. For example, you can configure a range policy to specify a range of 200 and 499 for all IDs for a service. You can configure a format policy to specify that service names do not exceed 10 characters. The object creation form indicates when a range or format policy is in effect for an object.

Format and range policies are not distributed to NEs. The policies are configured when services, LSPs, L2 and L3 access interfaces are created from the 5620 SAM GUI. You cannot configure format and range policies when the services, LSPs, L2 and L3 access interfaces are created using templates. However, the 5620 SAM allows an operator to use pre-configured examples of LSPs and services that have format and range policies applied to them. The examples can be used to create a template. For more information about creating templates from a pre-configured example, see the *5620 SAM Scripts and Templates Developer Guide*.

Table 59-1 lists the objects and associated parameters that can be managed using format and range policies.

Table 59-1 Format and Range policy objects and associated parameters

Object name	Format policy parameter	Range policy parameter
B-VPLS Service Site	Description, Name	—
Bypass-only LSP	Description, Name	ID
Customer	—	ID
Dynamic LSP	Description, Name	ID
I-VPLS Service Site	Description, Name	—
IES Group Interface	Description, Name	Interface ID
IES L3 Access Interface	Description, Name	Interface ID, Outer Encapsulation Value
IES Service	Description, Service Name	Service ID
IES Service Access Point	Description, Name	Outer Encapsulation Value
IES Service Site	Description, Name	—
IES Subscriber Interface	Description, Name	Interface ID
IP Mirror Interface	—	Interface ID
MVPLS B-L2 Access Interface	Description	Outer Encapsulation Value
MVPLS I-L2 Access Interface	Description	Outer Encapsulation Value
MVPLS L2 Access Interface	Description	Outer Encapsulation Value
MVPLS Service	Description, Service Name	Service ID
Mirror L2 Access Interface	—	Outer Encapsulation Value
MVPLS Service B-Site	Description, Name	—
MVPLS Service I-Site	Description, Name	—

(1 of 2)

Object name	Format policy parameter	Range policy parameter
MVPLS Service Site	Description, Name	—
Mirror Service	Description, Service Name	Service ID
Mirror Service Site	Description, Name	—
Redundant Interface	—	Interface ID
Spoke SDP Binding	—	VC ID
Static LSP	Description, Name	ID
Tunnel	Description, Name	ID
VLAN L2 Access Interface	Description	—
VLAN Service	Description, Service Name	Service ID
VLAN Service Access Point	Description, Name	—
VLAN Service Site	Description, Name	—
VLL Apipe Service	Description, Service Name	Service ID
VLL Apipe Service Site	Description, Name	—
VLL Cpipe Service	Description, Service Name	Service ID
VLL Cpipe Site	Description, Name	—
VLL Epipe Service	Description, Service Name	Service ID
VLL Epipe Service Site	Description, Name	—
VLL Fpipe Service	Description, Service Name	Service ID
VLL Fpipe Service Site	Description, Name	—
VLL Ipipe L2 Access Interface	Description	Outer Encapsulation Value
VLL Ipipe Service	Description	Service ID
VLL Ipipe Site	Description, Name	—
VLL L2 Access Interface	Description	Outer Encapsulation Value
VPLS B-L2 Access Interface	Description	Outer Encapsulation Value
VPLS I-L2 Access Interface	Description	Outer Encapsulation Value
VPLS L2 Access Interface	Description	Outer Encapsulation Value
VPLS L2 Management Interface	—	Interface ID
VPLS Service	Description, Service Name	Service ID
VPLS Service Site	Description, Name	—
VPRN Group Interface	Description, Name	Interface ID
VPRN L3 Access Interface	Description, Name	Interface ID, Outer Encapsulation Value
VPRN Service	Description, Service Name	Service ID
VPRN Service Access Point	Description, Name	Outer Encapsulation Value
VPRN Service Site	Description, Name	—
VPRN Subscriber Interface	Description, Name	Interface ID

(2 of 2)

Table 59-2 lists the policies that support format and range policies.

Table 59-2 Format and Range policy objects and associated parameters for policies

Policy	Format policy	Range policy
Access Ingress QoS	Description, Displayed Name	ID
Access Egress QoS	Description, Displayed Name	ID
ATM QoS policy	Description, Displayed Name	ID
Egress Queue Group template	Description, Displayed Name	—
7705 SAR Fabric Profile	Description, Displayed Name	ID
Policer Control policy	Description, Displayed Name	—
HSMDA Pool policy	Description, Displayed Name	—
HSMDA Scheduler policy	Description, Displayed Name	—
HSMDA WRED Slope policy	Description, Displayed Name	—
Ingress Queue Group template	Description, Displayed Name	—
MCFR Egress QoS Profile	Description	Profile ID
MCFR Ingress QoS Profile	Description	Profile ID
MLPPP Egress QoS Profile	Description	Profile ID
MLPPP Ingress QoS Profile	Description	Profile ID
Named Buffer Pool policy	Description, Name	—
Network policy	Description, Displayed Name	ID
Network Queue	Description, Name	—
Port Scheduler policy	Description, Displayed Name	—
Sap Access Ingress for 7210	Description, Displayed Name	ID
Network Policy for 7210	Description, Displayed Name	NW Mgr ID, Policy Id
Network Queue for 7210	Description, Name	—
Port Access Egress for 7210	Description, Displayed Name	ID
Port Scheduler for 7210	Description, Displayed Name	—
Slope Policy for 7210	Description, Displayed Name	—
Scheduler policy	Description, Displayed Name	—
WRED Slope policy	Description, Displayed Name	—
ACL IP filter	Description, Displayed Name	Filter ID
ACL IPv6 filter	Description, Displayed Name	Filter ID
ACL MAC filter	Description, Displayed Name	Filter ID
ANCP policy	Displayed Name	—
Host Tracking policy	Description, Displayed Name	—
MSAP policy	Description, Displayed Name	—
PPPoE policy	Description, Displayed Name	—
SLA Profile	Description, Displayed Name	—
Subscriber Explicit Map Entry	Description, Displayed Name	—

(1 of 2)

Policy	Format policy	Range policy
Subscriber Identification policy	Description, Displayed Name	—
Subscriber Profile	Description, Displayed Name	—
AA Application filter	—	Entry ID
Egress Multicast Group	Description, Displayed Name	—
Multicast Package	Description, Displayed Name	ID
Multicast CAC	Description, Name	—
Multicast PathMgmt BW policy	Description, Name	—
Multicast PathMgmt Info policy	Description, Name	—
AS Path	Description, AS Path Name	—
Community	Description, Community Name	—
Damping	Damping Name	—
Prefix List	Description, Prefix List Name	—
Statement	Description, Statement Name	—
MPLS Adminstrative Groups	Displayed Name	Value
Static Configuration for SRLGs	Displayed Name	—
Shared Risk Link Group Static Config	Displayed Name	Value
Accounting policy	Description, Displayed Name	ID
File policy	Description, Displayed Name	ID
Maintenance Domain	Description, Name	MD Mgr ID
Network Address Translation policy	Description, Displayed Name	—
PAE 802_1x policy	Description, Displayed Name	—
RADIUS Based Accounting	Description, Displayed Name	—
RMON	Description, Displayed Name	—
Time of Day Suite	Description, Name	—
Time Range	Description, Name	—
VRRP policy	Description, Displayed Name	ID, Service ID

(2 of 2)

59.2 Format and range policies procedures

The following procedures describe how to configure and manage format and range policies.

Procedure 59-1 To create or configure a format policy

Use this policy to specify the number and format of characters that can be used for text fields such as service names and descriptions.

1 Choose Administration→Format and Range from the 5620 SAM main menu. The Format and Range Polices form opens.

2 Click on Format/Range (Property Values). A navigation tree is displayed.

3 Click on Format Policy (Property Rules).

4 Perform one of the following:

a Click on the Search button to specify a filter to search for and modify a policy. A list of format policies is displayed. Go to step 5.

b Click on the Create button. The Format Policy (Create) form opens with the General tab displayed. Go to step 6.

5 Select a format policy in the list. A Format Policy (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- Priority
- Administrative State

7 Click on the Select button beside the Object Type parameter. The Select Property - Format/Range Policy form opens.

8 Select an object for which you need to apply the name format policy.

9 Click on the OK button. The Select Property - Format/Range Policy form closes and the Format Policy (Create) or (Edit) form is updated with the object type.

10 Click on the Select button beside the Property Name parameter. The Select Property - Format/Range Policy form opens with a list of configurable properties for the object. The content of the list depends on the object that you specified in step 8.

11 Choose the property for which you need to apply the format policy.

12 Click on the OK button. The Select Property - Format/Range Policy form closes and Format Policy form is updated with property name.

13 Click on the Users tab button.

Note — Only users and user groups that are assigned to this policy are affected by the policy. You can apply one or more format policies to a user or user group. See procedures 8-13 and 8-14 for more information about creating users and user groups.

14 Click on the Add button. The Select User form opens with a list of users.

15 Select one or more users in the list and click on the OK button. The Format Policy form is refreshed with the selected users.

16 Click on the User Groups tab button.

17 Click on the Add button. The Select Group form opens with a list of user groups.

18 Choose one or more user groups in the list and click on the OK button. The Format Policy (Create) or (Edit) form is refreshed with the selected user groups.

19 Click on the Text Block Formats tab button to further define the format of the text. For example, an operator can classify a group of services with a similar name. The operator can also create a tool tip text to describe the purpose of the parameter.

20 Click on the Move Up or Move Down buttons to change the sequence of the text blocks in the text string.

21 Click on the Create button and perform one of the following:

a Choose Auto-Filled Parameter. The Auto-Filled Parameter (Create) form opens.

b Choose Masked Text Parameter. The Formatted Text (Create) form opens. Go to step 24.

c Choose Text Parameter. The Text (Create) form opens. Go to step 26.

22 Configure the parameters:

- Source Object Name
- Source Property Name
- Copy Text From Position
- Through To Position
- Displayed Text (Placeholder)
- Tooltip Text

23 Go to step 27.

24 Configure the parameters:

- Mask
- Tooltip Text

25 Go to step 27.

26 Configure the parameters:

- Default Value
- Read Only
- Min. Length
- Max. Length
- Tooltip Text

Note — The Min. Length and Max. Length parameters are not configurable when the Read Only parameter is enabled.

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The Format Policy form reappears.

29 Click on the OK button. The Format Policy form closes.

30 Close the Format and Range Policies form.

Note — After a format policy is applied to a service, a combo box is displayed beside the object field during object creation, to indicate that a format policy is in effect. When there is only one matching policy, the combo box is dimmed. When there are multiple matching policies, the combo box is used to choose a policy. The sequence of the policies in the combo box is based on the value of the Priority parameter.

Procedure 59-2 To create or configure a range policy

Use this policy to specify the ID range for services, LSPs, L2 and L3 access interfaces.

1 Choose Administration→Format and Range from the 5620 SAM main menu. The Format and Range Polices form opens.

2 Click on Format/Range (Property Values). A navigation tree is displayed.

3 Choose Range Policy (Property Rules).

4 Perform one of the following:

a Click on the Search button to specify a filter to search for and modify a policy. A list of range policies is displayed. Go to step 5.

b Click on the Create button. The Range Policy (Create) form opens with the General tab displayed. Go to step 6.

5 Select a range policy in the list. A Range Policy (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- Priority
- Administrative State
- Minimum
- Maximum
- Auto Assignment Enabled
- Auto Assign By Default

7 Click on the Select button beside the Object Type parameter. The Select Property - Format/Range Policy form opens.

8 Select an object for which you need to apply the range policy.

9 Click on the OK button. The Select Property - Format/Range Policy form closes and the Range Policy (Create) form is updated with the object type.

10 Click on the Select button beside the Property Name parameter. The Select Property - Format/Range Policy form opens.

11 Choose the property for which you need to apply the range policy.

12 Click on the OK button. The Select Property - Format/Range Policy form closes and Range Policy (Create) form is updated with the property name.

13 Click on the Users tab button.

Note — Only users and user groups that are assigned to this policy are affected by the policy. You can apply one or more range policies to a user or user group. See procedures 8-13 and 8-14 for more information about creating users and user groups.

14 Click on the Add button. The Select User form opens with a list of users.

15 Choose one or more users in the list and click on the OK button. The Range Policy form is refreshed with the users.

16 Click on the User Groups tab button.

17 Click on the Add button. The Select Group form opens with a list of user groups.

18 Choose one or more user groups in the list and click on the OK button. The Range Policy form is refreshed with the user groups.

19 Click on the OK button. The Range Policy form closes and the Format and Range Policies form reappears.

20 Close the Format and Range form.

Note — After a range policy is applied to a service, a combo box is displayed beside the object field during object creation, to indicate that a range policy is in effect. When there is only one matching policy, the combo box is dimmed. When there are multiple matching policies, the combo box is used to choose a policy. The sequence of the policies in the combo box is based on the value of the Priority parameter.

Service management

60 — Service management and QoS

60.1 Service management and QoS overview

The 5620 SAM supports the configuration of the following network services:

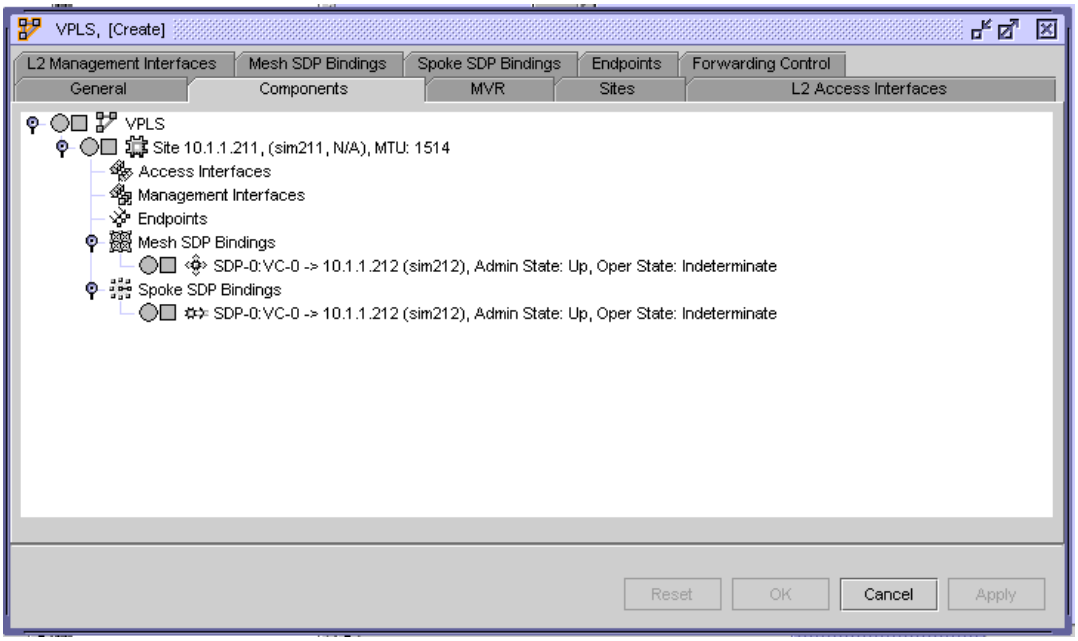
- VLL service
- VPLS / MVPLS / HVPLS
- IES
- VPRN service
- VLAN service
- composite service
- mirror service

A 5620 SAM operator can create, configure and delete services on sites and routers that are within their span of control.

The benefits of the 5620 SAM service model include:

- end-to-end service management on the 5620 SAM using configuration forms and a navigation tree. An example of the navigation tree is shown in Figure 60-1.
- the linking of services to create composite services that support complex customer applications
- template-based creation of policies that specify the classification, policing, shaping, time of day restrictions, and marking of traffic handled by the managed devices. Policies can be used by multiple services.
- traffic management capabilities to customize the delivery of different services according to the most stringent SLAs
- closely integrated fault-management capabilities
- the capability to make changes to a single service component (such as a service, service site, tunnel, circuit [service-tunnel binding], or interface) rather than multiple ports on multiple devices
- tunnel configurations and transport that are independent of the services that they carry

Figure 60-1 Navigation tree - service management form



For distributed VLL service and VPLS, devices are deployed at the provider edge. Customer traffic is fed into the service using access interfaces. Traffic is transported across IP/MPLS-provider core networks in unidirectional service tunnels that are created using GRE or MPLS LSPs. Many services can use the same tunnel. Figure 60-2 shows a sample distributed VLL service.

You can also configure a local VLL service or a local VPLS. A local VLL service consists of two access interfaces on the same node. A local VPLS consists of multiple access interfaces on the same node.

Figure 60-2 Sample distributed VLL service

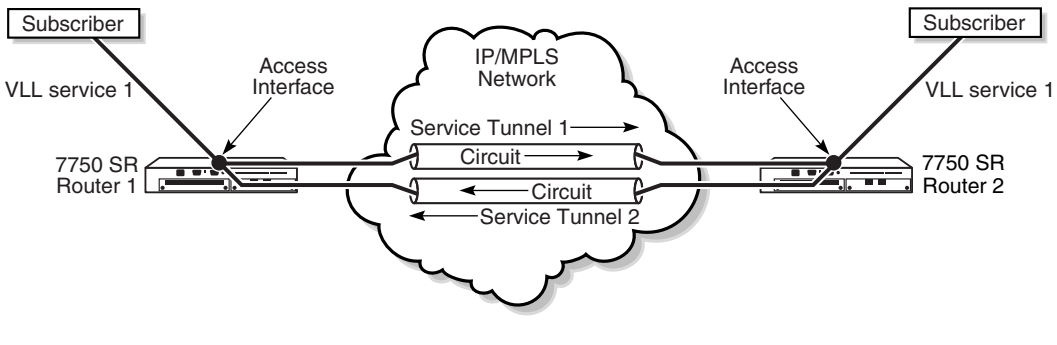
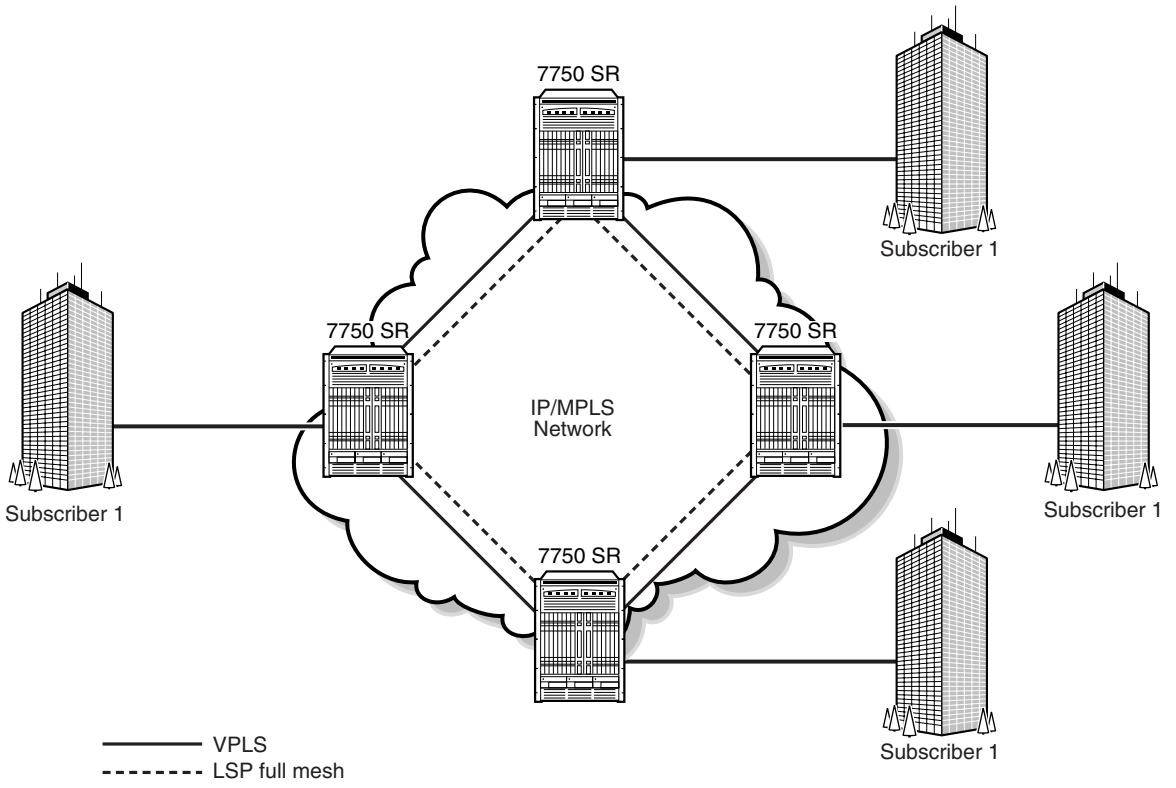


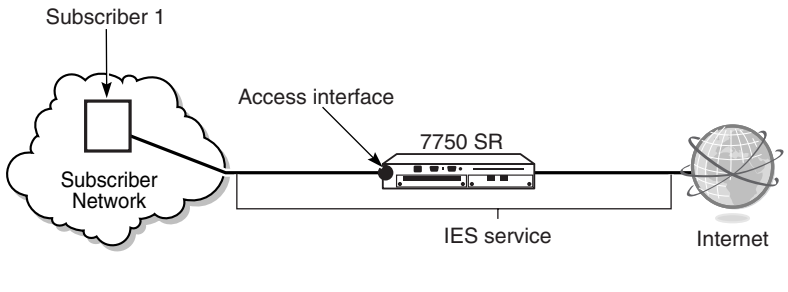
Figure 60-3 shows a sample distributed VPLS.

Figure 60-3 Sample distributed VPLS



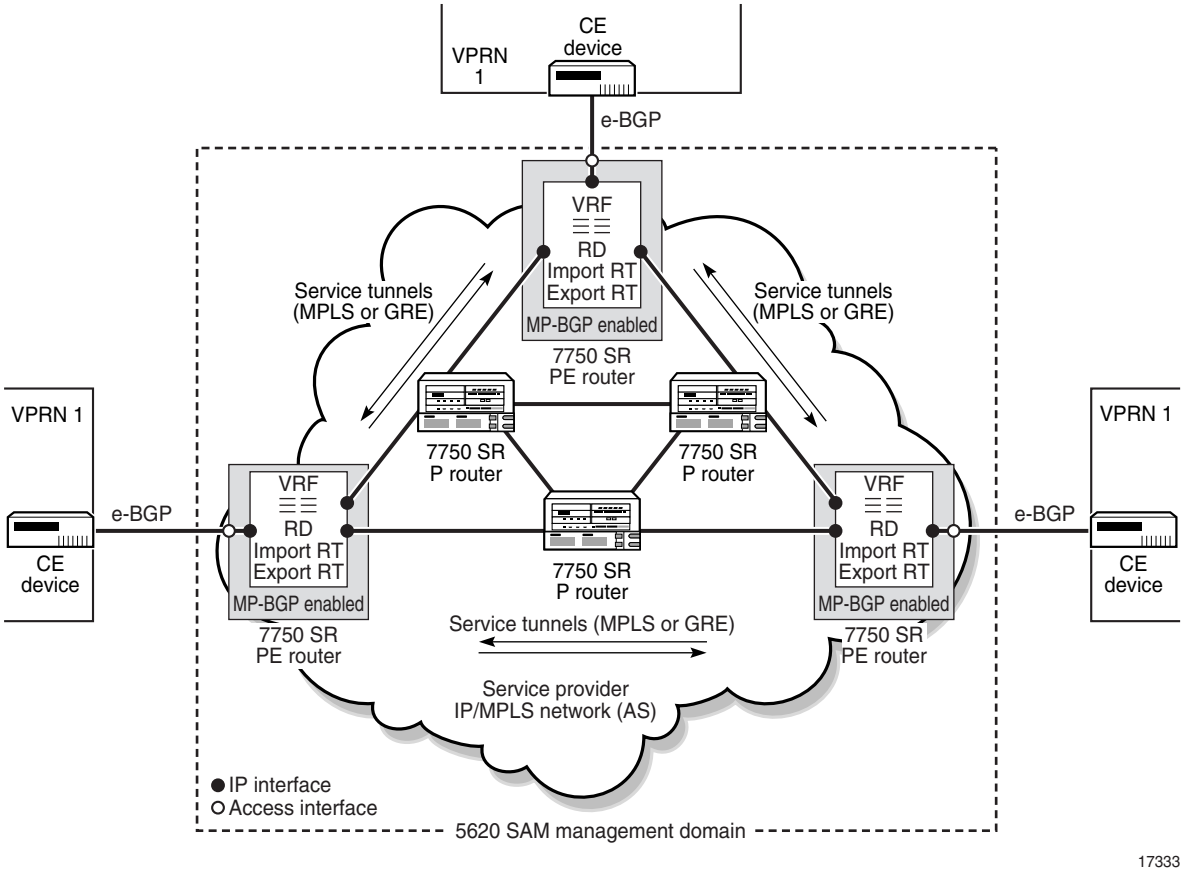
For IES, the managed devices are deployed at the provider edge and customer traffic enters the service using access interfaces. IES is a routed connectivity service where the customer communicates with an IP router interface to send and receive Internet traffic. Figure 60-4 shows a sample IES.

Figure 60-4 Sample IES



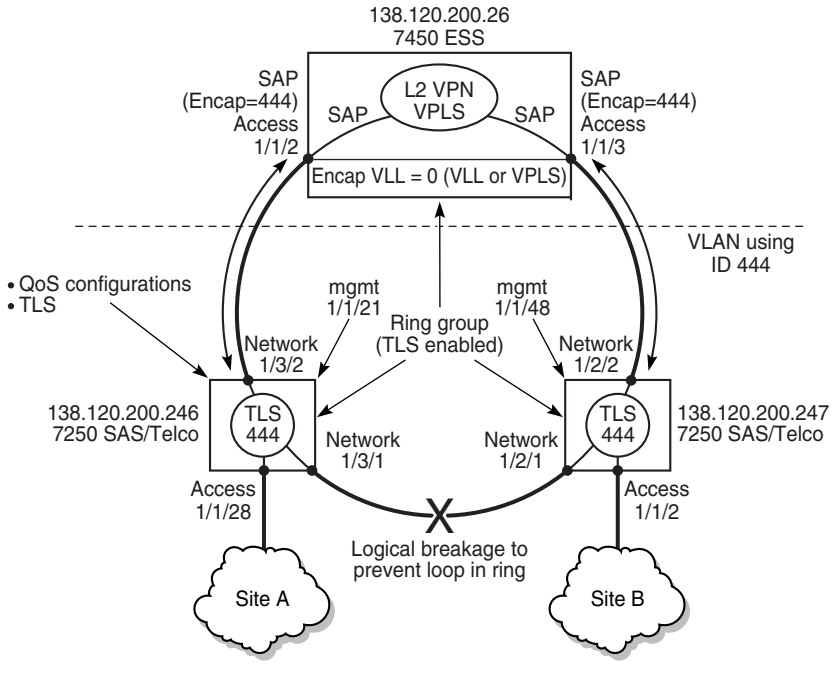
For VPRN services, the managed devices can be deployed as PE or provider core routers. Data and distribution of routing information are forwarded across an IP/MPLS service provider core network. Figure 60-5 shows a sample VPRN service.

Figure 60-5 Sample VPRN service



VLAN ring groups are used to send traffic across an Ethernet ring using copper or fiber optic connections from the source traffic device, for example, a 7450 ESS, to all devices in the ring. STP configuration on 7250 SAS and Telco devices ensures that there is a constant stream of traffic in either direction. Any breaks in the physical links between devices are rerouted. Figure 60-6 shows a sample VLAN for L2 VPNs.

Figure 60-6 Sample VLAN configuration for L2 VPNs



A composite service allows the interconnection of different service types to form a service delivery network that is tailored to a specific application. For example, VPRN, VPLS, and VLAN services can be joined to create a routed multicast TV distribution mechanism that spans a wide geographical area.

A mirror service is a unidirectional service function that duplicates a specified traffic stream and sends the duplicate stream to a monitoring device for troubleshooting or surveillance purposes. With pseudo-wire redundancy support, an ICB can be enabled in a mirror service spoke and a remote source, which can provide bidirectional service that enables support for active and standby PE redundancy.

QoS provides the ability to rate limit across multiple queues from one or more access interfaces for a customer, and to differentiate service levels for different types of traffic. For higher priority traffic such as VoIP or video, you can specify reserved bandwidth. Lower priority applications, such as data traffic, may not have reserved bandwidth but can burst to use all the available bandwidth.

The main elements of QoS are:

- QoS markings

  Customer traffic may be marked with QoS markings, such as DSCP, EXP, and dot1p, that are mapped to forwarding classes.

  All forwarding classes support profile marking of packets as in-profile or out-of-profile. In-profile packets have a high enqueuing priority. Out-of-profile packets have a low enqueuing priority. Profile marking of packets can occur at two points: when packets are classified into forwarding classes at access ingress and when packets are classified at service egress. Profile marking is only done on the internal header and not in an actual encapsulation.

- forwarding classes

  Provide network elements with a method to weigh the relative importance of packets, only in relation to other forwarding classes. A forwarding class is also referred to as a Class of Service.
- queues

  Location for buffering packets that are to be forwarded before they are scheduled.
- schedulers

  Hardware scheduling (or single-tier scheduling) exists by default on a device and consists of a high-priority and a low-priority scheduler.

  Scheduler policies (or multi-tier scheduling) provide a more complex, hierarchical structure of virtual schedulers that override the default hardware behavior for more flexible scheduling capabilities.
- slope policies

  Define the WRED slope characteristics of hardware buffer space that is used by the ingress and egress queues

See chapter 43 for more information about policies on the 5620 SAM. See the *7750 SR OS Services Guide* for more detailed information about QoS.

Access interfaces

Each customer service is configured with at least one access interface point called a SAP. The access interface identifies the point of customer interface for a service on the managed device.

A Layer 2 or Layer 3 access interface is uniquely identified using these parameters:

- physical Ethernet port or POS port and channel
- encapsulation type (if applicable)
- encapsulation id (if applicable)

Depending on the encapsulation type, a physical port or channel can have more than one access interface associated with it. Using encapsulation or a SONET/SDH channel, devices can support multiple services for a customer or for multiple customers.

Access interfaces can only be created on ports or channels that are designated as access in the physical port configuration. Access interfaces cannot be created on ports designated as core-facing network ports because these ports have a different set of features enabled in software.

Access interfaces can participate in policies. Time of day suites can also be associated with access interfaces to apply a set of time-based policies, filters, and schedulers. Configuration of access interfaces can be performed during service configuration or modification. When you configure an access interface, consider the following:

- An access interface is owned by and associated with the service in which it is created.
- An access interface is a local entity and is locally unique to a specific device. The same access interface ID value can be used on another device.
- There are no default access interfaces. All access interfaces must be created.

- The default administrative state for an access interface at creation time is administratively enabled.
- If a port or channel is shut down (administratively or operationally), access interfaces on that port/channel are operationally out of service.

Automatic SDP (service tunnel) binding for services

You configure automatic service tunnel (SDP) binding for services when you configure a service using configuration forms or templates.

The 5620 SAM defines its own internal rules on how automatic mesh SDP bindings are performed.

1 The 5620 SAM tries to find the least-used SDP (service tunnel) with the lowest load factor (the lower the number of bindings, the lower the load factor) from the source to destination node when the service tunnel meets the following conditions:
   - the service tunnel operational state is up
   - the operational MTU is greater than or equal to the MTU value of the service site
   - T-LDP is set for SDP bindings of VPLS, IES, or VLL services
   - the selected transport method, either GRE, LDP, or RSVP
2 When no service tunnel operational state is up, 5620 SAM tries to find the least-used service tunnel with the lowest load factor in an operationally down state.
3 For mirror services, binding are created from the source sites to the destination sites.
4 When a service tunnel cannot be found for a service site, a change in the site leads to another search. For example, if the service MTU is 1500 and the highest path MTU in all SDPs from that site is 1472, no SDP binding can be successful. If the service MTU is lowered to 1472 or less, a successful SDP binding results.
5 When a service tunnel is not found, and the transport method selected is GRE, 5620 SAM attempts to create a GRE service tunnel with a path MTU equal to the service site service MTU with T-LDP signaling turned on.

See "MTU size and port configuration" in section 15.17 for more information on MTU size considerations.

Automatic PBB tunnel binding

This feature is applicable only to VLL Epipes and I-VPLS services using a PBB tunnel.

Note — This feature has limited availability. Contact your Alcatel-Lucent technical support representative for more information about the availability of this feature.

The configuration of the service CAC functionality allows you to manage bandwidth at the service level and at the link level, which in turn enables the 5620 SAM to automatically select the best tunnel based on the number of active links and on the amount of available bandwidth on the service. For 5620 SAM release 8.0 R5 and later, the shortest available path will also be considered by the system when allocating bandwidth.

Although the 5620 SAM can select tunnels automatically—see Automatic SDP (service tunnel) binding for services—if service CAC is not configured, bandwidth will not be considered by the 5620 SAM when selecting the tunnel.

Bandwidth availability for the tunnel is calculated at the service admission request time and is based on the links currently used by the tunnel forwarding path. The booking of reserved bandwidth by the service is done directly on the link and directly on the tunnel, for a bandwidth-reserved tunnel.

The link monitors the bandwidth used by all of the services using that link. Since the bandwidth reserved on each tunnel that is used by a service can be different, the link monitors bandwidth usage through the tunnels rather than through a service.

You can perform a system-wide audit to ensure that the bandwidth on each link is properly calculated. The audit visits all tunnels in the network and adjusts the available bandwidth in all links currently being used by the forwarding tunnel path. The adjustments are made based on total bandwidth requests per CoS for all EVPLs currently using the tunnels.

You can perform this audit by clicking on the CAC Audit button on the Manage Services form. The audit also occurs automatically on system startup and when service CAC is switched from disabled to enabled. See chapter 5 for information about enabling and disabling service CAC.

Lightweight SAPs

SAPs that are associated with residential split horizon groups on VPLS sites are called lightweight SAPs. An RSHG uses dual-pass queue optimization and does not support downstream broadcast or multicast traffic. Lightweight SAPs have fewer internal configuration settings than regular SAPs. Therefore, you can create more lightweight SAPs on a node. The SAP Lightweight property is automatically set at creation time, when the SAP is associated with an RSHG, and cannot be modified later.

Users can:

- assign SAPs to residential split horizon groups
- list lightweight SAPs using the Lightweight filter property

Note — To get the most recent state of a lightweight SAP, it is recommended that users perform a resynchronization by clicking on the Resync button in the SAP configuration window.

60.2 5620 SAM and the triple play service delivery architecture

The TPSDA is based on three major components, as shown in Figure 60-7:

- broadband service aggregator
- broadband service router
- service and policy activation

Figure 60-7 TPSDA components

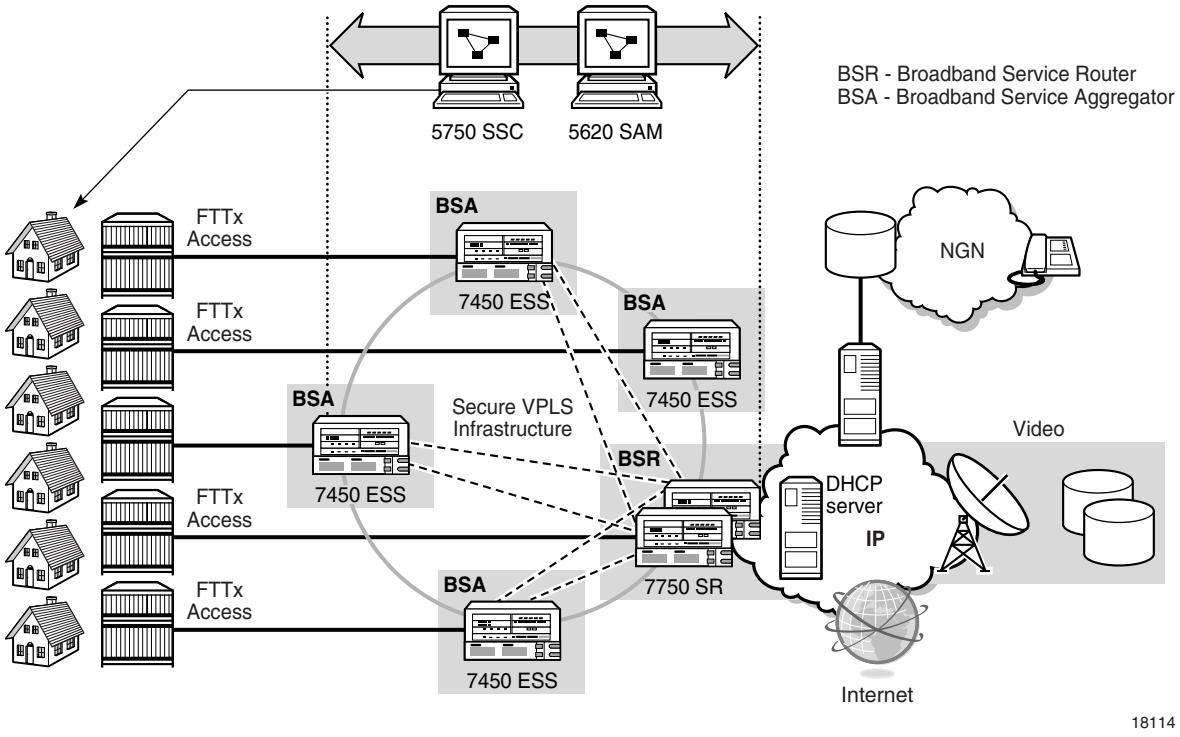


Table 60-1 lists the Alcatel-Lucent TPSDA product components.

Table 60-1 Product components of the TPSDA

Product	Role	Notes
5620 SAM	Provides network, service, and policy management across the TPSDA architecture, including a unified interface for element management and simple service activation and monitoring.	Create and configure QoS, filtering, and accounting templates that can then be reapplied to multiple L2 and L3 interfaces, and configure managed BSA and BSR devices to allow DHCP relay.

(1 of 2)

Product	Role	Notes
5750 SSC	Provides centralized control of host access services for triple play service delivery, for example, as a DHCP server to identify hosts and trigger service configuration or on-demand service profile changes made by the customer. Interworks with the 5620 SAM to enable per-customer QoS and bandwidth changes in the network.	Provide a customer self-service web portal and manage information that determines the levels of service allowed for an end user.
7750 SR	BSR	Support per-service and per-content type differentiation of QoS levels and supports distribution of multicast traffic.
7450 ESS	BSA	Aggregate traffic from DSLAMs and other FTTx access devices that are connected to end-user residential gateways.

(2 of 2)

DSLAMs or other access nodes are connected to Ethernet access ports on the broadband service aggregator. Typically, a single VLAN for each customer is set up between the access node and the BSA. This a configuration enables the application of consistent per-customer policies, such as QoS, filtering, and accounting, to be applied on the BSA.

Scaling of traffic and services is done by dividing L2 and L3 functions between the BSA and the BSR. The BSA aggregates traffic over Gigabit Ethernet ports and performs per-customer service queueing, scheduling, accounting and filtering, as described later in this chapter. The BSR terminates L2 access and routes over IP/MPLS with support for all protocols, including multicasting. Time of day QoS policies can be applied using 5620 SAM policy management.

Interconnectivity between BSAs and BSRs is provided by VPLS. VPLS instances can be automatically established using hub-and-spoke or ring topologies. Both can be configured and sites added to the VPLS using the 5620 SAM. Regardless of the fiber plant layout, VPLS enables a full mesh between all sites that are receiving and distributing customer traffic in the TPSDA, ensuring efficient transport and protection from node or fiber failures.

VPLS also provides mechanisms for traffic security, including residential split horizon groups in which direct user bridging is prohibited; ARP and broadcast suppression; DHCP-populated MAC and IP address filtering to prevent denial or service and theft of service using DHCP snooping, and RADIUS or TACACS+ authentication.

Service differentiation and QoS

This TPSDA approach provides a model based on call admission for video and VoIP, with the need to guarantee delay, jitter, and loss characteristics after the service connection is accepted. The architecture also meets the different QoS needs of HSI, namely per-user bandwidth controls, including shaping and policing functions that have little or no value for video and VoIP service delivery.

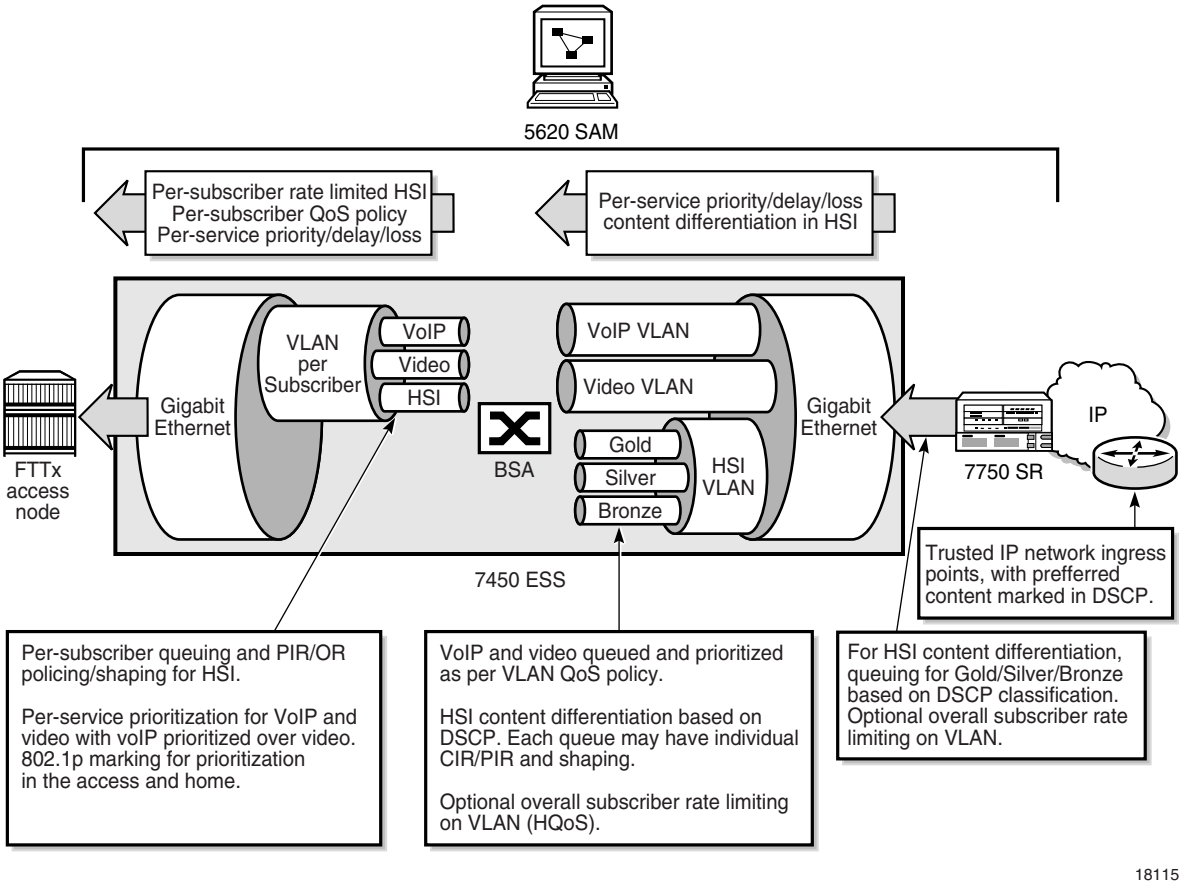
In conjunction with the architecture's support for content differentiation, this approach enables differentiated service pricing within high-priority data packages, also known as HSI. The distribution of QoS policy and enforcement across BSA and BSR allows the service provider to implement meaningful per-user service level controls. Sophisticated and granular QoS in the BSA allows the service provider to deliver truly differentiated IP services differentiation based on the user as well as on the content.

In the BSR to BSA downstream direction, IP services rely on IP layer classification of traffic from the network to queue traffic appropriately towards the BSA. Under extreme loading (only expected to occur under network fault conditions), lower priority data services and/or HSI traffic are compromised to protect video and voice traffic. Classification of HSI traffic based on source network address or IEEE 802.1p marking allows the QoS information to be propagated to upstream or downstream devices.

The BSR performs service distribution routing based on guarantees required to deliver the service and associated content, rather than on individual end users. The BSR only needs to classify content based on its forwarding class for a specific BSA to ensure that traffic for each service receives the appropriate treatment towards the BSA.

Figure 60-8 shows the downstream QoS configurations.

Figure 60-8 TPSDA downstream QoS configurations

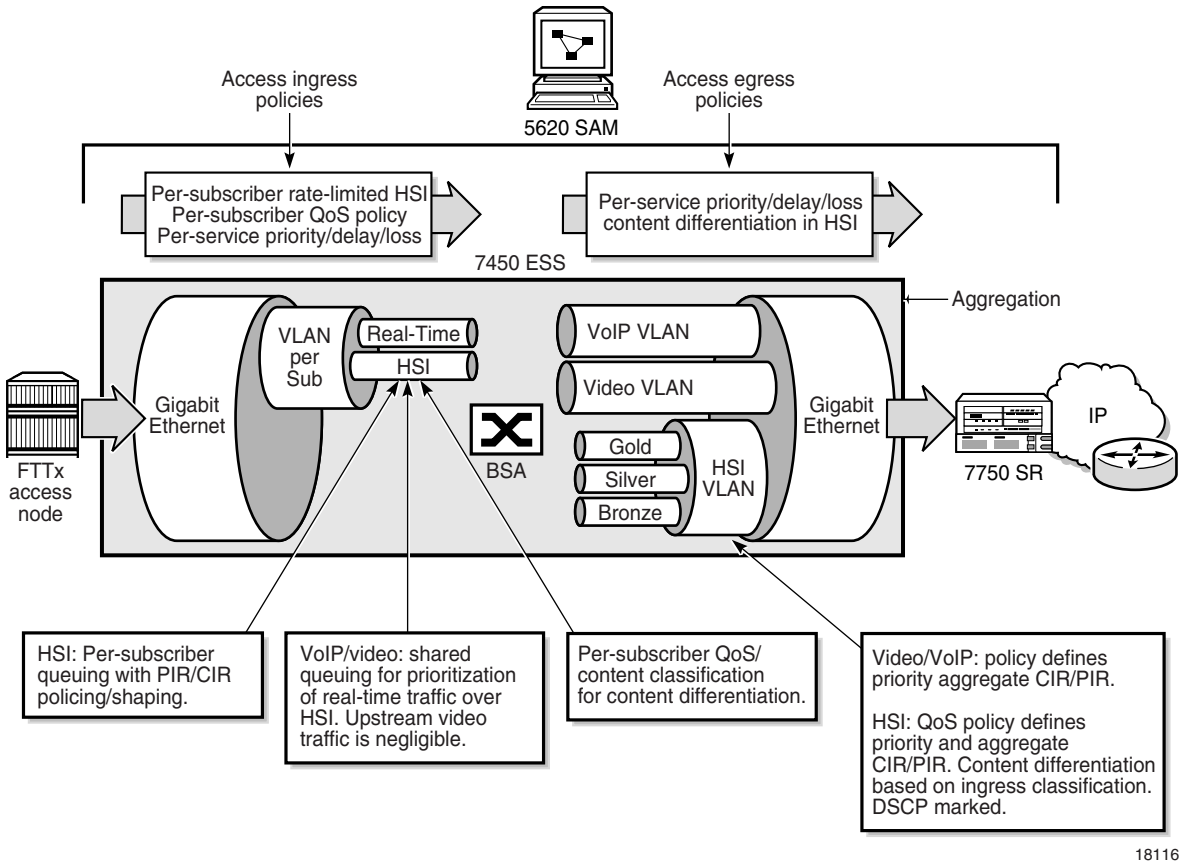


In the BSA-to-BSR upstream direction, traffic levels are substantially lower. Class-based queuing is used on the BSA network interface to ensure that video traffic is forwarded with minimal delay and that preferred data or HSI high-priority data traffic services receive better treatment than for best-effort Internet traffic. The IP edge device (BSR) therefore does not need to enforce per-user policies for hundreds of thousands of users. This function is distributed to the BSAs, and the per-user policies can be implemented on the interfaces directly facing the access nodes.

The BSA is capable of scheduling and queuing functions on a per-service, per-user basis, in addition to performing wire-speed packet classification and filtering based on both L2 and L3 interfaces. In addition to per-service rate limiting for Internet services, service traffic for each user can be rate-limited as an aggregate using a bundled service policy created using the 5620 SAM. These functions allow different users to receive different service levels independently and simultaneously.

Figure 60-9 shows the upstream QoS configurations.

Figure 60-9 TPSDA upstream QoS configurations



When a residential host device, such as a residential gateway or a set-top box in the customer's home, starts up, it requests network information, including the required IP address from a DHCP server. Figure 60-10 shows IP address assignment. See chapter 10 for information about using the 5750 SSC as a DHCP server. See Table 60-2 for more information about DHCP configuration options in the TPSDA.

Figure 60-10 DHCP IP address assignment in the TPSDA

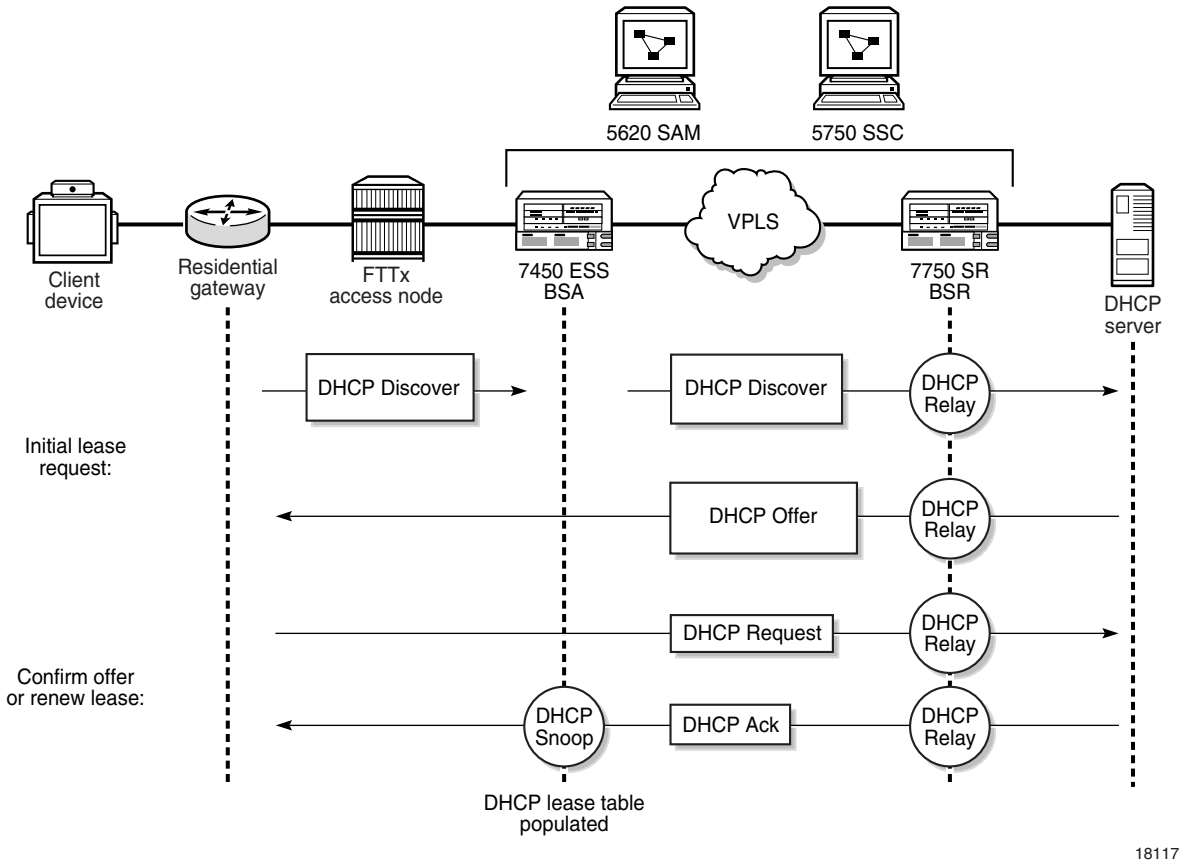


Table 60-2 lists the TPSDA features that you can configure using the 5620 SAM.

Table 60-2 TPSDA features

Feature and use	Notes	Reference
Split horizon groups		
For the TPSDA, there can be no user-to-user communication in the BSA; instead, all communication is done through the BSR. This residential bridging is done using split horizon groups, which ensures that traffic from different SAPs in the same service are not forwarded to other SAPs or spokes.	Traffic arriving on a spoke service tunnel or SAP within the split horizon group is not copied to other SAPs or spoke service tunnels. Traffic is copied to SAPs and spokes in other split horizon groups existing within the same service, such as a VPLS.	See chapter 68 for configuration of split horizon groups.
DHCP		

(1 of 3)

Feature and use	Notes	Reference
For the TPSDA, host devices, such as a residential gateway, SIP phone, or set-top box, use DHCP to obtain IP address and other network configuration information. The client device sends a DHCP discover message to request an IP address. The sequence of events is shown in Figure 60-10.	Information added to the DHCP discover requests may include information added by the FTTx access node or the BSA, for example, the shelf, slot, port, VPI, VCI, or other identifier of the host. You can use the 5620 SAM to configure DHCP relay on the first IP interface in the upstream direction. The BSA or BSR relays the message to a DHCP server. The gateway (residential gateway) IP address indicates to the DHCP server the subnet an IP address should be allocated to for the host.	See the appropriate service configuration chapter, as DHCP, option 82, and DHCP relay are configured at the service level.
DHCP relay DHCP discover messages are broadcast packets that typically do not leave the IP subnet. DHCP relay agents intercept the requests and forward them as unicast messages to a DHCP server. DHCP request messages from subscriber hosts are usually sent from the FTTx access node, with information appended to uniquely identify the residential gateway, either by MAC address of the residential gateway or by an option 82 string identifier that indicates the device, port type, rack, shelf, slot, port, and VLAN ID or VPI/VCI of the circuit connected to the residential gateway.	The DHCP relay agent sets the GIADDR in the packet to the IP address of the ingress interface (SAP). You must configure the BSA and BSR devices as DHCP relay agents when the DHCP requests are going to be forwarded to a DHCP server, or a 5750 SSC configured as a DHCP server. The maximum DHCP relay packet size is 1500 bytes.	See the appropriate L3 service (IES and VPRN) or L2 service (VPLS) configuration chapter. See the *5750 SSC Service Manager User Guide* and chapter 10 for more information about configuring the 5750 SSC as a DHCP relay agent.
DHCP lease state table The BSA maintains the identities of hosts that are allowed network access for each SAP on each service.	The lease state information is collected by snooping DHCP acknowledge messages on the SAP, using DHCP snooping. Entries in the DHCP lease state table remain valid for the duration of the IP address lease.	See chapter 17.
DHCP snooping The BSA can copy DHCP packets and inspect them to help secure the system. For example, if malicious user A sends an IP packet requesting a video stream intended for user B, return packets sent to user B could jam B's connection.	Use the 5620 SAM to configure DHCP snooping for the following purposes: • To insert Option 82 information when the system is not configured for DHCP relay by enabling DHCP snooping on the SAP closest to the host. • To build a DHCP lease state table by enabling DHCP snooping on the service tunnel nearest the network egress and on the SAP closest to the host. • To efficiently associate dynamic hosts with subscriber instances and associated network resources in a triple play service configuration	See the appropriate service chapters for configuration of the lease populate and snooping parameters. See chapter 64 for information about using DHCP snooping for subscriber identification purposes.

(2 of 3)

Feature and use	Notes	Reference
Option 82 The DHCP relay option allows managed devices to append information to the DHCP request that identifies where the DHCP request originated. You can also independently insert Option 82 information when DHCP snooping is enabled on a VPLS SAP. The Option 82 information can be: • The DHCP Option 82 string circuit ID value associated with the 7330 ISAM FTTN, or other ISAM family of nodes in the form ssc(*SSL-7330-1 atm 1/1/04/06:8.35*). The *device port_type rack/shelf/slot/port:VPI:VCI* identifier on the 7330 ISAM FTTN indicates that this is the connection configured for residential use, which is connected to the user's residential gateway. • The DHCP Option 82 string remote ID value associated with the 7330 ISAM FTTN, or other ISAM family of nodes in the form ssc(*remote ID*).	Using Option 82, you can identify: • the circuit ID (service tunnel binding) that is unique to the device relaying the circuit • the remote ID (MAC address) of the host at the far end of the circuit • the subscriber to which a host belongs for the purpose of assigning network resources The maximum DHCP relay packet size is 1500 bytes. If adding Option 82 information to the packet causes the packet to exceed 1500 bytes, the DHCP relay request is forwarded without including the Option 82 information.	See the appropriate service configuration chapter. For DHCP option 82 information inserted because of 5750 SSC DHCP server authentication, see chapter 10. For DHCP option 82 information inserted to identify subscribers, see chapter 64.

(3 of 3)

BTV multicast

This section describes, through the use of examples, how the 5620 SAM can be used to configure and manage the delivery of BTV multicast traffic streams.

Optimizing for broadcast TV means implementing multicast packet replication throughout the network. Multicasting improves the efficiency of the network by reducing the bandwidth and fiber needed to deliver broadcast channels to the end user. A multicasting device can receive a single copy of a broadcast channel and replicate it to any downstream devices that require it, thus substantially reducing the required network resources. This efficiency becomes increasingly important closer to the end user.

Multicast routing overview

Multicast routing delivers source traffic to multiple receivers without any additional burden to the source or the receivers, as is the case with increased bandwidth requirements in a unicast environment.

Multicast routing is based on an arbitrary group of receivers that expresses an interest in receiving a specific data stream. The group does not have physical boundaries—the hosts can be located anywhere on the Internet. The hosts must join the group using IGMP to receive the data stream.

A multicast-enabled device, such as a switch or router, distributes a data stream to multiple receivers. Multicast packets are replicated in the network by routers that are enabled with PIM, which results in the efficient delivery of data to multiple receivers using less bandwidth.

1 A switch or router distributes a data stream to multiple receivers, such as multicast-enabled PE switches or routers.

2 The multicast-enabled switch or router replicates the data stream, when required, and transmits a copy to each downstream switch or router in the multicast tree.

3 Each client receives the data stream it has subscribed to from the downstream switch or router.

The NEs involved in delivering BTV multicast streams are first preconfigured through CLI for discovery and management by 5620 SAM. After discovery, routing protocols are applied to the NEs using 5620 SAM. Routing, QoS, and network queue policies are then created. On some devices, multicast package and ACL filter policies are created. These policies are applied to NEs during service creation through 5620 SAM.

Content delivery

BTV source traffic consists of one IP multicast stream per broadcast channel. As a multicast stream enters the core network, it is directed by PIM to the RP, which replicates the multicast traffic to all DRs that have requested the specific multicast stream. DRs distribute the multicast stream directly to set-top receivers or through an M-VPLS to BTV VLAN rings to which customer set-top receivers are connected. Multicast streams are forwarded only to those set-top receivers that have requested them through IGMP and are entitled to them as subscriber hosts.

Content management

Multicast package policies on some devices define the available multicast addresses (BTV channels) for end users in a BTV network. Typically, a root package policy which includes all BTV channels associated with a 5620 SAM customer service is created. Subsets of the root policy are then created as BTV content packages to which end customers can subscribe. ACL filter policies on CE devices ensure that only the channels to which an end customer has subscribed are delivered to the customer set-top receiver.

PIM

PIM uses RPF to correctly forward multicast packets down a distribution tree, using the independent multicast and unicast routing tables created by the 7450 ESS in mixed mode or the 7750 SR. The unicast routing table is populated by the unicast routing protocols, such as OSPF, BGP, IS-IS, or static routes, which can also be configured to submit routes to the multicast routing table.

Depending on the configuration of the PIM routing instance, RPF can use the unicast routing table, the multicast table populated by the unicast routing protocols, or both to determine the upstream sources of multicast streams. PIM forwards a multicast packet only if it is received on an upstream interface that is associated with a source address of an upstream router. This RPF check assures that there are no loops in the distribution tree.

PIM uses a multicast domain to group receiver hosts on a router called the rendezvous point (RP). A bootstrap router (BSR) elects an RP from available candidates. The BSR manages RP information, disseminates it to all PIM routers in the multicast domain, and elects a new RP in the case of RP unavailability.

A receiver host becomes a member of a multicast domain by sending an IGMP join request for a multicast stream to a PIM designated router (DR). If the router does not currently receive the multicast stream, PIM updates the DR routing table with the receiver host IP address and requests the multicast stream from the RP. The RP adds the router to the distribution tree. Packets sent to the multicast IP address are propagated down the distribution tree to the receiver host. DRs use the RP as the source for a multicast stream unless a source with a lower path cost is available.

PIM stops sending a multicast stream to a router when it determines that there are no active receiver hosts for the multicast stream in that branch of the distribution tree.

MVR on VPLS

PIM is not supported on 7450 ESSs. When receiver hosts are connected to a PIM DR by way of a 7450 ESS, MVR must be configured on the switch. MVR allows multicast traffic to be forwarded downstream from the DR to the receiver host over an MVR VPLS.

IGMP

IGMP is used to dynamically register individual hosts in a multicast group on a specific LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a specific subnet.

MLD and MLD-snooping

The Multicast Listener Discovery protocol is essentially the IPv6 version of IGMP. It is used by IPv6 routers to discover the presence of multicast listeners (that is, nodes that wish to receive multicast packets) on their directly attached links, and to discover specifically which multicast addresses are of interest to those neighboring nodes.

MLD version 2 (MLDv2) is designed to be interoperable with MLD version 1 (MLDv1). MLDv2 adds the ability for a node to report interest in listening to packets with a specific multicast address only from specific source addresses or from all sources except for specific source addresses.

While 5620 SAM currently does not support MLD, it does support MLD-snooping. The 7x50 and 7710 SR routers allow the enabling of MLD snooping for VPLS services.

BTV multicast configuration examples

Figure 60-11 shows a simple BTV network and three methods of content delivery, examples A, B, and C. The sequence of specific configuration steps for each example follows general device, network and multicast configuration information common to all examples.

Note — In the examples on the following pages, references to "IGMP-snooping" may generally be read as "IGMP- or MLD-snooping", provided the routers employed in the configurations support the MLD protocol.

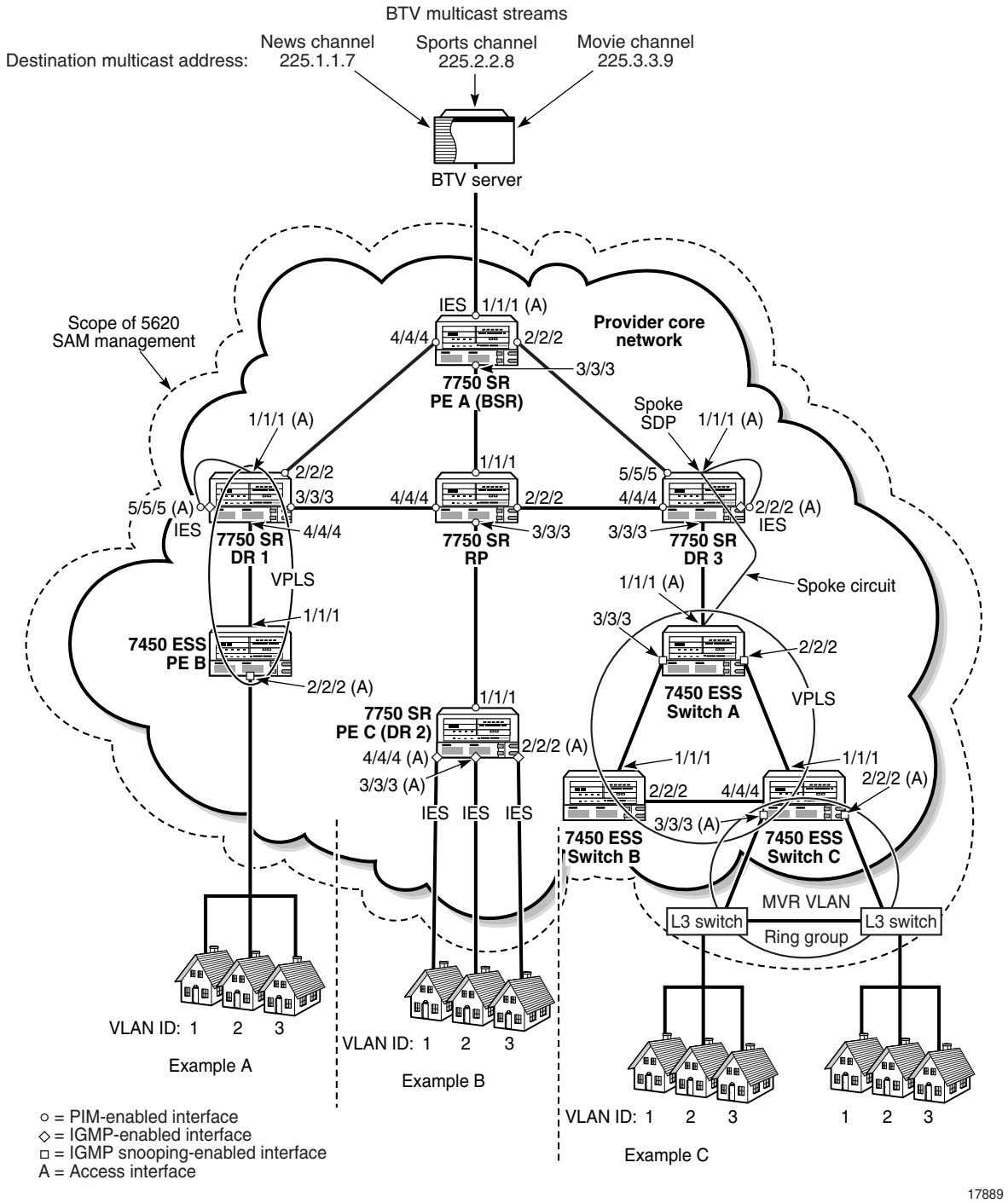
Device preconfiguration

A network device requires CLI preconfiguration before it can be managed by the 5620 SAM. The primary CLI preconfiguration actions for a device are:

- Assigning a system ID to the device
- Enabling and configuring SNMP on the device
- Enabling Telnet access on the device

See chapter 3 and the specific device documentation for more information about enabling device functionality before using the 5620 SAM.

Figure 60-11 BTV multicast delivery examples



After CLI preconfiguration, further actions are required:

- Discover devices, including mediation configuration with CLI user names and passwords.
- Use 5620 SAM to set the discovered device in a managed state.

See chapter 13 for more information about device discovery and management using 5620 SAM.

Network preconfiguration

The core network shown in Figure 60-11 represents a fully meshed group of devices. For simplicity, only the devices relevant to the BTV multicast examples are shown. Network preconfiguration consists of the following sequence of actions:

1 Configure network devices for in-band or out-of-band management. See chapter 12 for more information.

2 Configure a system interface on each device to serve as the identifier for the device. See chapter 27 for more information.

3 Configure network interfaces on each router to establish a full mesh of interconnectivity between devices. In Figure 60-11 the interfaces to be configured are PE A, ports 1/1/1, 2/2/2, 3/3/3, and 4/4/4; DR 1, port 2/2/2; RP, ports 1/1/1, 2/2/2, and 4/4/4; and DR 3, ports 1/1/1 and 4/4/4. See chapter 27 for more information.

4 Cable the network-interface ports between routers in the core network to establish the physical connectivity shown in Figure 60-11.

5 Use CLI ping commands to check IP connectivity between devices. See the device documentation for more information.

6 Enable IGPs such as RIP, OSPF, or IS-IS on devices according to network size and complexity. See chapter 28 for information about enabling routing protocols.

7 Enable an inter-AS routing protocol such as BGP or OSPF to PE routers, if required. See chapter 28 for more information.

8 Create routing policies as required. Create one multicast group for each BTV multicast destination address during policy creation. See chapter 27 for more information.

9 Configure routing protocols and apply routing policies as required. See chapter 28 for more information.

10 Configure LDP and MPLS, if required. See chapter 28 for information about configuring LDP. See chapter 29 for information about configuring MPLS.

- Enable MPLS and LDP on the routing instance of each device that is participating in the MPLS network.
- Assign a Layer 3 interface to the MPLS instance on each MPLS-enabled device.
- Create a mesh of MPLS paths.
- Create a mesh of LSPs.
- Use the 5620 SAM to create MPLS administrative groups, and assign the groups to MPLS interfaces and LSP paths as required.

Multicast configuration common to all examples

The network connections shown between PE A and DR 1 and between PE A and DR 3 represent redundant multicast routes used by PIM in the event of an RP failure. PIM dynamically adjusts to BSR or RP failure by electing a replacement BSR or RP or by using a previously defined backup BSR or RP. PIM chooses the most appropriate source for a multicast stream based on path cost and source availability and bypasses the RP if a better source for a multicast stream is found.

For simplicity, Figure 60-11 does not show routes to PE C (DR 2) from DR 1 or DR 3. As shown, PE C (DR 2) is isolated from multicast traffic in the event of RP failure.

Network multicast configuration common to all three examples involves the following sequence of actions:

1 Enable IGMP on routers DR 1, PE C (DR 2), and DR 3. See Procedure 28-35 for more information.

2 Configure IGMP on routers DR 1, PE C (DR 2), and DR 3. See Procedure 28-36 for more information.

3 Enable PIM on routers PE A, RP, DR 1, PE C (DR 2), and DR 3. See Procedure 28-31 for more information.

4 Configure PIM on routers PE A, RP, DR 1, PE C (DR 2), and DR 3. See Procedure 28-32 for more information.

- Specify PE A as the candidate bootstrap router.
- Specify RP as the candidate rendezvous point. You can also specify it as a static RP for a multicast domain, if there are multiple BTV domains, and configure a second router as a redundant RP.
- Specify IES as the Apply to parameter value on routers PE A, DR 1, PE C (DR 2), and DR 3.

5 Create PIM interfaces at PE A, ports 1/1/1, 2/2/2, 3/3/3, and 4/4/4; RP, ports 1/1/1, 2/2/2, 3/3/3 and 4/4/4; DR 1, ports 2/2/2 and 3/3/3; DR 2, port 1/1/1 and DR 3, ports 4/4/4 and 5/5/5. See Procedure 28-34 for more information.

6 Create QoS, scheduling, and accounting policies for the ingress BTV traffic. See chapter 43 for more information.

7 Create an IES from PE A, port 1/1/1, to the BTV multicast provider's network. See Procedure 70-1 for more information.

- Enable PIM on the IES SAP during IES creation.

Example A configuration

In Example A, IGMP join requests from residential hosts ingress a VPLS SDP. IGMP snooping on the VPLS registers the join requests on the local switch. The switch sends the requests over the VPLS, which is physically cross-connected to an IGMP- and PIM-enabled IES SAP on the DR. PIM on the DR requests the desired multicast stream, if not present, from the RP. The requested stream then traverses the VPLS and is sent to end users.

1 Configure PE B, port 1/1/1 and DR 1, port 4/4/4 as network ports. See Procedure 17-61 for more information.

2 Configure PE B, port 2/2/2 and DR 1, port 1/1/1 as access ports. See Procedure 17-61 for more information.

3 Cable DR 1, port 3/3/3, and PE B, port 1/1/1 to establish physical connectivity.

4 Configure DR 1, port 5/5/5 as an access port. See Procedure 17-61 for more information.

5 Create an IES on DR 1, port 5/5/5. See Procedure 70-1 for more information.

- Enable IGMP on the IES SAP during IES creation.
- Enable PIM on the IES SAP during IES creation.

6 Connect a cable between ports 1/1/1 and 5/5/5 on DR 1 as a service cross connect.

7 Create QoS, scheduling, filter, and accounting policies to apply to egress BTV traffic during service creation. See chapter 43 for information about policy creation.

8 Create a distributed VPLS with endpoints at PE B, port 2/2/2 and DR 1, port 1/1/1. See Procedure 68-1 for more information.

- Enable IGMP snooping on the VPLS SDP at PE B, port 2/2/2.
- Apply previously defined QoS, scheduling, filter, and accounting policies to the VPLS SDP at PE B, port 2/2/2.

Example B configuration

In Example B, an IGMP join request ingresses an IES SAP on the DR. PIM on the DR requests the desired multicast stream, if not present, from the RP. The requested stream is then delivered over an IES to an end user.

1 Configure PE C (DR 2), ports 2/2/2, 3/3/3, and 4/4/4 as access ports. See Procedure 17-61 for more information.

2 Create QoS, scheduling, filter, and accounting policies to apply to egress BTV traffic during IES creation. See chapter 43 for information about policy creation.

3 Create IES services on PE C (DR 2), ports 2/2/2, 3/3/3, and 4/4/4 that terminate on the CE set-top devices. See Procedure 70-1 for more information.

- Enable IGMP on each IES SAP during IES creation.
- Apply previously defined QoS, scheduling, filter, and accounting policies to each IES, as required.

Example C configuration

In Example C, IGMP join requests from residential hosts pass over an MVR VLAN to an VPLS. IGMP snooping on the VPLS registers the join requests on the local switch, which passes them over the VPLS to a spoke SDP on the DR. The spoke SDP's port is physically cross-connected to an IGMP- and PIM-enabled IES SAP on the DR. PIM on the DR requests the desired multicast stream, if not present, from the RP, then sends the stream over the VPLS and MVR VLAN to the end users.

1 Create a BTV MVR VLAN of L3 switches, such as 7250 SAS or Telco devices, in a ring group with endpoints on Switch A, ports 2/2/2 and 3/3/3. See section 65.4 and Procedure 65-1 for more information. For redundancy, the MVR VLAN can be configured with endpoints on different switches. A VLL between the two switches acts as an unbreakable connection.

2 Enable and configure IGMP snooping on the bridge instances for the L3 switches included in the MVR VLAN. See section 28.1 for information specific to 7250 SAS Telco devices or see the specific device documentation if the L3 switch a type not managed by the 5620 SAM.

3 Create QoS, scheduling, filter, and accounting policies to apply to egress BTV traffic during service creation. See chapter 43 for information about policy creation.

4 Configure the following as network ports:

- Switch A, ports 1/1/1, 2/2/2, and 3/3/3
- Switch B, ports 1/1/1 and 2/2/2
- Switch C, ports 1/1/1, 2/2/2, 3/3/3 and 4/4/4

See Procedure 17-61 for more information.

5 Create a distributed VPLS consisting of Switch A, Switch B, and Switch C. See Procedure 68-1 for more information.

- Apply previously defined QoS, scheduling, filter, and accounting policies to the VPLS SDPs.
- Enable and configure IGMP snooping on the VPLS SDPs that are part of the MVR VLAN.
- Ensure that the encapsulation value of the VPLS SDPs that are part of the MVR VLAN matches the MVR VLAN ID.
- Create a split horizon group during VPLS creation to allow later addition of a spoke circuit to the VPLS.
- Configure STP on the VPLS, as required.

6 Configure DR 3, port 2/2/2 as an access port. See Procedure 17-61 for more information.

7 Create an IES on DR 3, port 2/2/2. See Procedure 70-1 for more information.

- Enable IGMP on the IES SAP during IES creation.
- Enable PIM on the IES SAP during IES creation.

8 Connect a cable between ports 1/1/1 and 2/2/2 on DR 3 as a service cross connect.

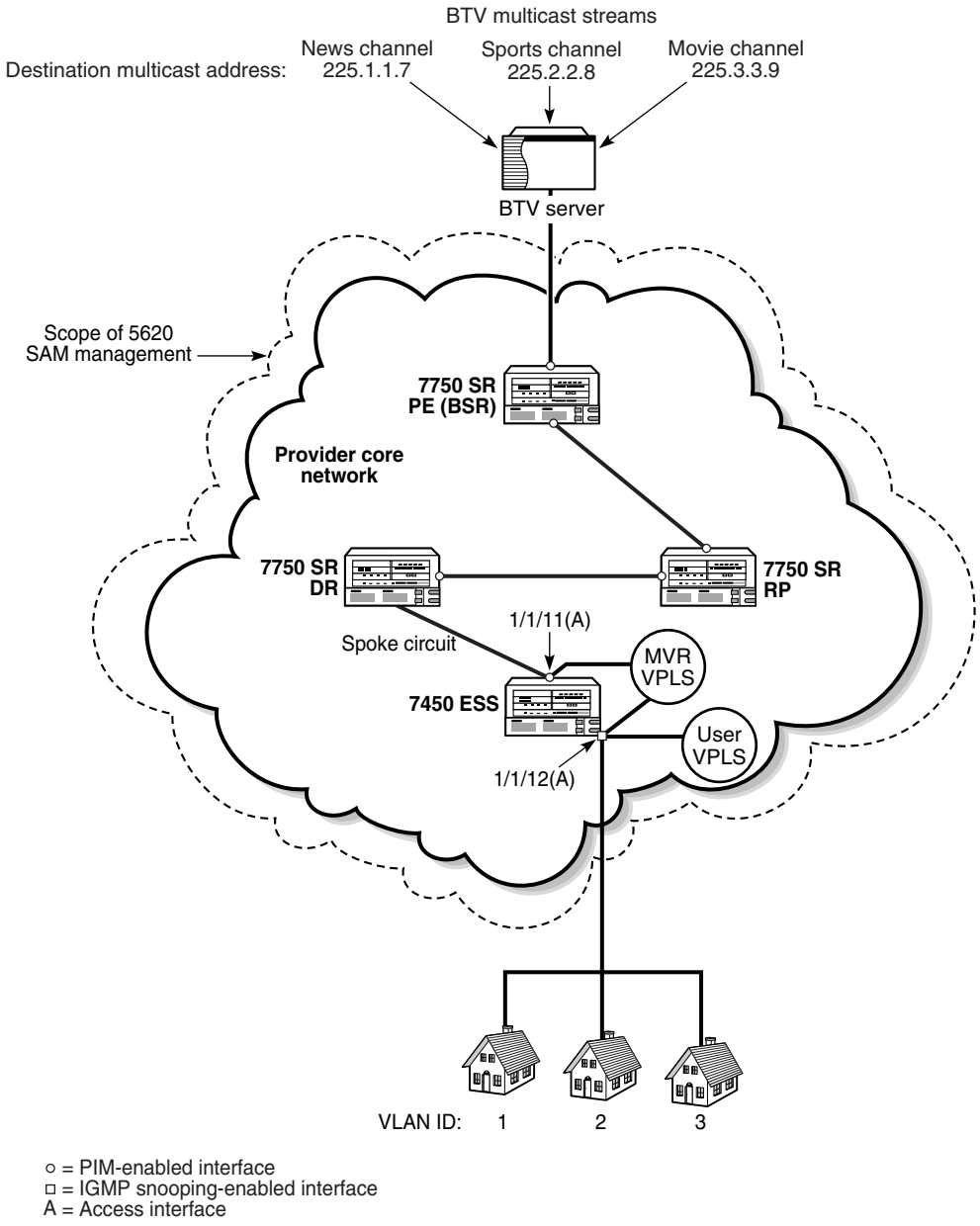
9 Create a VPLS spoke SDP at DR 3, port 1/1/1. See Procedure 68-9 for more information.

Example D configuration

Figure 60-12 shows an example of BTV multicast delivery using MVR on VPLS.

See Figure 60-11, and sections "Network preconfiguration" and "Multicast configuration common to all examples" for common network configuration information.

Figure 60-12 BTV multicast delivery using MVR on VPLS example



In Example D, IGMP join requests from residential hosts are sent to a user VPLS on the 7450 ESS. IGMP snooping on the user VPLS registers the join requests on the switch, which sends them to the 7750 SR DR. PIM on the DR requests the desired multicast stream, if not present, from the RP, then sends the stream over the MVR VPLS to the user VPLS, from which the multicast stream is sent to the end users.

1 Create a multicast package policy to apply to the 7450 ESS that belongs to the MVR VPLS. See chapter 46 for more information.

2 Configure the following ports as access ports. See Procedure 17-61 for more information.
   - 7450 ESS, port 1/1/11
   - 7450 ESS, port 1/1/12

3 Create an MVR VPLS on the 7450 ESS with SAPs 1/1/11 and 1/1/12. Apply the previously defined multicast package policy to the MVR VPLS.

4 Create a user VPLS on SAP 1/1/12 of the 7450 ESS.
   - Associate the user VPLS with the previously created MVR VPLS to identify the MVR VPLS as the source of the multicast traffic.
   - Enable and configure IGMP snooping on the site.

5 Create a spoke circuit between the 7450 ESS (endpoint 1/1/11) and the 7750 SR DR.

60.3 Implementing QoS workflow on an OmniSwitch

1 Enable or disable QoS.

2 Configure global settings such as global port parameters, default disposition for flows, and timeouts. The parameters that you need to configure globally depend on the types of policies that you need to configure.

Typically, you do not need to change any of the global defaults. See Procedure 28-51 for information about configuring global QoS parameters.

3 Configure QoS port parameters, which includes setting QoS parameters on a per port basis. Typically you do not need to change the port defaults. See Procedure 17-62 for information about configuring port QoS parameters.

4 Configure QoS policies. A QoS policy contains a condition and an action. The condition specifies parameters that the switch checks in incoming flows. The action specifies how the switch responds to a flow that matches the condition. See chapter 44 for more information about configuring QoS policies.

60.4 Implementing QoS workflow on the 7750 SR, 7450 ESS, 7710 SR, and 7705 SAR

Planning and configuration

1 Perform network planning activities:

i Determine the required types of services or applications (For example, voice, video, and data).

ii Review SLAs.

iii Perform traffic engineering activities at the IP/MPLS core level to ensure that resources are available.

2 Configure IP and MAC ACL filters, as required.

3 Configure the slope policies.

   i Configure the high slope parameters.

   ii Configure the low slope parameters.

   iii Configure the TAF (weight) parameter.

4 Configure the scheduler policies. Scheduler policies can be shared between ingress and egress policies, depending on your specific requirements.

5 Configure the port scheduler policies.

6 Create the aggregation schedulers, if required.

7 Configure the access ingress policies.

   i Configure the forwarding classes.

   ii Configure the queues.

   iii Map QoS markings on ingress packets to the forwarding classes.

   iv Map forwarding classes to the queue definitions.

   v Map queue definitions to the scheduler policies.

8 Configure the access egress policies.

   i Configure the queues.

   ii Map forwarding classes to the queue definitions.

   iii Map queue definitions to the schedulers policies.

9 Configure the network policies.

   i Configure for ingress:

   - Map QoS markings on ingress packets to the forwarding classes.
   - Map forwarding classes to the queue definitions.

   ii Configure for egress:

   - Configure remarking, if required.
   - Map QoS markings to the forwarding classes, if required.

10 Configure the network queue policies.

   - Configure the queue parameters.
   - Queue-to-forwarding class mapping is pre-defined and is not configurable.

11 Configure the time of day policies.

   - Configure the time ranges.
   - Create time of day suites.

Application of policies and schedulers to equipment and interfaces

12 Associate the slope policies with ports or daughter cards.

13 Associate the network queue policies with MDAs.

14 Assign the aggregation schedulers at the interface level, if required.

Configuration of customers and services

15 Configure the customers.

16 Create the customer services, and assign policies during the configuration.

60.5 5620 SAM QoS policies

Policies group and manage the various QoS elements used to determine how traffic is routed.

- access ingress policies
  Specify how QoS marking is interpreted, how customer traffic is mapped into queues, and how queues are classified.
- access egress policies
  Specify how customer traffic is mapped into queues, specify queue classification, queue parameters, and QoS marking.
- network policies
  Specify QoS marking to forwarding class mapping on ingress and QoS marking to forwarding class mapping on egress.
- network queue policies
  Specify CIR, PIR, and burst sizes for each queue. Forwarding class to queue mapping is not configurable.
- scheduler policies
  Specify custom settings and a hierarchical structure of virtual schedulers to replace the default hardware schedulers on the device.
- port scheduler policies
  Specify bandwidth allocation at the egress port level.
- HSMDA scheduler policies
  Specify schedulers to define egress port and ingress scheduler behavior on an HSMDA.
- slope policies
  Specify WRED settings to customize how in-profile and out-of-profile traffic is processed in hardware buffers, applied to daughter cards or ports.
- HSMDA slope policies
  Specify settings for controlling how the depth of HSMDA queues is managed.
- ATM QoS policies
  Specify ATM QoS settings to customize ATM traffic parameters including service category and shaping.

Figure 60-13 shows where QoS policies are applied at the service level.

Figure 60-13 Service-level view of policies

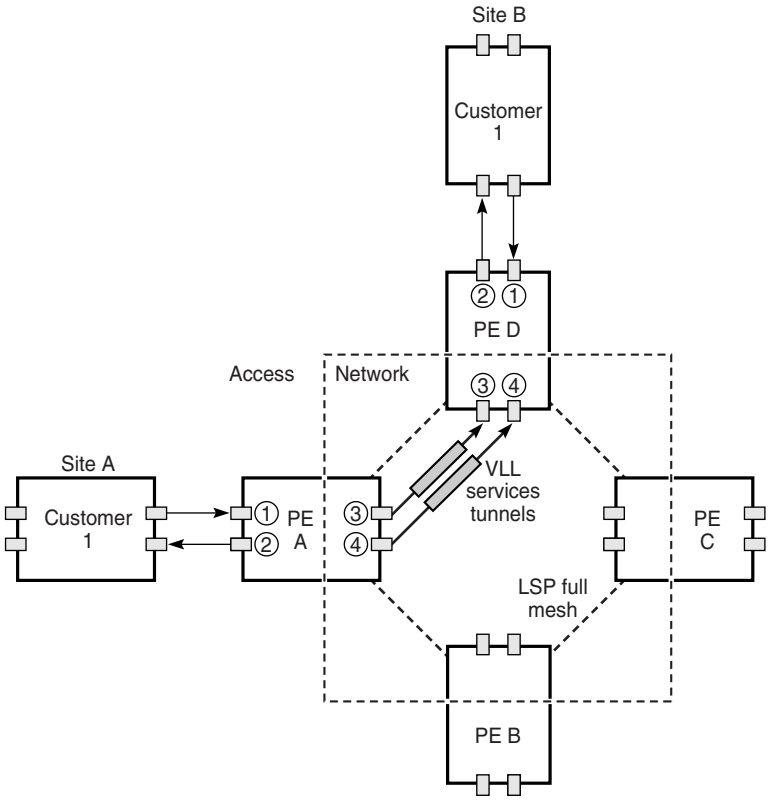
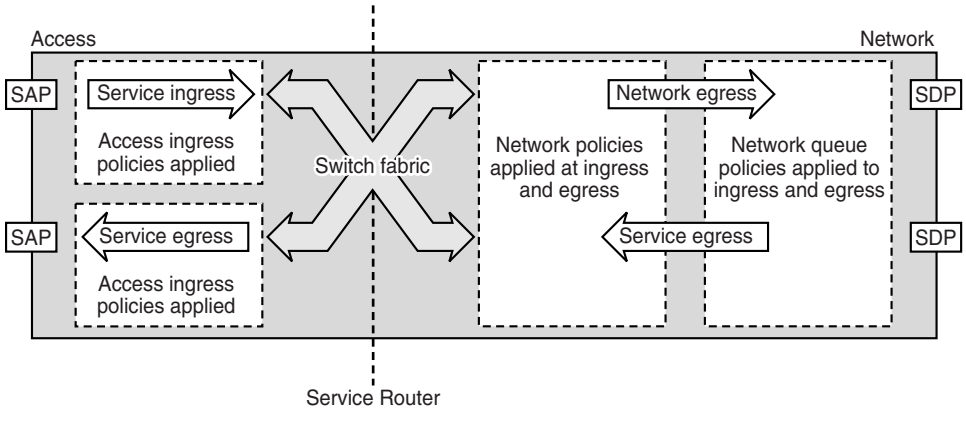


Figure 60-14 shows where policies are applied on a device with respect to access and network ingress and egress traffic.

Figure 60-14 Types of traffic on a device and applied policies



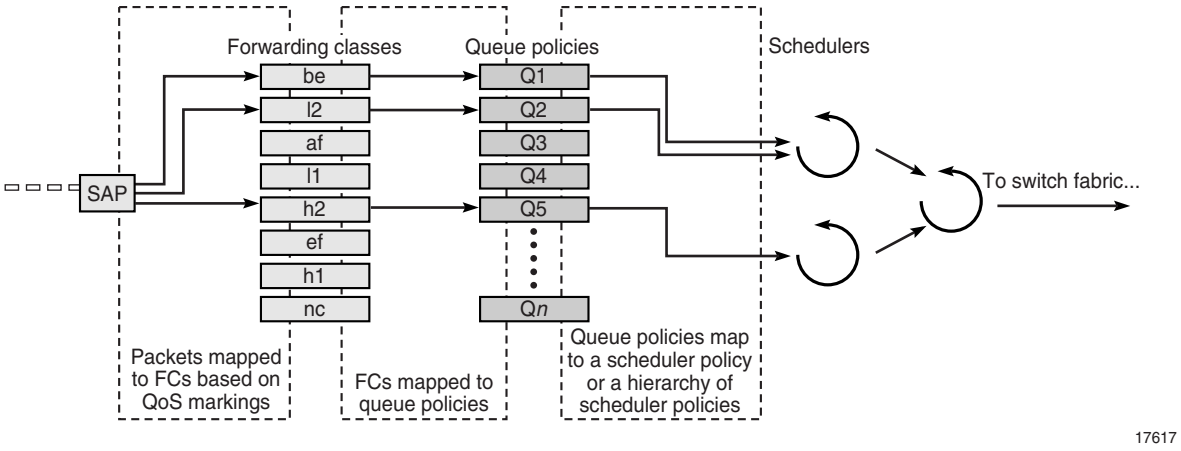
Access ingress policies

Access ingress policies are applied to access interfaces and specify QoS characteristics on ingress. Participation in access ingress policies is defined when access interfaces are configured or modified. Access ingress policies include:

- mapping of QoS marking, such as dot1p, DSCP, and precedence, and IP/MAC address information to forwarding classes
- forwarding class definitions and mapping to queues
- queue definitions and mapping to schedulers

Figure 60-15 shows the access ingress policy elements.

Figure 60-15 Access ingress policy elements



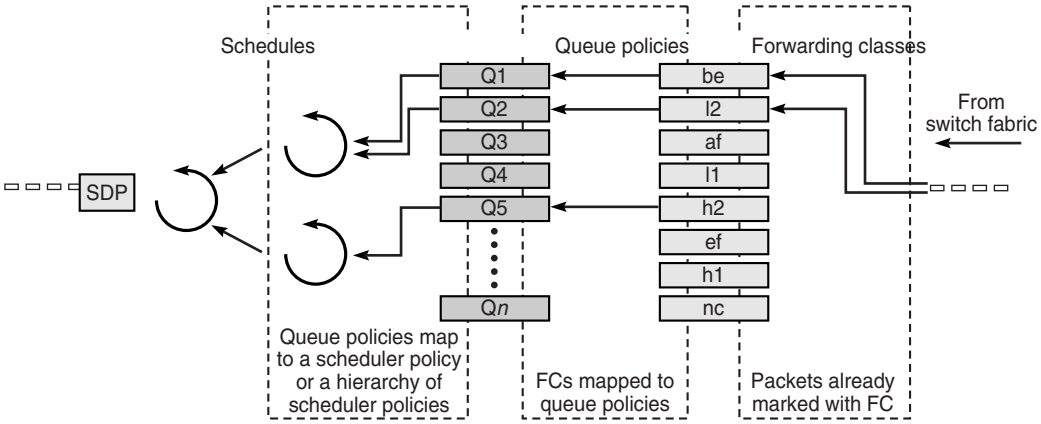
See "Access ingress policies" in section 44.1 for more information about access ingress policies.

Access egress policies

Access egress policies are applied to access egress interfaces and specify QoS characteristics on egress. Participation in Access egress policies is defined when access interfaces are configured or modified. Access egress policies include:

- forwarding class definitions and mapping to queues
- queue definitions and mapping to schedulers

Figure 60-16 Access egress policy elements



In Figure 60-16, packets are marked with an FC, either by:

- ingress policy if the packet was received on the same device
- in the tunnel transport encapsulation if received using a service tunnel

See "Access egress policies" in section 44.1 for more information.

Network policies

Network policies define egress QoS markings and ingress QoS interpretation for traffic on core network IP interfaces. A network policy defines:

- DSCP name mapping to forwarding classes
- LSP EXP value mappings to forwarding classes
- whether QoS remarking is enabled

Figure 60-17 shows the sequence of how the elements of network and network queue policies are applied at ingress.

Figure 60-17 Network and network queue policy elements on ingress

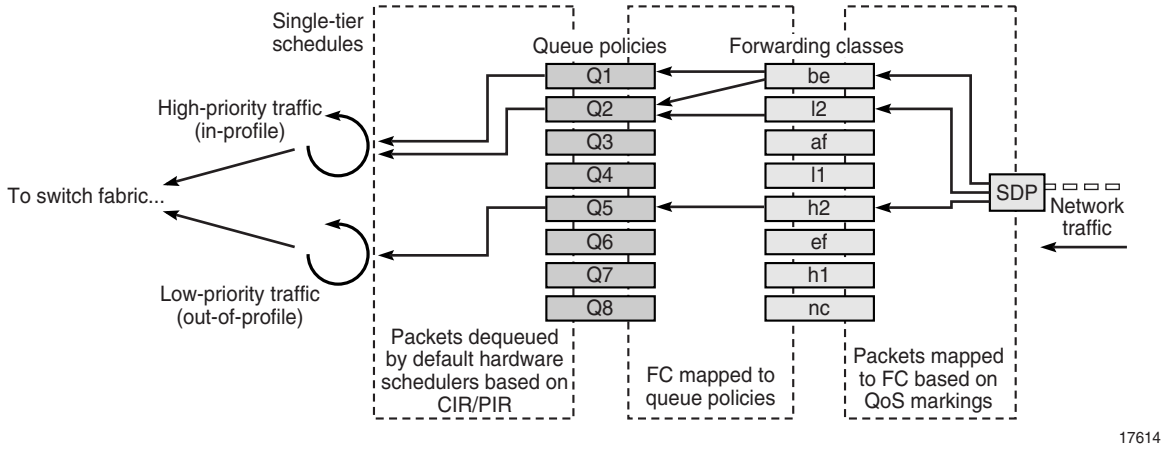
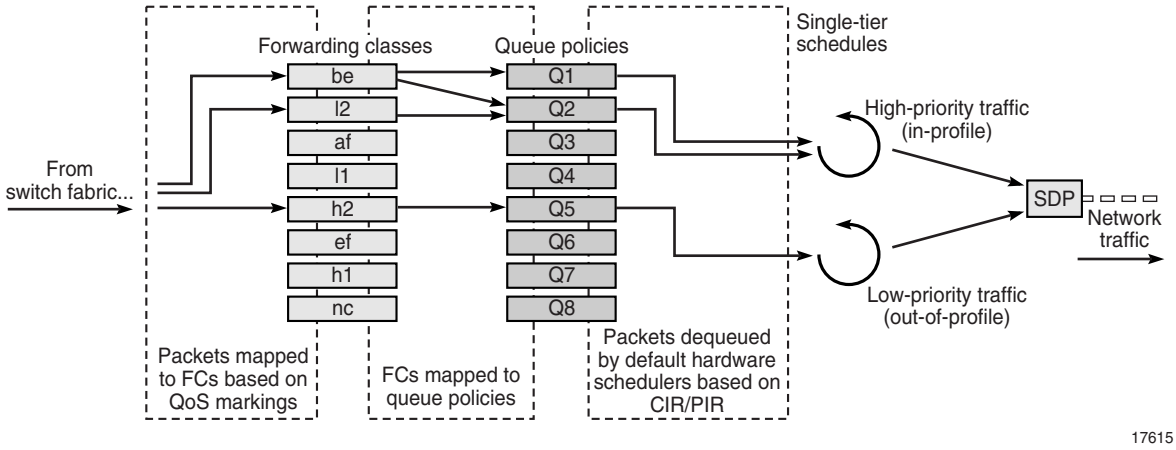


Figure 60-18 shows the sequence of how the elements of network and network queue policies are applied at egress.

Figure 60-18 Network and network queue policy elements on egress



See "Network policies" in section 44.1 for more information.

Network queue policies

Network queue policies define the network forwarding class queue characteristics for core egress network ports and for ingress on MDAs.

See Figure 60-17 and Figure 60-18 for the sequence of how the different elements of network and network queue policies are applied on ingress in and on egress.

The queued packets are serviced by single-tier schedulers on the device and are forwarded to a single destination switch fabric port or a network interface.

See "Network queue policies" in section 44.1 for more information about network queue policies.

Scheduling

Scheduling defines the order and method for how packets which are enqueued in different queues, are dequeued. Ingress schedulers control the data transfer between the queues and the switch fabric. Egress schedulers control the data transfer between the egress queues and the switch fabric. Packets are not actually forwarded to schedulers, but are forwarded from the queues directly to ingress and egress interfaces. Participation in scheduler policies is defined when access interfaces are configured or modified. There are two types of scheduling:

- Single-tier scheduling is the hardware-based default method for scheduling queues on the device. There are no configurable parameters for single-tier schedulers. When a scheduler policy is not specified for an access interface, rate limiting is specified by the values specified in the queue and scheduling is performed by the default hardware scheduler on the device. Single-tier scheduling consists of a pair of scheduling priority loops in the 7750 SR and bases scheduling on the CIR and the PIR set in the queue policy. One loop is for scheduling high-priority (in-profile) traffic, and the other loop is for low-priority (out-of-profile) traffic.
- Virtual hierarchical (multi-tier) scheduling can provide more flexible scheduling for access ingress and egress interfaces, and determine how queues are scheduled. They are defined using a Scheduler policy, and can be configured to override default hardware scheduling. You can create up to three tiers of virtual schedulers.

  Aggregation schedulers are used to share a scheduler policy across a number of ports or daughter cards. This can be useful when a number of ports or cards are dedicated to the same customer. See "Scheduler policies" in section 44.1 for more information about configuring aggregation schedulers.

Port scheduler policies

Port scheduler policies define the bandwidth allocation based on the available bandwidth at the egress port level. A port scheduler policy manages a bandwidth allocation algorithm that represents a virtual multi-tier scheduling hierarchy.

The port scheduler allocates bandwidth to each service or subscriber that is associated with an egress port. Egress queues on the service may have a child association with a scheduler policy on the SAP or multi-service site. All queues must compete for bandwidth from an egress port. There are two methods of bandwidth allocation on the egress access port:

- **direct association of port scheduler on a SAP or multi-service site with service or subscriber queue**

  A service or subscriber queue is associated with a scheduler on the L2 access interface or multi-service site, and the service-level scheduler policy is associated with a port level scheduler.
- **direct association of port scheduler with service or subscriber queue**

  A service or subscriber queue is associated with a port scheduler. The port scheduler hierarchy allocates bandwidth at each priority level to each service or subscriber queue.

See "Port scheduler policies" in section 44.1 for more information about configuring port scheduler policies.

HSMDA scheduler policies

The port-based scheduler manages forwarding for each egress port on the HSDMA. Each port-based scheduler maintains up to eight forwarding levels. Eight scheduling classes contain each of the queues that are assigned to the port scheduler. Membership in a scheduler is defined by the queue identifier.

The port-based scheduler supports a port-based shaper that is used to create a sub-rate condition on the port. Each scheduling level can be configured with a shaping rate to limit the amount of bandwidth allowed for that level.

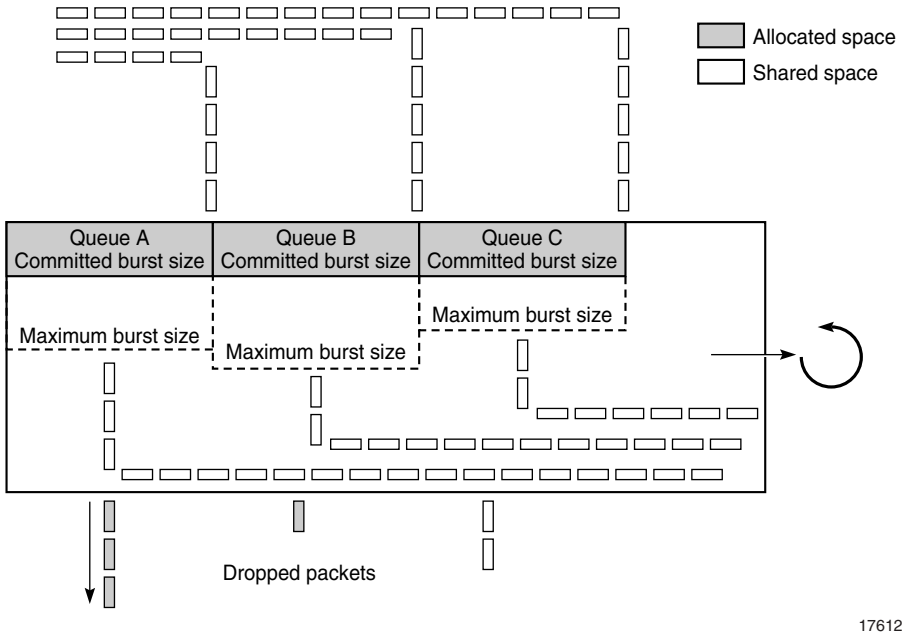
The port-based scheduler allows two weighted groups (group 1 and group 2) to be created. Each group can be populated with three consecutive scheduling classes.

See "HSMDA scheduler policies" in section 44.1 for more information about configuring slope policies.

Slope policies

Slope policies manage how shared buffers are utilized on the SR. When traffic is queued, the WRED slope parameters in the slope policy determine how the traffic is buffered for dequeuing, as shown in Figure 60-19.

Figure 60-19 Slope policy characteristics



All queues are in contention for shared buffer space when they exceed their CBS, and can use their MBS, when space is available in the shared buffer space. The WRED parameters determine whether a packet is discarded or not, and, as a result, determine whether the packet is dequeued. When the shared buffer space exceeds or approaches the maximum percentage defined by the WRED configuration, packets are discarded.

By using two independent slope policy configurations, one for in-profile traffic and one for out-of-profile traffic, you can configure in-profile traffic to receive preferential treatment over out-of-profile traffic.

See "Slope policies" in section 44.1 for more information about configuring slope policies.

HSMDA slope policies

HSMDA slope policies control the HSMDA queues. Each queue supports an index for an HSMDA slope policy table. Each policy in the table consists of two RED slopes (one high priority and another for low priority) to manage queue congestion. HSMDA RED slopes operate on the instantaneous depth of the queue.

A packet that attempts to enter a queue triggers a check to see whether the packet is allowed based on queue congestion conditions. The packet contains a congestion-priority flag that indicates whether the HSMDA is to use the high or low slope. The slope policy containing the slope is derived from the policy index in the queue configuration parameters on the HSMDA.

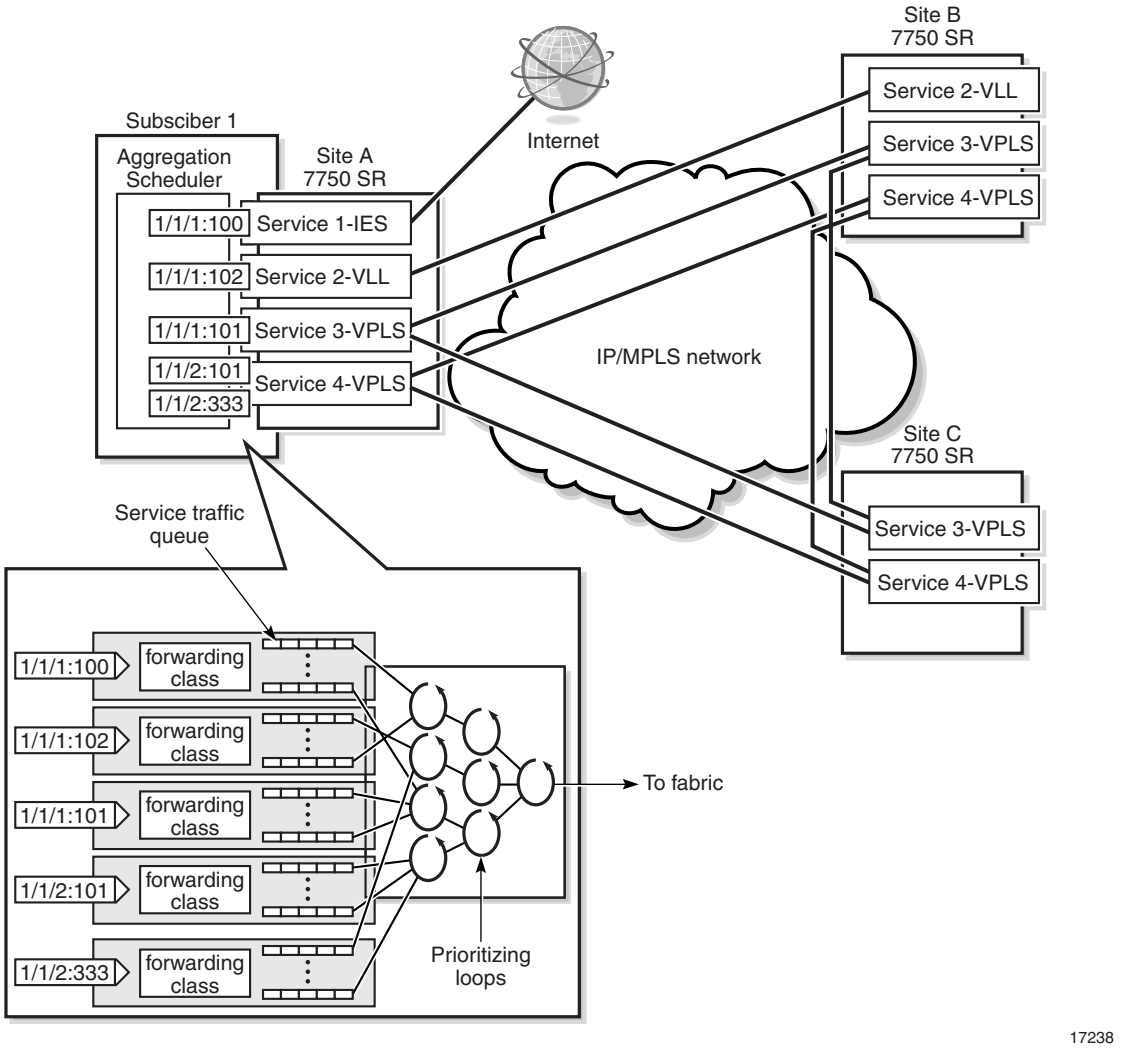
The RED slope discards are based on the current queue depth before a packet is allowed into the queue. Therefore, a queue may consume buffers that are greater than the configured MBS value based on the size of the packet. After the packet maximum is reached, packets that are associated with the queue are discarded. When the schedule removes packets from the queue, the queue depth decreases, which eventually lowers the depth of the threshold.

See "HSMDA slope policies" in section 44.1 for more information about configuring HSMDA slope policies.

60.6 Sample network configuration using QoS

Figure 60-20 shows a sample service configuration using QoS.

Figure 60-20 Sample service configuration using QoS



In this configuration, the following services are provisioned:

- Service 1: IES for Internet access, which requires a CIR of 10 Mb/s and a PIR of 100 Mb/s
- Service 2: VLL service for FTP connectivity between Site A and Site B, which requires a CIR of 10 Mb/s and a PIR of 20 Mb/s
- Service 3: VPLS for video-conference service over sites A, B, and C, which requires a CIR of 20 Mb/s and a PIR of 50 Mb/s
- Service 4: VPLS for voice traffic, which requires a CIR of 10 Mb/s and a PIR of 20 Mb/s

The cumulative rate at site A needs to be limited to 70 Mb/s.

The following high-level steps are required to create the Figure 60-20 configuration with rate limiting using QoS at Site A. Similar steps are required to configure QoS for Subscriber 1 on Sites B and C:

1 Configure a scheduler policy.

2 Create Subscriber 1.

3 Create the aggregation scheduler for Subscriber 1 on site A and assign ingress and egress scheduler policies to the aggregation scheduler.

4 Create IES, VLL, and VPLS for Subscriber 1.

- Specify sites for the services.
- Specify access interfaces for the sites.
- Specify the aggregation scheduler policy for the access interfaces.
- Bind the services to tunnels for transport through the IP/MPLS network.

Access interfaces 1/1/1:100, 1/1/1:101, 1/1/1:102, and 1/1/2:101 participate in the aggregation scheduler and are usually rate limited by the rate specified in the scheduler policy.

Access interface 1/1/2:333 does not participate in scheduler policy; rate limiting is specified by the queue values.

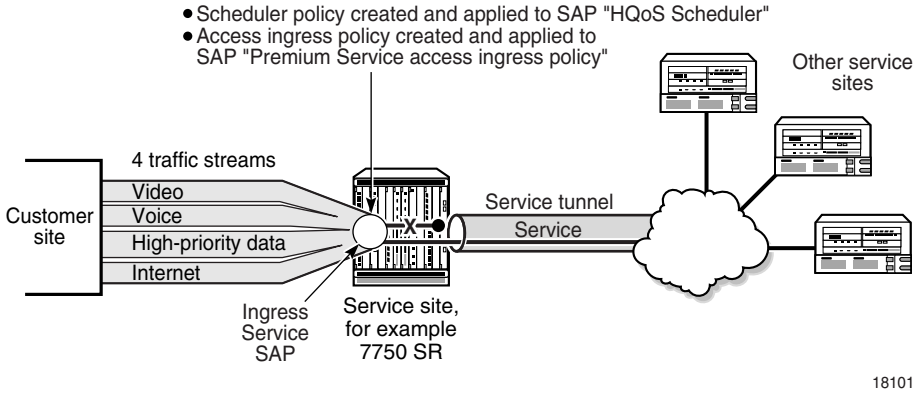
If one of the access interfaces does not participate in the scheduler aggregator, it may be managed by a separate scheduler policy.

60.7 Sample SAP QoS configuration

You can use 5620 SAM to configure and enforce traffic rate limiting, based on the priority of the traffic entering the ingress SAP of a service. This configuration limits bandwidth, to ensure that SLAs are met and higher priority traffic is processed first.

Figure 60-21 shows traffic of different priorities from a customer site to an ingress SAP.

Figure 60-21 Sample ingress traffic to a service SAP



Based on the example, use the 5620 SAM client GUI to perform the following actions:

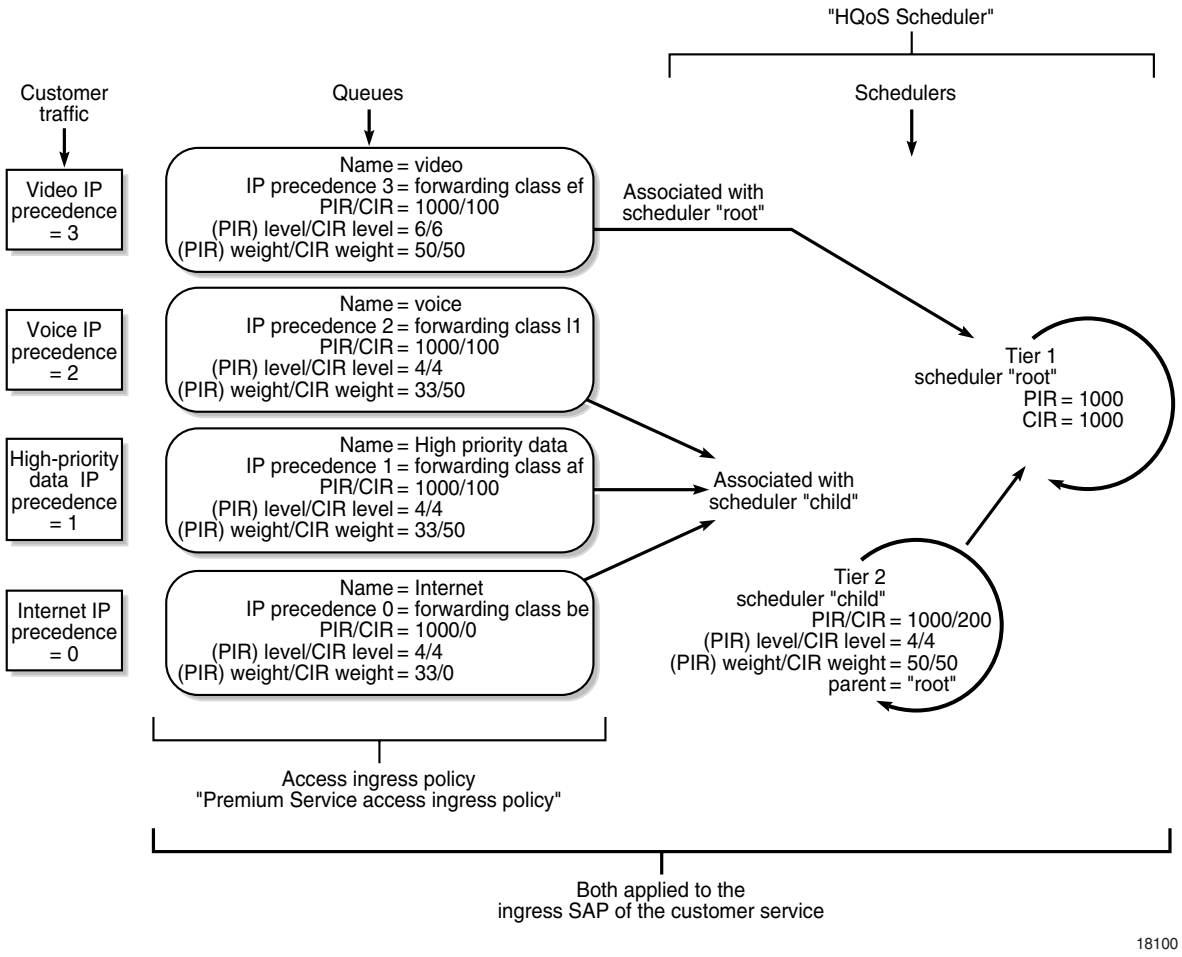
- Configure a parent scheduler that handles scheduling for a child scheduler.

Note — You do not have to configure a parent tier 1 scheduler for a child tier 2 scheduler. You can create a tier 2 scheduler on its own, with no parent. This example is meant to show hierarchical QoS.

  - Add a root tier 1 scheduler
  - Add one child tier 2 scheduler with the root scheduler as a parent
- Create an access ingress policy named Premium service access ingress policy.
  - Create 4 queues within the access ingress policy, one for each type of traffic from the customer site.
  - Associate each queue with a forwarding class
  - Classify the incoming customer site traffic to a forwarding class. For this sample, IP precedence is used to classify traffic. You could classify traffic other ways, for example, based on filters for IP address or DSCP marking.
  - Associate each queue with the appropriate scheduler.
- Apply the schedulers and access ingress policy to the appropriate L2 or L3 interface for the customer service, for example, a VPLS L2 interface.

Figure 60-22 shows how traffic is handled based on the ingress access policy and scheduler queue handling applied to the ingress service SAP.

Figure 60-22 Traffic handling based on ingress access policy and scheduler queue



In this sample:

- higher-priority video traffic, with IP precedence bit 3 set, goes into queue 4 with a PIR of 1000 Kb/s and a CIR of 100 Kb/s. This traffic is handled by the tier 1 scheduler. The levels and weights associated with the video queue (forwarding class of ef, level of 6, PIR/CIR weights of 50/50) ensure this traffic gets all required bandwidth.
- all other traffic goes into its appropriate queues, based on the mapping of the IP precedence bit with the forwarding class.
- The voice, high-priority data, and Internet queues are serviced by the tier 2 scheduler.
- Because the voice and high-priority data queues have higher PIR/CIR weight than the Internet queue, when there is contention for bandwidth, the voice and high-priority data queues are processed first.

Procedure 60-1 To configure QoS on a SAP

You must have:

- the service ingress SAP configured as access
- all necessary cabling and network routing protocol configurations complete to handle routing packets to and from the CPE equipment

1 Choose Policies→QoS→SROS QoS→Scheduler from the 5620 SAM main menu. The manage scheduler policies form opens.

2 Click on the Create button. The scheduler policy create form opens.

3 Configure the parameters. Set the displayed name to High QoS.

4 Click on the Schedulers tab button.

5 Click on the Add button. The scheduler entry form opens.

6 Create a root, tier 1 scheduler entry,

i Configure the parameters.

- Displayed name to root
- tier to 1
- Summed CIR to false
- PIR (kbps) to 1000
- CIR (kbps) to 1000

ii Click on the OK button. The root scheduler appears in the list of scheduler entries.

7 Create a child, tier 2 scheduler entry.

i Click on the Add button.

ii Configure the parameters.

- Displayed name to child
- tier to 2
- Summed CIR to false
- PIR (kbps) to 1000
- CIR (kbps) to 200
- Parent scheduler to root, using the Select button to choose root from the list.
- Level (PIR level) to 4
- Weight (PIR weight) to 50
- CIR Level to 4
- CIR Weight to 50

iii Click on the OK button. The child scheduler appears in the list of scheduler entries.

8 Click on the Apply button.

9 Close the Scheduler form.

10 Choose Policies→QoS→SROS QoS→Access Ingress from the 5620 SAM main menu. The manage access ingress policies form opens.

11 Click on the Create button. The access ingress policy create form opens.

12 Configure the parameters. Set the displayed name to Premium service access ingress policy.

13 Click on the Queues tab button. Create four queues. For this sample, default queue 1 is modified, and three new queues are added. The default multicast queue 11 is unchanged.

14 Select queue 1 from the list.

i Click on the Properties button. The queue 1 edit form opens.

ii Configure the parameters.

- Displayed Name to Internet
- Scheduler to child by using the Select button and choosing child from the list
- Level (PIR level) to 4
- CIR Level to 4
- Weight (PIR weight) to 33
- CIR Weight to 0

iii Click on the CIR/PIR tab button.

iv Configure the parameters.

- deselect both MAX buttons
- Cir (kbps) to 0
- Pir (kbps) to 1000

v Click on the OK button.

15 Add queue 2.

i Click on the Add button. The queue create form opens.

ii Configure the parameters.

- ID to 2
- Displayed Name to High-priority traffic
- Scheduler to child by using the Select button and choosing child from the list
- Level (PIR level) to 4
- CIR Level to 4
- Weight (PIR weight) to 33
- CIR Weight to 50

iii Click on the CIR/PIR tab button.

iv Configure the parameters.

- deselect both MAX buttons
- Cir (kbps) to 100
- Pir (kbps) to 1000

v Click on the OK button. The queue is added to the list.

16 Add queue 3.

i Click on the Add button. The queue create form opens.

ii Configure the parameters.

- ID to 3
- Displayed Name to Voice
- Scheduler to child by using the Select button and choosing child from the list
- Level (PIR level) to 4
- CIR Level to 4
- Weight (PIR weight) to 33
- CIR Weight to 50

iii Click on the CIR/PIR tab button.

iv Configure the parameters.

- deselect both MAX buttons
- Cir (kbps) to 100
- Pir (kbps) to 1000

v Click on the OK button. The queue is added to the list.

17 Add queue 4.

i Click on the Add button. The queue create form opens.

ii Configure the parameters.

- ID to 4
- Displayed Name to Video
- Scheduler to root by using the Select button and choosing root from the list
- Level (PIR level) to 6
- CIR Level to 6
- Weight (PIR weight) to 50
- CIR Weight to 50

iii Click on the CIR/PIR tab button.

iv Configure the parameters.

- deselect both MAX buttons
- Cir (kbps) to 100
- Pir (kbps) to 1000

v Click on the OK button. The queue is added to the list.

18 Click on the Apply button to save the changes. Confirm the action.

19 Associate each queue with a forwarding class.

i Click on the Forwarding Classes tab button.

ii Click on the Add button. The forwarding class create form opens.

iii Configure the parameters.

- Forwarding class to be
- Queue ID to 1. This is the best-effort Internet traffic queue.

iv Click on the OK button. Confirm the action.

v Click on the Add button. The forwarding class create form opens.

vi Configure the parameters.

- Forwarding class to af
- Queue ID to 2. This is the high-priority data traffic queue.

vii Click on the OK button. Confirm the action.

viii Click on the Add button. The forwarding class create form opens.

ix Configure the parameters.

- Forwarding class to l1
- Queue ID to 3. This is the voice traffic queue.

x Click on the OK button. Confirm the action.

xi Click on the Add button. The forwarding class create form opens.

xii Configure the parameters.

- Forwarding class to ef
- Queue ID to 4. This is the highest priority, video traffic queue.

xiii Click on the OK button. Confirm the action.

20 Click on the Apply button. Confirm the action.

21 Associate the IP precedence bits of the incoming customer traffic with the forwarding class. The forwarding class is already associated with a queue. For this sample, IP precedence bits are used to associate different types of traffic with the forwarding class. You could classify traffic other ways, for example, based on filters for IP address or DSCP marking.

i Click on the Precedence tab button.

ii Click on the Add button. The precedence create form opens.

iii Configure the parameters to associate IP precedence 0 (Internet traffic from the customer site) with forwarding class be (the be forwarding class is associated with queue 1)

- Precedence is 0
- Forwarding Class is be

iv Click on the OK button. Confirm the action. The association between precedence 0 and the be forwarding class is added to the list.

v Click on the Add button. The precedence create form opens.

vi Configure the parameters to associate IP precedence 1 (high-priority data traffic from the customer site) with forwarding class af (the af forwarding class is associated with queue 2)

- Precedence is 1
- Forwarding Class is af

vii Click on the OK button. Confirm the action. The association between precedence 1 and the af forwarding class is added to the list.

viii Click on the Add button. The precedence create form opens.

ix Configure the parameters to associate IP precedence 2 (voice traffic from the customer site) with forwarding class l1 (the l1 forwarding class is associated with queue 2):

- Precedence is 2
- Forwarding Class is l1

x Click on the OK button. Confirm the action. The association between precedence 2 and the l1 forwarding class is added to the list.

xi Click on the Add button. The precedence create form opens.

xii Configure the parameters to associate IP precedence 3 (video traffic from the customer site) with forwarding class ef (the ef forwarding class is associated with queue 3)

- Precedence is 3
- Forwarding Class is ef

xiii Click on the OK button. Confirm the action. The association between precedence 3 and the ef forwarding class is added to the list.

22 Click on the Apply button. Confirm the action.

23 Click on the Relations tab button to view the associations between the IP precedence bit number, the forwarding class, and the queues.

24 Associate a service SAP with the created High QoS scheduler and the created Premium service access ingress policy. There are many ways to associate policies with L2 or L3 interfaces used as service SAPs, for example, from the service creation form or the port properties form. This sample modifies an existing L2 interface for an existing VPLS.

i Choose Manage→Service→Services from the 5620 SAM main menu. The manage services form opens.

ii Set the filters and click on the Search button. A list of filtered services appears.

iii Select the service and click on the Properties button. The service form opens.

iv Click on the L2 Access Interfaces tab button.

v Choose an interface and click on the Properties button. The L2 interface edit form opens.

vi Click on the QoS tab button.

vii Configure the parameter. Use the Select button to set the Ingress Policy to Premium service access ingress policy. The policy ID and displayed name appear.

viii Click on the Schedulers tab button.

ix Configure the parameter. Use the Select button to set the Ingress Scheduler to High QoS. The displayed name appears.

x Click on the Apply button to save the changes. Confirm the action.

61 — Queue groups

61.1 Queue group overview

Queue groups are objects created on access or network Ethernet port that allow SAP or IP interface forwarding classes to be redirected from standard queue mapping to a shared queue. Access ingress ports support a single queue group for each ingress port. Access egress and network egress ports support the creation of multiple queue groups.

Queue Group Template policies

Queue Group Template policies allow you to define the queuing and parenting structure for queue groups on Ethernet ports. The policy defines the number and types of queues within the port queue group, and provides the default queue parameters.

See "Queue Group Template policies" in section 44.1 for more information.

Port queue groups

The port queue group contains the queue groups that are created based on the queue IDs defined within the associated Ingress/Egress Queue Group Template policies. Port queue groups are supported on Ethernet ports and can be created on ports within a LAG. Port queue groups are not supported on HSMDA Ethernet ports and VSM MDAs. Network egress queue groups are not supported on the following IOM-1 cards:

- IOM-10 G
- IOM-20 G
- IOM-20 G-B

You can create a port queue group after creating an Ingress/Egress Queue Group Template policy.

Note — You must use the same name for the port queue group and Ingress/Egress Queue Group Template policy.

LAGs

When a port queue group is created on a LAG, the group is individually instantiated on each link in the LAG. The queue parameters for a queue within the queue group are used for each port queue.

You can create, modify, or delete a port access ingress, access egress, or network egress queue group on the primary port of the LAG. (The primary port is the port with the lowest port ID.) The NE automatically replicates the create, modify, or delete action for the queue group on all other ports within the LAG.

Note — The 5620 SAM does not allow you to create, modify, or delete an Access Ingress, Access Egress, or Network Egress queue groups on non-primary ports.

When you add a port to a LAG, the port must use the same access ingress, access egress, or network egress queue groups as the existing ports on the LAG. To ensure this requirement for the port, the 5620 SAM implements the following sequential comparison:

- number of queue groups
- queue group names
- number of queue overrides
- individual parameters

Note — Alcatel-Lucent recommends that you add all required ports to the LAGs before the configuration of the port queue group.

Access SAP forwarding class-based redirection

Typically, each SAP has dedicated ingress and egress queues that are only used by that specific SAP. Individual SAP queuing requires a more complex provisioning model to configure the SAPs ingress and egress SLAs. The configuration requires service awareness at the aggregation locations in the network. There are cases where individual SAP queuing is not preferred. In these cases, you can use a shared queue or an individual port queue model. You can configure a shared queue by creating access ingress and access egress queue groups, and mapping the SAPs forwarding classes to the queues within the queue group.

You can configure forwarding class redirection on a SAP to a queue group queue ID using the Access Ingress /Egress QoS policy. In each policy, the forwarding class to queue ID mapping can specify a queue group name.

Table 61-1 describes a sample workflow to configure an Access Ingress/Egress SAP forwarding class-based redirection.

Table 61-1 Sample configuration for a forwarding class-based redirection on a Access Ingress/Egress SAP

Component	Description
Ingress/Egress Queue Group Template policy	1. Create a new global Ingress/Egress Queue Group Template policy. To create an Ingress Queue Group Template Policy, see Procedure 44-21. To create an Egress Queue Group Template Policy, see Procedure 44-22.
	2. Distribute the global Ingress/Egress Queue Group Template policy to the NEs. To distribute the policy, see Procedure 43-1.
Port Ingress/Egress Queue Group	3. Create an Ingress/Egress Queue Group on the Ethernet Access port configuration form. To create an Access Ingress/Egress Queue Group on an Ethernet access port, see Procedure 17-61.

(1 of 2)

Component	Description
Access Ingress/Egress QoS policy	4. Create a new or modify an existing global Access Ingress/Egress QoS policy with the forwarding class mapped to the Queue Group Queue ID. The Queue Group Queue ID must be included in the Queue Group Template policy. To create an Access Ingress QoS policy, see Procedure 44-1. To create an Access Egress QoS policy, see Procedure 44-3.
	5. Distribute the global Access Ingress/Egress QoS policy to the NEs. To distribute the policy, see Procedure 43-1.
SAP	6. On the SAP configuration, assign the Access Ingress/Egress QoS policy to the SAP bound to the port on which the Access Ingress/Egress Queue Group was created in step 3. **L2 access interface** To assign an Access Ingress/Egress QoS policy to a SAP on a VLL, see Procedure 67-11. To assign an Access Ingress/Egress QoS policy to a SAP on a VPLS, see Procedures 68-3, 68-13, and 68-14. **L3 access interface** To assign an Access Ingress/Egress QoS policy to an L3 access interface on an IES, see Procedure 70-1. To assign an Access Ingress/Egress QoS policy to an L3 access interface on a VPRN, see Procedure 71-2. **SAP** To assign an Access Ingress/Egress QoS policy to a SAP on an IES, see Procedure 70-8. To assign an Access Ingress/Egress QoS policy to a SAP on a VPRN, see Procedure 71-11.

(2 of 2)

Network IP interface forwarding class-based redirection

You can create queue groups on egress network ports to provide network IP interface queue redirection. A single set of egress port-based forwarding class queues are available by default, and all IP interfaces on the port share the queues. The creation of a network queue group allows one or more IP interfaces to selectively redirect forwarding classes to the group to override the default behavior.

The redirection of the egress forwarding class on an IP interface to an egress queue group queue ID is provisioned using the Network policy. The actual queue group name can be specified when the Network Policy is applied to the IP interfaces.

You can configure dedicated queues for each IP interface using network egress queue groups.

Table 61-2 describes a sample workflow to configure a network IP interface forwarding class-based redirection.

Table 61-2 Sample configuration for a forwarding class-based redirection on a network IP interface

Component	Description
Egress Queue Group Template policy	1. Create a new global Egress Queue Group Template policy. To create an Egress Queue Group Template policy, see Procedure 44-22.
	2. Distribute the global Egress Queue Group Template policy to the NEs. To distribute the policy, see Procedure 43-1.
Port Egress Queue Group	3. Create an Egress Queue Group on the Ethernet network port configuration form. To create an Egress Queue Group on an Ethernet network port, see Procedure 17-61.
Network policy	4. Create a new or modify the existing global Network policy with the forwarding class mapped to the Queue Group Queue ID. The Queue Group Queue ID must be included in the Egress Queue Group Template policy, which is specified when the network policy is applied to the IP interface. To create a network policy, see Procedure 44-6.
	5. Distribute the global Network policy to the NEs. To distribute the policy, see Procedure 43-1.
Network interface	6. On the Network interface configuration form, assign the Network policy and the Queue Group Template Policy to the network interface. The network egress queue group must be created on the port to which the network interface is bound. The network egress queue group must use the same name as the selected Queue Group Template policy. To assign a Queue Group Template Policy to a network interface, see Procedure 27-4.

Configuration validation rules

Table 61-3 describes the validation rules that are enforced for NE queue group configurations.

Table 61-3 Validation requirements for queue group configurations

Component		Validation action
Ingress Queue Group Template policy	Queue deletion	The deletion is blocked if there is an Access Ingress QoS policy with a forwarding class that is associated with the queue ID. The deletion can be blocked by the 5620 SAM or the NE. You can use the name binding list to verify dependencies.
	Policy deletion	The deletion is blocked if there is an Access Ingress QoS policy with a forwarding class that is associated with the policy.

(1 of 3)

Component		Validation action
Egress Queue Group Template policy	Queue deletion	The deletion is blocked if there is an Access Egress QoS policy with a forwarding class that is associated with the queue ID. The deletion can be blocked by the 5620 SAM or the NE. You can use the name binding list to verify dependencies.
		The deletion is blocked if there is a Network policy with a forwarding class that is associated with the queue ID.
	Policy deletion	The deletion is blocked if there is an Access Egress QoS policy with a forwarding class that is associated with the policy.
		The deletion is blocked if there is a network IP interface associated with the policy.
Port queue groups	Port Access Ingress Queue Group deletion	The deletion is blocked if there is an Access Ingress QoS policy, applied to the SAP, with a forwarding class that is associated with the port queue group. The SAP is directly or indirectly bound to the port by a LAG associated with the port queue group.
	Port Access Egress Queue Group	The deletion is blocked if there is an Access Egress QoS policy, applied to the SAP, with a forwarding class that is associated with the port queue group. The SAP is directly or indirectly bound to the port by a LAG associated with the port queue group.
	Network Egress Queue Group	The deletion is blocked if there is a network IP interface that is directly or indirectly bound to the port by a LAG associated with the port queue group.
Access SAP forwarding class-based redirection	Access Ingress QoS policy	The Queue Group name must exist as an Ingress Queue Group Templates policy.
		The Queue ID must exist within the associated Ingress Queue Group Templates policy with appropriate queue type.
		Only one unique Queue Group may be referenced within one Access Ingress QoS policy.
		The current Access Ingress QoS policy should not be applied to the SAPs on a non-Ethernet port or an Ethernet port where the specified Access Ingress Queue Group does not exist.
		The current Access Ingress QoS policy should not be applied to a SLA Profile policy.
	Access Egress QoS policy	The Queue Group name must exist as an Egress Queue Group Templates policy.
		The Queue ID must exist within the associated Egress Queue Group Templates policy.
		The current Access Egress QoS policy should not be applied to the SAPs on a non-Ethernet port or an Ethernet port where the specified Access Egress Queue Group does not exist.
		The current Access Egress QoS policy should not be applied to a SLA Profile policy.
	Access Ingress/Egress QoS policy assignment	When an Access Ingress/Egress QoS policy with a forwarding class redirection to a Queue Group Queue ID is applied to a SAP, the following configurations are verified: • The Queue Group specified in any forwarding class redirection must exist as an Access Ingress/Egress Queue Group on the port associated with the SAP • The Access Ingress/Egress QoS policy with Queue Group specified cannot be applied to SLA Profile policy

(2 of 3)

Component		Validation action
Network IP Interface forwarding class-based redirection	Network policy	The specified queue ID must exist within the Egress Queue Group Templates policy for all IP interfaces where the Network policy is applied. If the Network policy is currently applied to any IP interfaces without an explicit Network Egress Queue Group specified, the configuration fails.
		The following configurations are verified when the Network policy is applied to a network IP interface: • The network policy with a redirected queue group cannot be applied to the network IP interface without a port binding. • The redirected queue group name must exist as a Network Egress Queue Group on the port or LAG associated with the IP interface. • The queue ID for the redirected queue group in the associated Network policy must exist within the associated Egress Queue Group Templates policy.

(3 of 3)

Statistics

The packets sent to the queue of a SAP are statistically tracked by a set of counters associated with the queue group queue, not the SAP counters. The tracking occurs when a forwarding class is redirected to an ingress or egress port queue group queue.

On a network interface, the counter sets are created for each egress IP interface, not for each egress queue. The same counter set is used when a forwarding class for an egress IP interface is redirected from the default egress port queue to a queue group queue.

Workflow to configure statistics collection

Table 61-4 describes the configuration workflow to enable the collection of queue groups statistics.

Table 61-4 Statistics collection for queue groups

Component	Configuration
1. Accounting policy	Configure the Type parameter on the Accounting Policy form to collect one of the following statistics options: • Combined Queue Group • Queue Group Octets • Queue Group Packets To configure a policy that specifies the type and frequency of accounting statistics collection, see Procedure 4-2.
2. Port queue group	Enable the Collect Accounting Statistics parameter on the port queue group - Physical Port form. To create an Access Ingress/Egress Queue Group on an Ethernet access port, see Procedure 17-61.

See the *5620 SAM Statistics Management Guide* for information about managing statistics collection and to view a list of the MIB counters that are available for collection using the 5620 SAM.

62 — Virtual ports

62.1 Virtual port overview

A 7750 can act as a Broadband Network Gateway (BNG), fairly distributing bandwidth among the subscriber host sessions by accounting for the packet encapsulation overhead and ATM bandwidth expansion for each type of broadband session. In this way, subscriber packets are less likely to be dropped downstream in the DSLAM DSL port. Furthermore, the BNG shapes the aggregate rate of each subscriber and the aggregate rate of all subscribers destined to a given DSLAM to prevent congestion of the DSLAM.

In the BNG application, when a set of per FC queues are applied to each subscriber host context, the host per FC queue packet rate is overridden by the rate provided in the Radius access-accept message. This rate represents the ATM rate that will be seen on the last mile and includes the encapsulation offset and the per packet expansion due to ATM segmentation into cells at the BSAN.

In order to enforce the aggregate rate of each destination BSAN, a virtual port must be configured. Virtual ports are scheduling nodes that operate like port schedulers, with the exception that multiple virtual ports can be created on the egress context of an acess/hybrid Ethernet port. A virtual port and a port scheduler cannot exist simulatenously on a single port.

Virtual ports can be created on a port that is a member of a LAG. When a virtual port is created, modified, or deleted on the primary port of a LAG, this action is replicated on all other ports within the LAG. These actions can only be perfoemd on the primary port. When a port is added to a LAG, it must have the same virtual ports defined as the existing ports on the LAG. The name of a virtual port is local to the port on which it is applied, but must be the same for all member ports of a LAG.

Virtual ports are supported on Ethernet ports on IOM3/IMM in 7750, 7750 sparrow, and 7450.

Virtual ports are not supported on SR1 or ESS1 platforms, HSMDA Ethernet ports, or VSM MDA.

See Procedure 62-1 for more information.

SLA Profiles

A subscriber host queue with the port-parent option enabled can be scheduled within the context of a port scheduler policy associated with a port or a virtual port. To specify that a subscriber host queue with the port-parent option enabled be scheduled within the context of a virtual port, the Scheduler Type parameter must be set to Virtual port when configuring an SLA Profile.

See Procedure 64-3 for more information.

Subcriber Profiles

The subscriber aggregate rate is adjusted to account for the fixed offset and per packet variable expansion of the last mile for the specific session used by the subscriber host. The adjustment is based on the average frame size.

See Procedure 64-2 for more information.

Procedure 62-1 To configure virtual ports

1 Configure an SLA Profile, as described in Procedure 64-3.

2 Configure a Subscriber Profile, as described in Procedure 64-2.

3 Perform one of the following:

a Create a virtual port using the navigation tree, as described in Procedure 62-2.

b Create a virtual port using the Port QoS form, as decribed in Procedure 62-3.

Procedure 62-2 To create virtual ports using the navigation tree

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view.

2 Right-click on an access/hybrid Ethernet port in the Equipment view and choose Properties from the contextual menu. The Physical Port (Edit) form opens with the General tab displayed.

3 Click on the Egress Scheduling Virtual Port tab button.

4 Click on the Add... button. The Egress Scheduling Virtual Port (create) form opens with the General tab displayed.

5 Configure the parameters:

- Name
- Description

6 Click on the Select button in the Port Scheduler Policy panel to choose a Port Scheduler Policy. The Select Port Scheduler Policy form opens.

7 Select a Port Scheduler Policy and click on the OK button. The Select Port Scheduler Policy form closes and the Egress Scheduling Virtual Port (create) form reappears with the Port Scheduler Policy information displayed.

8 Click on the Host Matching tab button.

9 Click on the Add... button. The Host Matching form opens.

10 Configure the Destination String parameter.

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The Egress Scheduling Virtual Port (create) form reappears with the Destination String information displayed.

13 Click on the OK button. A dialog box appears.

14 Click on the OK button. The Physical Port (edit) form reappears with the Egress Scheduling Virtual Port information displayed.

15 Click on the OK button. A dialog box appears.

16 Click on the Yes button. The Physical Port (edit) form closes.

Procedure 62-3 To create virtual ports using the Port QoS form

1 Choose Manage→Equipment→Port QoS from the 5620 SAM main menu. The Port QoS list form opens.

2 Select Egress Scheduling Virtual Port from the object type drop-down list.

3 Click on the Create button and choose Create Virtual Port(s). The Egress Scheduling Virtual Port (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Name
- Description

5 Click on the Select button in the Port Scheduler Policy panel to choose a Port Scheduler Policy. The Select Port Scheduler Policy form opens.

6 Select a Port Scheduler Policy and click on the OK button. The Select Port Scheduler Policy form closes and the Egress Scheduling Virtual Port (create) form reappears with the Port Scheduler Policy information displayed.

7 Click on the Host Matching tab button.

8 Click on the Add... button. The Host Matching form opens.

9 Configure the Destination String parameter.

10 Click on the Targeted Physical Ports tab button.

11 Click on the Add... button. The Select Site form opens.

12 Click on the Search button. The form displays a list of sites.

Note — The count displayed on the form reflects the total number of found ports and may not align with the number of applicable ports displayed in the list.

13 Select a site in the list and click on the OK button. The Select Site form closes and the Egress Sheduling Virtual Port (create) form reappears with the site information displayed.

14 Click on the OK button. The Egress Scheduling Virtual Port (create) form closes and the Port QoS list form reappears.

15 Close the form.

Procedure 62-4 To copy virtual ports

1 Choose Manage→Equipment→Port QoS from the 5620 SAM main menu. The Port QoS list form opens.

2 Select Egress Scheduling Virtual Port from the object type drop-down list.

3 Click on the Search button. The form displays a list of virtual ports.

4 Select a virtual port in the list and click on the Copy... button. The Egress Scheduling Virtual Port (create) form opens with the virtual port's values populated.

5 Click on the Targeted Physical Ports tab button.

6 Click on the Add... button. The Select Site form opens.

7 Click on the Search button. The form displays a list of sites.

8 Select one or more sites in the list and click on the OK button. The Select Site form closes and the Egress Sheduling Virtual Port (create) form reappears with the site information displayed.

9 Click on the OK button. The Egress Scheduling Virtual Port (create) form closes and the Port QoS list form reappears.

10 Close the form.

63 — Customer configuration and management

63.1 Customer configuration and management overview

The 5620 SAM allows you to manage customers.

An end user is the recipient of application content that is delivered through a service. The service is a means of transport for the application content and is owned by a service customer. For example, an end user subscribes to a high-speed Internet access service, and the Internet access service is owned by a service provider who is a service customer of the network provider. The 5620 SAM provides only customer management, not end-user management. Customers were called subscribers in earlier versions of 5620 SAM.

On the General tab of a customer management form, you can configure basic customer information. From the other tabs on the form, you can configure and monitor service sites, templates, and aggregation schedulers for a customer.

Each customer is associated with an ID that is assigned when the customer account is created. When configuring a service, you can use the ID or the listed name of the customer to associate a customer with a service.

A customer can own more than one service, but an individual service is owned by only one customer. Two or more services can be joined to form a composite service. The individual services that comprise the composite service can be owned by different customers. Customers that own services participating in a composite service are associated with the composite service.

63.2 Workflow to configure and manage customers

1 Create customers that will purchase and use services.

- Configure or modify key customer contact and billing information.
- Assign or associate equipment or resources to customers, as appropriate.

2 Create or modify services, such as VPLS, VPRN, or VLL, that are associated with the customer.

3 Monitor or troubleshoot customers based on SLAs between the customer and the service provider.

- Retrieve customer information and contact the customer when service problems or maintenance windows occur.
- Perform diagnostics as appropriate to troubleshoot problems.

63.3 Customer configuration and management procedures

The following procedures describe how to configure and manage customers.

Procedure 63-1 To create a customer

1 Choose Manage→Service→Customers from the 5620 SAM main menu.

2 Click on the Create button. The Customer (Create) form opens with the General tab displayed. The General tab shows contact and billing information.

3 Configure the parameters.

- Auto-Assign ID
- ID
- Name
- Description
- Address
- Phone Number
- Contact
- Email

The information in the General tab is used to create a database of customer information, including contact information, so that the customer can be contacted if there is a service or equipment problem.

4 Click on the Apply button to save the customer information.

Procedure 63-2 To modify and manage customer information

Use this procedure to view and modify an inventory of all the services, interfaces, circuits, and other information that is associated with a customer.

1 Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.

2 Search for the customer whose information you want to change. The search results are displayed in the bottom panel of the form.

3 Choose the customer and click on the Properties button. The Customer (Edit) form opens.

4 View or modify the information for the customer.

Each tab lists parameters you can view or modify, or functions that you can perform, related to customer management.

- The General tab lists the ID, the customer name, and contact information.
- The Sites tab lists PE devices used by the customer.
- The Aggregation tab lists aggregation schedulers defined for the customer. See chapter 44 for information about creating aggregation schedulers.
- The Associated Templates tab lists service templates used to create services for the customer.

5 Modify customer information as appropriate:

a To modify text in the General tab:

i Make the changes in the appropriate fields and click on the OK button. A dialog box appears.

ii Click on the Yes button. The Customer (Edit) form closes.

b To modify site or template information for the customer:

i Click on the appropriate tab button on the Customer (Edit) form.

ii Select the object in the list for which you want to modify information.

iii Click on the Properties button. The configuration form for the object opens.

Caution — Ensure configuration changes do not affect customer services. Use the Turn Down button to turn down a service before making any changes that may affect customer traffic.

iv Modify the information on the configuration form as required and click on the OK button. The changes are saved and the object configuration form closes.

Procedure 63-3 To delete customers

Note — You cannot delete customers that have associated services

1 Choose Manage→Service→Customers from the 5620 SAM main menu. The Manage Customers form opens.

2 Search for the customer that you want to delete. The search results are displayed in the bottom panel of the form.

3 Choose the customer from the list and click on the Delete button. A Confirm dialog box appears.

Caution — Removing a customer deletes all information associated with the customer. Ensure that the correct customer has been selected.

4 Perform one of the following:

a Click on the No button to avoid deleting the customer. The Confirm dialog box closes.

b Click on the Yes button. The customer is deleted from the 5620 SAM database.

Procedure 63-4 To view a service map for a customer

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose Service (Service Management) from the object drop-down list.

3 Use the filter for the Customer Name column to filter the list results.

4 Click on the Search button. A list of services matching the filter criterion appears.

5 Choose a service from the list and click on the Topology View button. A dialog box appears.

6 Click on the Yes button. The Service Topology - *Service Name* form opens.

7 Scroll the map to view the topology of the service and the devices used for the service.

8 Click on the Close button to close the map.

Procedure 63-5 To list customer services

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens with Service (Service Management) selected in the filter list.

2 Use the filter for the Customer Name column to filter the list results.

3 Click on the Search button. A list of services matching the filter criterion appears.

64 — Residential subscriber management

64.1 Residential subscriber management overview

The emergence of residential broadband networks and the availability of multiple service offerings, such as triple play applications create a requirement for greater service differentiation and control at the level of the individual service recipient. The 5620 SAM provides functionality for the efficient provisioning of access, QoS, and security features on IES, VPLS, and VPRN for residential subscribers, while service-level customization for end users is available using systems such as the Alcatel-Lucent 5750 SSC.

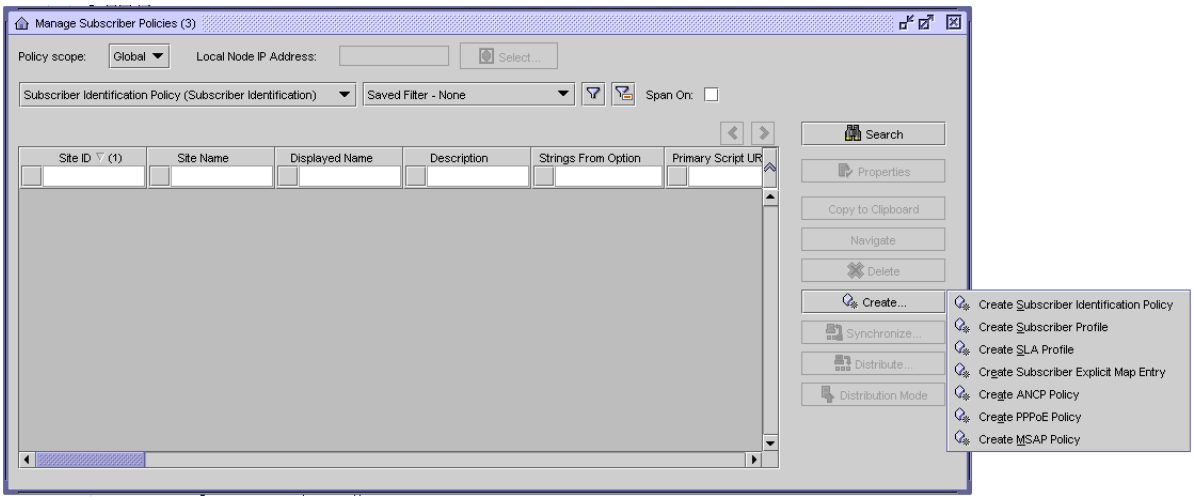
In the context of the 5620 SAM, a residential subscriber, sometimes called a subscriber, is a unique identifier that associates a group of end-user devices with policies. A subscriber can be associated with multiple SAPs on multiple NEs, and a customer can be associated with multiple subscribers.

A subscriber host, sometimes called a host, is an end-user device, such as a computer, VoIP telephone, or set-top box, that connects to the provider network and receives the service traffic. Hosts with the same subscriber identifier share overall HQoS and accounting characteristics as defined in a customer SLA, but may use QoS policies and queues that differ by the type and class of service offering.

Residential subscriber management supports service delivery models in a routed or bridged configuration, such as one VLAN per host, one VLAN per application, one VLAN for all applications, and one VLAN per service provider per application.

The 5620 SAM supports the creation and configuration of residential subscriber management components using configuration forms. Figure 64-1 shows the Manage Subscriber Policies form with the Create menu displayed. The search function returns global or local policy and profile instances, according to the specified scope.

Figure 64-1 Manage Subscriber Policies form



For detailed NE-specific residential subscriber management information, see the *7450 ESS OS Triple Play Guide* and the *7750 SR OS Triple Play Guide*.

Configuration

Configuring residential subscriber management on the 5620 SAM involves the creation and configuration of the following components, depending on the service delivery model:

- subscriber identification policy
- subscriber profile
- SLA profile
- subscriber explicit map
- ANCP policy
- PPPoE policy
- MSAP policy

A host requires subscriber-profile and SLA-profile associations to gain access to the network. Profiles define service attributes for hosts such as scheduling, accounting, security, and traffic prioritization by application type. A profile uses existing 5620 SAM policy definitions and allows the customization of policy parameters using override values.

A 5620 SAM user that is assigned the administrator, subscriber management, service management, or policy management scope of command role can perform all residential subscriber management functions, such as managing profile or DHCP-lease information.

The 5620 SAM allows the configuration of multiple components in one operation, but limits configuration to those parameters that are not specific to a component. For example, when a policy is applied to multiple profiles, the 5620 SAM removes pre-existing policy override values in the profiles.

Migrating to the TPSDA model

The following residential subscriber management functionality facilitates the migration of hosts from SAP-based aggregation to the TPSDA model. You can:

- Associate a subscriber with a SAP by using the SAP identifier as the subscriber identification string. The existing hosts on a SAP can then be automatically associated with a subscriber.
- Rename a subscriber. This changes the subscriber identification string for all hosts and facilitates a move from a default subscriber identification string to a string that complies with a particular naming scheme.
- Configure an intermediate destination identifier, such as a DSLAM name, for a static host and obtain the identifier from the Option 82 information in a DHCP packet. This functionality enables the listing of the hosts for a specific DSLAM and facilitates interworking with other TISPAN components such as the 5750 SSC.
- Configure a default subscriber identification string for the hosts on a SAP. This enables residential subscriber management functionality without the use of a subscriber identification policy or RADIUS authentication. This default string is associated with hosts when a string is not available from another source.
- Interpret an SLA profile string or subscriber profile string from a host as the profile name when a profile with a matching profile string is not found. This eliminates the need to map a profile string to a profile.

Configuration requirements

The following must be true before you can enable residential subscriber management on a SAP or deploy a profile to an NE.

- The NE must be a 7450 ESS, 7750 SR, or 7710 SR.
- For dynamic hosts on the SAP:
  - DHCP snooping is enabled on the upstream SAP or SDP.
  - For IES, DHCP relay is enabled on the downstream SAP.
- The NE has sufficient resources for creating the SLA profile instances, queues, and schedulers.
- For new or existing static hosts on the SAP:
  - Anti-spoofing on the SAP is configured with at least IP matching criteria.
  - A subscriber identification string is assigned.
  - A subscriber profile is assigned.
  - An SLA profile is assigned.
  - An IP address is assigned.

Functional description

When residential subscriber management on a SAP is enabled, a dynamic or static subscriber host that connects to the SAP requires a subscriber identification string to associate the host with a subscriber instance on the NE, or network access is denied. A subscriber identification string uniquely identifies a subscriber in the 5620 SAM.

You cannot delete an active component of a residential subscriber management configuration.

Enabling residential subscriber management on a SAP does not affect an existing dynamic host on a SAP until the host DHCP lease expires, at which point a subscriber identification policy manages lease renewal. Static hosts require the provisioning of a subscriber identification string for continued network access.

The 5620 SAM identifies the subscriber for a dynamic host by obtaining a subscriber identification string from a source such as the following:

- information that the host passes in the Option 82 field of a DHCP packet
- a RADIUS server
- the local user database

A static host requires explicit provisioning on the 5620 SAM that includes the association of a subscriber identification string.

You can optionally specify a default subscriber identification string for a SAP. You can enter the string or configure the 5620 SAM to use the SAP ID as the string.

The 5620 SAM deploys the components associated with a subscriber, such as policies and profiles, to an NE when one of the following occurs:

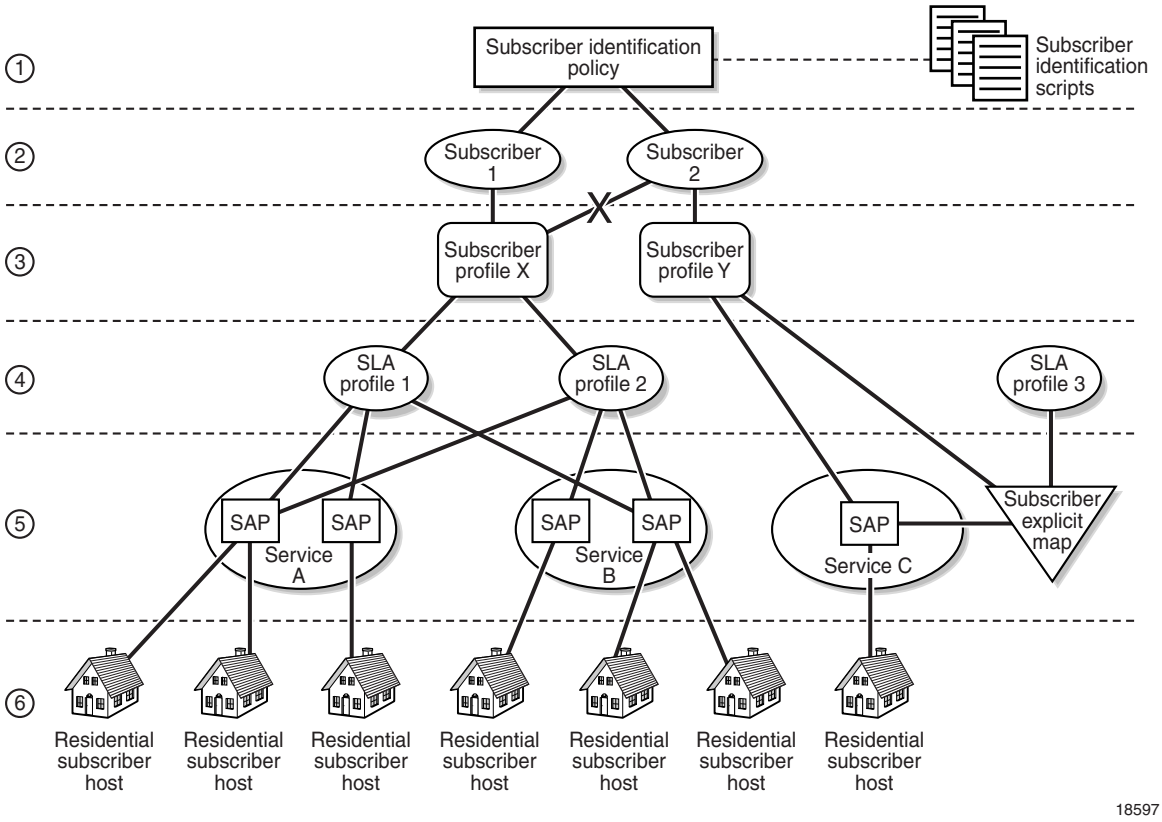
- The deployment of a subscriber identification policy with profile specifications
- The provisioning of the first static host for the subscriber on a SAP
- The provisioning of a Capture SAP with an MSAP Policy to automatically create an MSAP; see Managed SAP (MSAP) for more information

After the 5620 SAM deploys the subscriber and SLA profiles, the NE creates the queues, ACL filters and HQoS schedulers specified in the profiles. The NE ignores pre-existing queue or ACL filter policies on a SAP when subscriber management is enabled on the SAP.

The 5620 SAM maintains a record of subscribers that are deleted at the NE. Disconnected subscribers are marked as inactive. Subscriber information is retained in an inactive state in the Residential Subscriber and Residential Subscriber Instance views. In this way, the 5620 SAM treats the setup and teardown of a residential subscriber simply as a change of state, thereby avoiding the load imposed by object creation and deletion.

Figure 64-2 shows a conceptual model of the main component relationships in residential subscriber management. The model does not represent a specific type of service or service delivery mechanism and does not show all possible component configurations.

Figure 64-2 Residential subscriber management component relationships



As shown in Figure 64-2, there is a one-to-one relationship between a subscriber and a subscriber profile and a many-to-many relationship between subscriber profiles and SLA profiles. A subscriber profile or an SLA profile can apply to multiple SAPs or NEs, and can be specified as the default profile for the SAP or the NE.

Table 64-1 lists where to find configuration information for the components shown in Figure 64-2. The numbered levels segregate components for clarity only.

Table 64-1 Residential subscriber management components

Level	Component	Description	For more information, see	Procedure
1	Subscriber identification policy	Associates a dynamic host with a subscriber	"Subscriber identification policies" in this section	64-1
	Subscriber identification script	Parses DHCP Option 82 field to extract subscriber identification for a host, and optional profile, ANCP, and intermediate destination identification strings.	"Subscriber identification policies" in this section	64-27
2	Subscriber	Unique identifier that associates a group of subscriber hosts with policies	"Residential subscriber management overview" in this chapter	64-35
2	Subscriber instance	An instantiation of a subscriber on an NE	"Residential subscriber management overview" in this chapter	64-36
3	Subscriber profile	Names existing ingress and egress scheduler policies and an accounting policy for use by all hosts of a subscriber	"Subscriber profiles" in this section	64-2
4	SLA profile	Names existing QoS policies to define the traffic shaping for different classes of service within an application such as HSI, VoIP, VoD, or BTV Names existing ACL policies to filter the ingress and egress traffic	"SLA profiles" in this section	64-3
5	Subscriber explicit map	Lists subscriber identifiers and the associated SLA and subscriber profiles	"Subscriber explicit maps" in this section	64-15
6	Residential subscriber host (static)	A device such as a computer or set-top box that receives service traffic using a fixed IP address	"Static hosts and residential subscriber management" in this section	64-24 68-1, 70-1, and 71-1 access interface anti-spoofing configuration steps
	Residential subscriber host (dynamic)	A device such as a computer or set-top box that receives the service traffic using a temporarily assigned IP address	"Subscriber identification policies", "Subscriber profiles", "SLA profiles", "Subscriber explicit maps", Managed SAP (MSAP), and "PPPoE sessions"in this section	64-31
5	Local DHCP server and PPPoE group interface	A local user database is created and associated to a local DHCP server and PPPoE group interface configuration	"Local DHCP servers" in this section	64-17 64-34 71-1 70-8

The 5620 SAM treats residential subscriber management components like policies. Depending on the distribution mode configuration of a local instance, when you modify a global component using the 5620 SAM, all local instances of the residential subscriber management component on the associated NEs can be updated. The Local Definitions tab of a component management form lists the local instances of the component.

Global residential subscriber management components are created in draft mode. This allows operators to verify the configuration before they distribute it to the network elements. See chapter 43 for information about global and local policy instances and policy distribution modes.

The maximum number of subscribers that use a SAP is configurable. When a SAP is limited to one subscriber, you can specify the treatment of traffic that does not match the subscriber profile, such as BTV traffic, which uses an IP address in the multicast range as the destination address. During single-subscriber SAP configuration, the 5620 SAM operator specifies whether to allow non-profile traffic and specifies the SLA and subscriber profiles to use for non-profile traffic, if it is allowed.

The 5620 SAM supports the collection of accounting statistics for subscriber instances. The 5620 SAM uniquely identifies a subscriber instance by using a combination of the subscriber identifier and the NE identifier.

Subscriber identification policies

Subscriber identification policies apply to SAPs and associate dynamic residential subscriber hosts with NE subscriber instances. Hosts that use the same subscriber identifier, called a subscriber identification string, belong to the same subscriber and receive common general HQoS and accounting treatment as defined by the customer SLA specifications in a subscriber profile. Hosts from multiple SAPs can belong to the same subscriber, but for HQoS scheduling purposes, all hosts of a subscriber must be active on the same IOM.

When a dynamic residential subscriber host requests an IP address using DHCP, the host can include a subscriber ID string and optional profile ID strings in the Option 82 field of the DHCP packet. If the request is approved by a DHCP server, the NE obtains the subscriber ID string for the host from the Option 82 information in the returning ACK message. The subscriber ID string is a match criterion for the assignment of SLA and subscriber profiles to the host unless profile ID strings are explicitly encoded in the DHCP option information by the host or configured as SAP default profiles. You can also configure a default subscriber ID string on a SAP.

Note — If adding Option 82 information to a DHCP relay packet causes the packet to exceed the DHCP relay maximum of 1500 bytes, the NE forwards the DHCP request without the Option 82 information. For this reason, short strings can be used as aliases for profile names.

A subscriber identification policy includes:

- URLs for subscriber identification scripts
- subscriber profile map
- SLA profile map

Entries in the subscriber and SLA profile maps are optional and are used for the direct assignment of profiles to hosts when hosts include profile ID strings in the DHCP Option 82 field.

Although the 5620 SAM is installed with no default subscriber identification policy, an operator can create a subscriber identification policy and designate it as the default policy by giving it the case-sensitive name “default”.

Subscriber identification scripts

A URL in a subscriber identification policy points to the location of a subscriber identification script that an NE uses to parse DHCP option information. During initialization, an NE downloads scripts from the URLs that are specified in the applied subscriber identification policies. An NE can store a maximum of four subscriber identification policies; each policy can contain up to three scripts.

A subscriber identification script derives the mandatory subscriber ID string, as well as a DSLAM identifier and optional profile ID strings, from the DHCP option information.

The 5620 SAM operator assigns a priority to each script in a subscriber identification policy. Only the operationally enabled script with the highest priority is active. If an NE encounters an error in a script or cannot find a script at the specified location, the NE marks the URL as operationally down, raises an alarm, and attempts to use the script that is next in priority. The script-related alarms that the 5620 SAM raises against the local instance of a subscriber identification policy are:

- warning alarm when the primary URL is operationally up but a lower-priority URL is operationally down
- major alarm when the primary script is operationally down but one of the other scripts is operationally up
- critical alarm when all scripts are operationally down

A modification to a subscriber identification script or URL takes effect only after the URL is administratively disabled and then re-enabled, which causes an NE to reload the script. Replacing or modifying a subscriber identification script or a URL can be service-affecting if not done properly. To avoid a service disruption when you modify a subscriber identification script or URL, perform Procedure 64-27.

Local DHCP servers

5620 SAM supports configuring local DHCP servers on a 7750 SR, 7710 SR, and the 7450 ESS. The local DHCP server leases IP addresses to clients in the network. Options are configured to define the IP address properties, such as, the length of time an IP address is active and which DNS server must be used. A local user database is used to authenticate and authorize clients requesting IP addresses from the local DHCP server. If the local DHCP server does not use the local user database, the server can use the GI address to assign free IP addresses, however it is not possible to configure match or authentication parameters.

Three applications are targeted for the local DHCP server.

- Subscriber aggregation using a single NE or TPSDA.
- Business services running VPRN and locally attached to the host can request and obtain IP addresses directly from the server.
- The DHCP server identifies an IP request from a PPPoE client and provides an IP address and options.

DHCP servers can be integrated with Enhanced Subscriber Management for DHCP and PPPoE clients. A local DHCP server can be created in the routing instance window or VPRN service site window. A local DHCP server created in the VPRN service site can be associated with the L3 access interface on a VPRN service only. A local DHCP server created in the routing instance window can be associated with a network interface or L3 access interface on IES.

ARP host

You can use the 5620 SAM to configure and retrieve ARP hosts on a Release 7.0 or later 7750 SR. ARP hosts are a subtype of enhanced subscriber host objects. The creation of the object is triggered by the reception of ARP messages from end-user devices. ARP hosts can be configured as an alternative to DHCP subscriber hosts or PPPoE sessions.

ARP host configuration can be performed on VPLS and MVPLS L2 access interfaces, IES and VPRN group interfaces, and VPRN retailer subscriber interfaces. The configuration includes enabling the functionality, setting the maximum limit of hosts per SAP or interface, and setting the default authentication interval.The configuration must be performed in conjunction with other enhanced subscriber management configuration on these interfaces. ARP hosts can be retrieved from the VPLS, MVPLS, and IES or VPRN SAPs. ARP hosts can also reside on MSAPs.

You can retrieve ARP hosts from the Manage→Residential Subscribers→Manage Residential Subscribers form menu options. See Procedure 64-33 for more information about the persistence and retrieval of subscriber hosts.

Local user database

The 5620 SAM supports configuring a local database on a 7750 SR, 7710 SR, and the 7450 ESS. The local user database is configured and associated with the local DHCP server to provide local authentication. The local DHCP server must have a pool of IP addresses configured, otherwise it is not able to lease IP addresses.

A create local user database configuration form is available from the Manage Residential Subscribers form. Once a local user database is configured, it can be associated with a local DHCP server and PPPoE configuration on a group interface.

When a local user database is not configured, you can use GI addresses to access free IP addresses, however the clients requesting the IP address will not be authenticated.

Subscriber profiles

A subscriber profile defines the aggregate HQoS and accounting characteristics for the hosts of a specific subscriber. During the creation of a subscriber profile, the 5620 SAM operator chooses ingress and egress scheduler policies that apply to all host queues of the subscriber. A subscriber profile permits the optional selection of SLA profiles to override the SLA profiles that are named in the subscriber identification policy.

A subscriber profile can be specified in the following components, which an NE searches in the order shown when it attempts to assign a subscriber profile to a host:

- subscriber explicit map
- subscriber identification policy

A subscriber requires an association with one and only one subscriber profile. If no subscriber profile is associated with a subscriber ID string or explicitly specified by a host, and there is no available default subscriber profile on an NE or on a SAP, the NE rejects the host.

A subscriber profile can include associations to the following policy types:

- ingress scheduler
- egress scheduler
- accounting
- ANCP
- NAT
- host tracking
- RADIUS accounting
- SLA profile map
- ingress QoS
- egress QoS
- HSMDA packet byte offset override
- HSMDA queue override
- ingress and egress scheduler policy parameter overrides
- ingress and egress policer control
- ingress and egress policer control overrides

The 5620 SAM operator can define a default subscriber profile for an NE or a SAP by giving it the case-sensitive name “default” during profile creation. NE and SAP default subscriber profiles apply to hosts for which a subscriber profile is unspecified in the subscriber explicit map and subscriber identification policy.

SLA profiles

An SLA profile defines the resources that an NE assigns to a particular subset of subscriber hosts, such as VoIP telephones or BTV set-top boxes. These resources include network-access and ACL policies. An SLA profile also optionally defines the maximum number of hosts that use the profile and the action taken when the number of hosts reaches the maximum.

An SLA profile can be specified in the following components, which an NE searches in the order shown when it attempts to assign an SLA profile to a host:

- subscriber explicit map
- subscriber profile
- subscriber identification policy

An SLA profile includes:

- access ingress policy association
- access egress policy association
- ingress IP ACL filter policy association
- egress IP ACL filter policy association
- host limit that specifies the maximum number of hosts that use the SLA profile
- access ingress and access egress policy parameter override values
- access ingress and access egress policer override values

The queues in the access ingress and egress policies of an SLA profile must use a scheduler from the scheduler policy in the subscriber profile as their parent scheduler. All hosts that use the SLA profile must be active on the same IOM. When an SLA profile does not name an access ingress or access egress policy, an NE uses the SAP default policy.

A 5620 SAM operator can define a default SLA profile for a SAP. A default SAP SLA profile applies only to hosts for which an SLA profile is unspecified in the subscriber explicit map, subscriber profile, and subscriber identification policy.

Managed SAP (MSAP)

The automatic creation of subscriber hosts in a shared SAP has always been available in the 5620 SAM. However, the most secure mode of operation is the one subscriber per SAP model. In the one subscriber per SAP model, each subscriber is defined in its own VLAN, which requires a lengthy and complex configuration. Automatic SAP creation builds on the authentication mechanisms that the NE supports to provide an automatically created SAP that supports the one subscriber per SAP model. The automatically created SAP is called an MSAP.

You can use the 5620 SAM to configure parameters for the automatic creation of MSAPs (also known as Managed SAPs). MSAP creation employs the use of policies and a SAP template for the creation of a Capture SAP. The automatic creation of an MSAP is enabled from the creation of a Capture SAP. See Automatic MSAP creation process in this section for more information about creating a Capture SAP.

When a Capture SAP is configured, triggering packets initiate RADIUS authentication, which provides a service context. The authentication and the service context for this request creates an MSAP. The MSAP behaves in the same way as a regular SAP but its configuration is not editable. The MSAP is not maintained in the configuration file; however, it can be maintained in a separate persistency file. The MSAP remains active for as long as there are subscriber hosts on the MSAP. See MSAP management in this section for more information about managing the automatically created MSAP.

Note — MSAPs cannot be configured but are reconciled by the 5620 SAM on the NE.

Although MSAPs are not configurable, a user with a Policy Management or Subscriber Management role can create, list, delete, or modify an MSAP Policy to control how the parameters are applied to the MSAP when it is created. The MSAP Policy must be created before you create the Capture SAP so that the policy can be added to the Capture SAP configuration. See Procedure 64-7 for information about how to create an MSAP Policy.

Capture SAPs can be created in VPLS configurations only. MSAPs created by these Capture SAPs can be part of both Routed-CO (IES or VPRN) and VPLS TPSDA configurations. MSAPs for IES and VPRN services are created under group interfaces only. In most cases MSAPs are created for unique subscribers. In architectures that provide service access using a shared SAP, automatic SAP can be used to a limited extent to reduce the configuration needed and allow multiple subscribers to share a SAP. However, if more than one subscriber is allowed and an MSAP has been defined by a host, the installation fails and raises an event if a new host installation attempts to change the MSAP policy.

MSAPs are supported for both HA and dual-homing environments. For dual homing, the MSAP is synchronized to the other NE when the MSAP is created. For both HA and dual-homing environments, both NEs in the configuration must be configured with the same MSAP policy.

Automatic MSAP creation process

A Capture SAP must be defined to trigger the process that automatically creates an MSAP. The Capture SAP is not intended to forward traffic.

Encapsulation for the Capture SAP can be one of:

- dot1q—supports the parameter value 4095, which appears as an asterisk (*)
- Q-in-Q—supports the parameter values 1 to 4095 for the outer encapsulation value and 4095 only for the inner encapsulation value
- LAG—supports the parameter values 1 to 4095

The Capture SAP is used if a more specific match for the dot1q or Q-in-Q tags is not found.

Note 1 — Some providers use a Q-in-Q to represent a service.sub or sub.service SAP. When configured, the full Q-in-Q represents a subscriber.

Note 2 — Multiple leases for the same subscriber are allowed; however, only one MSAP policy is allowed. If an MSAP is defined by a host and a new host installation is attempting to change the policy, the installation fails and raises an event.

The Capture SAP is created in the same way as a regular SAP; however, you must change the SAP Sub Type parameter that appears on the General tab of the L2 Access Interface (Create) form from the default value of Regular to Capture. Capture SAP-specific configuration is performed on the Capture Access Interface tab of the L2 Access Interface (Create) form. In the Capture Access Interface tab you can configure the parameters and apply the PPPoE and MSAP policies that control MSAP creation.

You can create a Capture SAP on any VPLS service on an NE. MSAP creation can be configured to start on receipt of DHCP packets, PPPoE packets, ARP packets, or any combination of DHCP, PPPoE, and ARP packets. After you configure the Capture SAP, every DHCP packet, PPPoE packet, or ARP packet received on the SAP is sent to the CPM, which triggers RADIUS authentication to provide a service context. The MSAP is created in the specified service. Non-triggering packets captured by the Capture SAP are dropped. See Procedure 64-8 for information about how to create a Capture SAP.

The following triggers are supported to initiate MSAP creation:

- DHCP Trigger Packets—DHCP Discover (or Requests if configured) for DHCP clients; the MSAP lifetime is defined by the lease time.
- PPPoE Trigger Packets—PPPoE PADI for PPPoE client; the managed SAP lifetime is defined by the session time. The MSAP is installed after an IP address is provided.
- ARP Trigger Packets—ARP for static-ip hosts; the MSAP lifetime is defined by ARP entry time. Current ARP entry refresh behavior is maintained.

If RADIUS does not provide all of the required information to install the host (for example, RADIUS lacks the IP address), the MSAP is created with a short timer while waiting for the host to be installed. Default SAP polices are available on the NE and will be used if the MSAP policy is not configured.

An MSAP is created with dual-pass (shared) queuing. The SLA-profile of the host may change the queuing later in the process. The MSAP is always created with the default QoS and scheduling.

For MSAPs, the authentication policy is defined in the MSAP policy. Based on the configuration, the system reauthenticates the sessions when they are renewed. If the authentication policy is not used or when only PPPoE is used, the MSAPs, stay active when the session is renewed.

The authentication policy used in the Capture SAP must be the same policy as the policy used for the MSAP. For L3, the authentication policy is defined under the group-interface.

Note 1 — When PPPoE is used with MSAPs, the authentication policy must not use the username for MSAP creation.

Note 2 — The MSAP is not created (and an event is generated) if the group-interface name returned from RADIUS points to a different authentication policy than the policy defined by the Capture SAP.

MSAP management

MSAP management is applied using the MSAP policy. The MSAP policy is used to configure the parameters in the tabs that are available on the Properties forms of the MSAP. The original MSAP policy applied to the Capture SAP is the default Creation MSAP Policy, which is used to configure all of the parameters for the MSAP. You cannot modify an MSAP. However, you can modify the Creation MSAP Policy to make changes to an MSAP.

After MSAP creation, all of the MSAP parameters are read-only, except for the Creation MSAP Policy Re-evaluation parameter on the MSAP Properties tab. The Creation MSAP Policy Re-evaluation parameter allows you to reapply the MSAP policy associated with the local MSAP.

If you need to change an MSAP policy and you are in the Manage Subscriber Policy form, you can choose an MSAP policy, click on the Properties button, make your changes, and click on the Reevaluate MSAPs button to perform an MSAP policy re-evaluation. You can use the MSAP Policy Reevaluate button to update the MSAP policies on a global or local basis.

After an MSAP Policy Re-evaluate operation is performed on an MSAP, the MSAP form is not automatically updated with the new values. You must perform a resynchronization to update the parameter values. See Procedure 64-11 for more information about modifying and re-evaluating a Creation MSAP policy on an MSAP. See Procedure 64-12 for more information about modifying and re-evaluating an MSAP policy on one or more MSAPs.

Each MSAP can have one MSAP policy; however, the same MSAP policy can be applied to multiple MSAPs. The Capture L2 Access tab of the MSAP Policy form displays all of the Capture L2 access interfaces that are associated with this specific MSAP policy. You can change an MSAP policy locally or for all of the MSAPs that are associated with the MSAP policy. A change to a specific MSAP policy will cause the same change in all the MSAPs that use that policy if all of the MSAPs are re-evaluated or if the MSAP policy is re-evaluated.

Warning — If there is a disruption on the NE and the NE recovers by restarting, the MSAP policy that was changed and re-evaluated will be applied to all of the MSAPs associated to the policy.

The 5620 SAM treats the setup and teardown of MSAPs as state transitions to offset the load imposed by constant SAP creation and deletion. There are two states that an MSAP can have, active or inactive. These states cannot be configured. The state is automatically set to active when the MSAP is created on the NE. When the NE deletes the MSAP, the state changes to inactive. That is, when the MSAP is torn down, the state changes to inactive, the MSAP continues to be available in the 5620 SAM but is not used until it is reactivated by the NE. When the MSAP is reactivated, it will have the same identification so that the 5620 SAM can identify it with the same FDN.

The state information is not automatically updated in the 5620 SAM GUI. You must perform a resynchronization to retrieve the current state information. When the state is inactive, performance statistics for the MSAP are not retrievable; however, historical statistical records are available. You can schedule MSAP statistics or collect the statistics on demand. See the *5620 SAM Statistics Management Guide* for more information about scheduling and collecting statistics.

MSAPs are listed on the L2 Access Interface tab for VPLSs and on the Service Access Points tab of the IES and VPRN forms.

MSAPs are bound by the maximum number of SAPs allowed on the NE. Typically, and as long as services are not deleted, the number of MSAPs within the 5620 SAM are bound by the formula:

$$A \times B \times C$$

where:

A is the number of services

B is the maximum number of SAPs allowed on the NE

C is the number of NEs

Inactive services that previously contained MSAPs consume database space. MSAPs that have been in an inactive state for a long period of time or that are no longer used must be manually deleted. See Procedure 64-14 for more information about deleting an MSAP.

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 64-14 for more information about deleting MSAPs.

MSAP event logs

An MSAP event log records the date, time, and active state for each state change that occurs after the MSAP is created. An event log is not recorded when the MSAP is created, although the information is recorded in a time stamp. You can view the event log for each MSAP, purge the event log records, and modify the global MSAP log policy retention time and administrative state.

MSAP time stamps

You can view the following MSAP state time stamps:

- date and time that the MSAP was created
- date and time of the last active state change

See Procedure 64-9 for information about viewing MSAP properties.

MSAP creation and management tasks

Table 64-2 summarizes the tasks required for MSAP creation and management.

Table 64-2 MSAP creation and management

Task	Purpose
To create an MSAP policy	Create an MSAP policy that will be added to a Capture SAP
To create a Capture SAP	Create a Capture SAP that will enable creation of an MSAP
To list MSAPs and view MSAP properties	List MSAPs
To delete an MSAP policy	Delete an MSAP policy
To modify and re-evaluate an MSAP policy on an MSAP	Modify and reapply an MSAP policy
To modify an MSAP policy and re-evaluate the MSAPs	Modify and re-evaluate an MSAP policy on one or more MSAP
To view an MSAP event log, modify the global MSAP log policy, and purge MSAP log records	View the event log for an MSAP, modify the global MSAP log policy, and purge the log records for an MSAP
To delete an MSAP	Delete an MSAP to create more space

Subscriber explicit maps

A subscriber explicit map is a table that directly associates dynamic subscriber hosts with subscriber profiles and SLA profiles. The entries in a subscriber explicit map override the default profile definitions. A subscriber ID string is the unique key for a subscriber explicit map entry.

A subscriber explicit map includes:

- subscriber ID string
- subscriber profile name
- SLA profile name
- AA group policy name
- subscriber ID alias

A subscriber explicit map does not allow the association of a subscriber ID string with the subscriber profile called “default”. However, if the explicit mapping omits a subscriber profile, the subscriber ID string is associated with the SAP or NE default subscriber profile. An attempt to delete a subscriber profile that is named in a subscriber explicit map fails. A 5620 SAM operator can remove explicit map entries at any time.

If an operator creates a subscriber explicit map entry without using the 5620 SAM, for example, using CLI, the 5620 SAM creates a subscriber instance in the global subscriber explicit map. If the 5620 SAM subsequently discovers another NE with the same subscriber entry that has a mapping to different profile, the 5620 SAM treats the second mapping as a local mismatch to the global entry for the subscriber.

Static hosts and residential subscriber management

Static subscriber hosts require explicit provisioning rather than an association with a subscriber identification policy. Static hosts for VPLS are configurable on the anti-spoofing tab of the L2 access interface management form. For IES and VPRN services, static hosts are configurable using the management form for a SAP on a group interface. Static host configuration involves the following elements:

- IP address
- MAC address (optional)
- subscriber ID string, or the use of the SAP ID as the subscriber ID
- valid subscriber profile
- valid SLA profile
- ANCP string
- intermediate destination, such as a DSLAM
- application profile

Note — When residential subscriber management is enabled on a VPLS SAP that is part of an operational MC ring group, the following must be configured on each static host:

- an intermediate destination that is a ring node in the MC ring group
- subscriber identification, such as a subscriber ID string or the use of the SAP ID as the subscriber ID
- a subscriber profile
- an SLA profile

ANCP policies

An ANCP policy defines the behavior of the residential subscriber host with which the policy is associated. An ANCP policy includes one of the following:

- static ANCP association
- static ANCP MSS association
- dynamic subscriber-profile association on VPLS, IES, VPRN and VLL services

An ANCP policy conveys status and control information based on port-up/port-down messages and changes to the current access line rate between the edge device and the access node. This allows the 7450 ESS, the 7750 SR, or the 7710 SR to adjust the HQoS subscriber scheduler with the correct rate or raises an alarm when the rate goes below a set threshold. The policy can be changed if the rate drops below a minimal threshold value. The ANCP actual upstream synchronization rate is configured in the ingress panel while the ANCP actual downstream synchronization rate is configured in the egress panel.

Host tracking

A host tracking policy is used to allow a subscriber's video traffic (multicast) to be included in the egress rate control for the subscriber. When a host tracking policy is specified in a subscriber profile, the egress traffic rate for the subscriber takes into account the unicast and multicast traffic in the aggregate egress rate or in the egress scheduler rate specified in the ANCP policy. There is no default host tracking policy.

When a host tracking policy is applied to a subscriber profile, all subscribers associated with the subscriber profile are tracked using that host tracking policy. You can view the tracked subscribers on the associated local host tracking policy property form.

You can also configure IGMP host tracking parameters on VPLS, IES, and VPRN service sites and SAPs.

The following on-demand host tracking information is available:

- on the Residential Subscriber Instance form, Host Tracking Info tab button, which hosts are being tracked for this particular subscriber
- on the Residential Subscriber Instance form, Host Tracking Status tab button, the egress traffic rate reduction for this particular subscriber
- on the VPLS L2 access interface property form, Host Tracking Info tab button, which hosts are being tracked
- on the IES and VPRN service access point property form, Host Tracking Info tab button, which hosts are being tracked

On-demand historical and real-time host tracking statistics are supported for SAPs and residential subscribers. Only historical statistical plotting is supported. The statistics and read-only host tracking information can be cleared by the 5620 SAM.

Diameter

The 5620 SAM supports diameter policies and associated diameter peers. Diameter policies are used in a subscriber management context to provide a credit control mechanism. The diameter policy establishes a server/peer configuration, as well as Diameter Credit-Control Application (DCCA) support. The NE functions as the credit control client, while the peer acts as the credit control server.

DCCA represents an alternative to RADIUS for providing a mechanism to support pre-paid service model in access networks. Under a DCCA configuration, the credit control server is used to grant service to a subscriber for pre-defined duration. Before a subscriber host is created, the BNG queries the credit control server about the credit for the given subscriber. If credit is granted, the subscriber host is installed with the appropriate SLA level. If the subscriber has no credit, the credit control server denies access and no subscriber host is created.

The diameter policy is used to specify common diameter protocol parameters, while the diameter peer defines the relationship with an external diameter server. The diameter protocol parameters defined on the diameter policy describe connection and session characteristics, and indicate which attribute-value pairs (AVPs) to use in messages.

Peers

The diameter policy defines a set of peers with which to establish diameter sessions. Peers share the configuration of the policy with which they are associated, but can override individual timer parameters inherited from the policy. In addition, each peer defines transport and connection-specific parameters, values for destination-specific AVPs, and a preference value.

The 7750 SR and 7450 ESS provide read-only operational values and statistics for the peer definition of local diameter policies. The 5620 SAM can provide a snapshot view of operational values and statistics. Operational values include the peer's timer values, the current state of the peer's state machine, and the peer's order among the other peers within the policy.

DCCA

The 7710 SR and 7750 SR support a DCCA, which can be customized through a set of parameters on the diameter policy in the 5620 SAM. The parameters allow customization of DCCA error handling, DCCA timer(s), and AVP value definitions.

PPPoE sessions

PPPoE is used in subscriber networks to encapsulate PPP frames inside Ethernet frames. PPPoE combines the point-to-point protocol used with DSL sessions with the Ethernet protocol used to support multiple subscribers in a local area network. PPPoE takes advantage of the speed of a packet-based Ethernet network with the security and accounting functions of a PPP network. PPPoE allows service providers to use existing RADIUS authentication.

Since more than one subscriber is sharing the same connection to a service provider, PPPoE organizes subscribers during two stages:

- PPPoE discovery stage
- PPPoE session stage

During the discovery stage, the subscriber and service provider identify each other's MAC address and establish a PPPoE session ID.

The PPPoE discovery stage consists of the following steps:

1 PPPoE Active Discovery Initiation (PADI). The client initiates a session by broadcasting a PADI packet to the LAN to request a service.

2 PPPoE Active Discovery Offer (PADO). Any access device that can deliver the service requested by PADI packet, replies with a PADO packet that contains its name, unicast address and service requested.

3 PPPoE Active Discovery Request (PADR).The client selects one of the PADOs that it receives and sends a PADR packet to indicate the services required.

4 PPPoE Active Discovery Session Confirmation (PADS). When the selected device receives the PADR packet, it can accept or reject the PPPoE session. To accept the session the device sends the client a PADS packet with a unique ID and a service name. If the device rejects the session, it sends a PADS packet with a service name error and resets the session ID to zero.

During the session stage, PPPoE behaves as a peer-to-peer protocol. Each PPPoE session is identified by the MAC address of the peer and the session ID. Once a session is established, both end points build a point to point connection over the Ethernet and exchange packets. Once the connect is established, the RADIUS accounting policy can begin. LCP negotiates authentication parameters. After a session is authenticated IPCP sends an IP address to the PPPoE client. IP Addresses can be stored in the DHCP local user database, if configured.

After a session is established both end points monitor the session and can terminate a session after a configured number of keep alive intervals are exceeded. An alarm is raised by the 5620 SAM when a PPPoE session fails. Either peer can send a PPPoE Active Discovery Termination (PADT) packet. See "Local DHCP servers" in this chapter for more information on associating PPPoE with a local DHCP server.

Subscriber host connectivity verification

Aside from relatively infrequent IP-address lease renewal, DHCP has no session-monitoring or connection-monitoring capability. Residential subscriber management provides this functionality for DHCP hosts and static hosts using subscriber host connectivity verification, or SHCV.

When SHCV is enabled on a SAP, an NE issues a periodic ARP request to each host on the SAP. If the NE receives no reply to an ARP request within the specified interval, the NE raises an event. When SHCV is configured to drop a lost host, the NE immediately removes the host from its active subscriber host table.

SHCV records the state information that it collects for hosts on a SAP and maintains a history of connectivity-related events for troubleshooting purposes. The size of the history log is restricted by a size-constraint policy.

SHCV operates in conjunction with DHCP snooping and is configurable on VPLS, VPRN, and IES SAPs and on IES group interfaces. Because it uses ARP, SHCV automatically populates the FIBs of bridging devices in the access and provider networks. The configurable items for SHCV on a SAP include:

- frequency of connectivity checks
- source of the ARP request
- action to take when a host loses connectivity

Note — On an L2 access interface, SHCV uses the NE system IP address as the source of the ARP request. On an L3 access interface, SHCV uses the IP- and MAC-address combination of the interface or the VRRP state for the interface as the ARP source. On IES group interfaces, SHCV uses the address of the subscriber interface as the source.

The behavior that an NE exhibits toward SHCV events is configurable using the residential subscriber management form. The configurable NE SHCV items include:

- maximum host connectivity loss rate
- action to take when the connectivity loss rate exceeds the maximum
- action to take when the NE drops an event trap, as such an event may indicate a high connectivity loss rate

SHCV event handling on an NE is disabled by default. When SHCV is enabled on a SAP but is disabled on the NE, the 5620 SAM records the blocking of SHCV events in the SHCV log. This ensures that an operator is aware of SHCV activity when viewing the SHCV log, even if the NE is configured to suppress SHCV events.

The following conditions represent an SHCV host connectivity loss:

- absence of a host response
- inconsistency between the reply data and the DHCP lease state

An NE makes more than one SHCV attempt before it raises an event against a host to ensure that the absence of a host response indicates a host connectivity problem and is not simply the result of occasional packet loss.

When a SAP becomes operationally down, the NE generates one trap for the SAP rather than one trap for each host on the SAP. When the SAP returns to service, the NE forwards a trap for each host as it verifies the restoration of connectivity. SHCV generates the following event traps:

- SAP up
- SAP down
- host up
- host down
- trap dropped

Routed CO

A broadband access network typically requires the aggregation of the traffic from access equipment before routing of the traffic is possible. Routed CO functionality allows a network operator to directly connect a DSLAM or similar multiplexer to a router such as the 7750 SR. Residential subscriber management, combined with the use of DSCP or dot1p values, supports access-integration models such as the following:

- one SAP for all subscribers and service offerings
- one SAP per service offering
- one SAP per subscriber

Routed CO allows the configuration of subscriber interfaces and group interfaces on IES and VPRN. A subscriber interface defines the subnets that are available to a subscriber. A group interface is a child object of a subscriber interface that allows the configuration of multiple SAPs as part of a single interface. Routed CO functionality depends on residential subscriber management to maintain the subscriber host information.

The 5620 SAM supports routed CO in IES and VPRN services:

There is no direct association between the subnets and the group interfaces. Subnets can be shared between group interfaces. If the host IP address is not in one of the subnets, packets from the network to that host IP are not received by the subscriber or group interfaces.

A subscriber interface defines a maximum of 16 subscriber subnets and acts as the DHCP relay agent for a subscriber. For the forwarding of DHCP packets to a subscriber server, a subscriber interface requires the specification of a gateway address that is in one of the subscriber subnets. Group interfaces below the subscriber interface inherit this gateway address but can specify an override value if required.

All SAPs in a group interface use the same port. The first SAP on a group interface determines which port the group interface uses. Additional SAPs for the group interface must be associated with the group-interface port during SAP creation.

A group interface is similar to a regular IES interface except for the following.

- Multiple SAPs are configurable.
- No IP addresses are specified.
- No broadcast traffic is permitted.
- No loopback mode exists.
- No static ARP can be specified.
- VRRP is not supported.

When a subscriber interface or a group interface is operationally disabled, no packets are sent to or from the subscriber hosts on the SAPs of the interface, but the state information for a static or dynamic host persists until the static host is removed from the NE by an operator or the DHCP lease of the dynamic host expires.

Because the configuration of multiple SAPs on a group interface makes normal forwarding of DHCP responses to hosts impossible, DHCP relay for routed CO maintains a cache of DHCP requests. If a DHCP server response does not arrive within the specified interval time, the NE discards the cache entry. The 5620 SAM operator can choose to have the NE use the Option 82 circuit ID field in a DHCP request as the match criterion for the returning DHCP ACK message.

You can configure Network Address Translation, or NAT, for dynamic subscriber hosts in a routed CO deployment. NAT for routed CO requires a NAT policy that is associated with a subscriber profile. In an IES routed CO deployment, NAT is configured on the base routing instance of an NE. NAT in a VPRN routed CO deployment is configured on the VPRN routing instance. See chapter 27 for general information about configuring and deploying NAT. See chapter 43 for information about configuring a NAT policy. See Procedure 64-2 for information about associating a NAT policy with a subscriber profile.

Lease populate is enabled on a group interface by default, and the number of allowable lease entries is set to one. All SAPs on the group interface inherit this configuration during creation.

See chapters 70 and 71 for more information on configuring subscriber and group interfaces for IES and VPRN services.

Wholesale and retail configurations for VPRN services

A VPRN routed CO allows a service provider to resell wholesale carrier services while providing direct DSLAM connectivity. You can create a VPRN service for the retailer and also define subscriber access and configuration information for the retailer network. The implementation of configuration changes occurs as if the VPRN is a standalone router using the routed CO model. The benefit of this model is flexibility for the retailer and decreased involvement for the wholesaler.

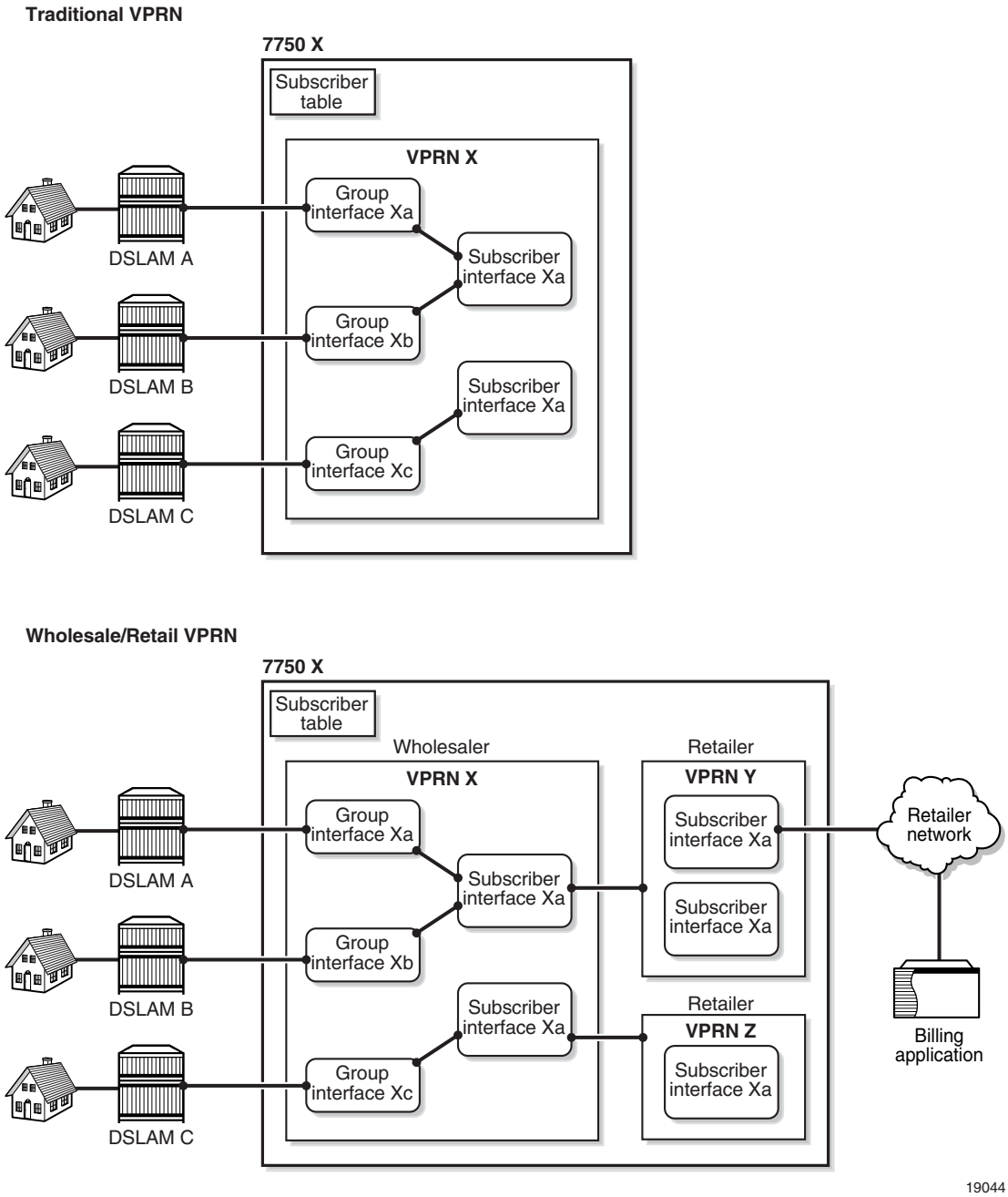
You must use a subscriber SAP to support shared access for multiple retailers. Another dependency of shared access is the requirement for the wholesaler to maintain separate access nodes for each retailer with network scaling issues.

In the wholesale and retail model, the wholesaler instance connections that are common to the access nodes are distributed to many retail instances. Upstream subscriber traffic ingresses into the wholesaler instance and, after identification, is then forwarded into the retail instance. The reverse principle occurs for traffic in the opposite direction. The wholesale and retail traffic flow is controlled with minimal communication to the RADIUS server. A RADIUS policy is defined in the wholesaler instance. The RADIUS response used during the subscriber instantiation provides the service context of the retailer VPRN. If the wholesaler has a retail business, the operator can configure a separate VPRN for their retail services.

The retailer subscriber interface primarily controls the DHCP configuration. The single exception to this model is the lease-populate value. The lease-populate value in the wholesale context controls the individual SAP limits. The lease-populate value in the retail subscriber interface controls the limits for that retailer interface. The wholesale and retail limits must be met before the instantiation of a new subscriber.

Figure 64-3 shows the configuration for a traditional and wholesale retail VPRN.

Figure 64-3 Routed CO for traditional and wholesale/retail VPRNs



See chapter 71 for more information on configuring the forwarding service component for wholesale and retail VPRN services.

Subscriber host polling and monitoring

Subscriber hosts can be periodically polled and monitored for certain DHCP event changes. A subscriber host monitoring configuration form is available from the Manage Residential Subscribers form.

The maximum number of hosts that can be selected for monitoring is configurable through XML; the default is five. Host monitoring has a performance impact, so only a small number are typically monitored at one time.

The Monitored Subscriber Host form displays a variety of polled information about the host that is obtained from the NE. You can also open a DHCP event log for the host from the Host Properties form. The logged events include information on DHCP lease renewals, lease expiration, and profile changes. An entry is added to the table whenever a new event occurs. You can purge event entries using the Host Properties form.

Host monitoring can be started, stopped, or removed from the monitoring configuration form, and the monitoring period and polling interval can be configured.

The Host monitored objects and associated events are stored in the 5620 SAM database. The monitoring continues until the monitoring period elapses or the monitoring is stopped by a 5620 SAM operator.

SAP monitoring

You can monitor the DHCP events on one or more SAPs. A SAP monitoring form is available from the Manage Residential Subscribers form.

The maximum number of SAPs that can be selected for monitoring is configurable through XML; the default is five. SAP monitoring has a performance impact, so only a small number are typically monitored at one time.

The Monitored Access Interface form displays a variety of DHCP-related events or notifications about subscriber hosts on a SAP that are compiled using traps received from NEs. You can also open an event log for the SAP from the SAP Properties form. The logged events include information on DHCP lease entries, lease states, and host connectivity. An entry is added to the table whenever a new event occurs. You can purge event entries using the Monitoring Configuration form.

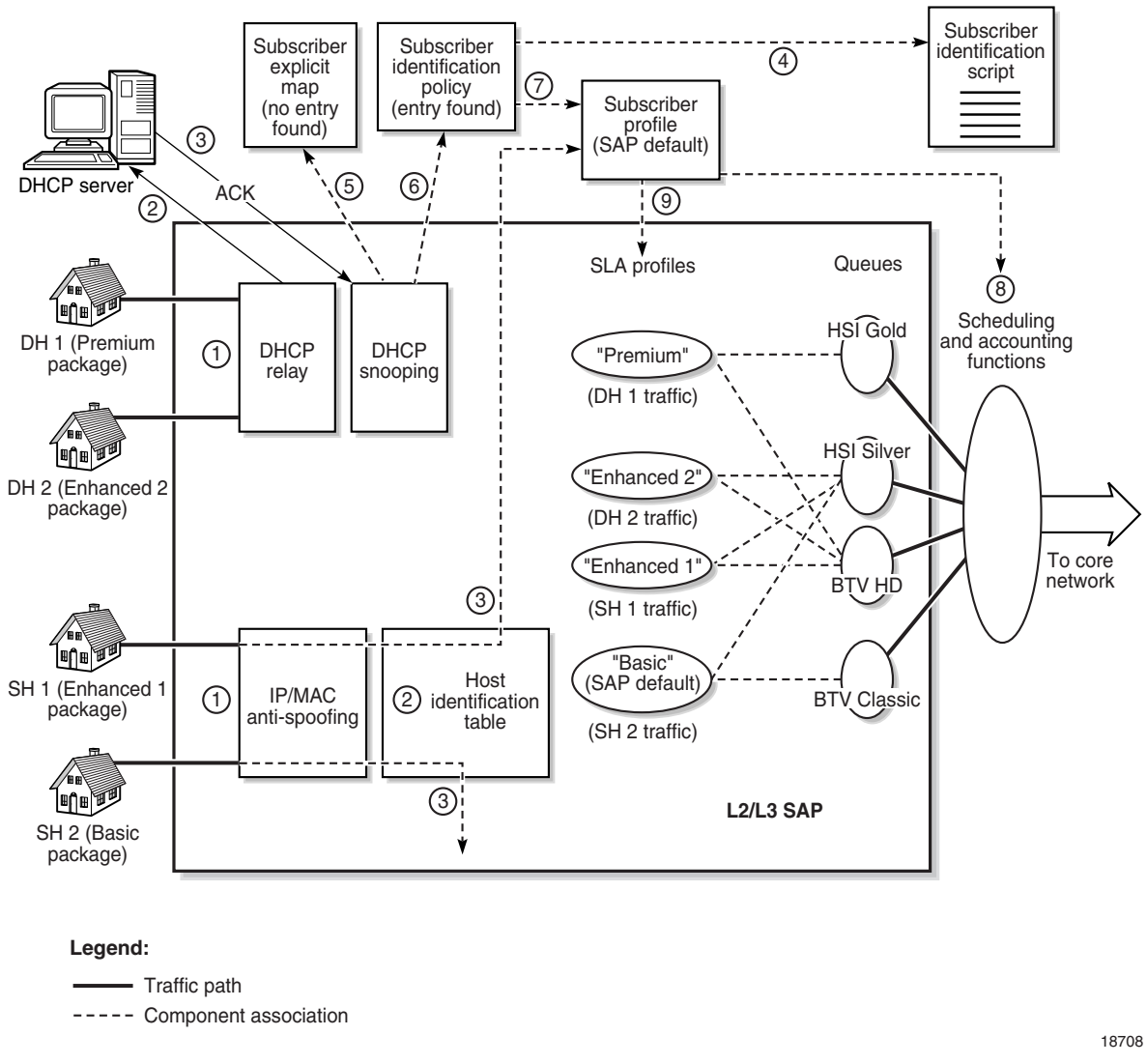
SAP monitoring can be started, stopped, or removed from the monitoring configuration form, and the monitoring period can be configured.

The SAP monitored objects and the associated events are stored in the database. The monitoring continues until the monitoring period elapses or the monitoring is stopped by a 5620 SAM operator.

64.2 Sample configuration

Figure 64-4 shows how residential subscriber management assigns resources to dynamic and static hosts. Many different configurations are possible; the sample portrays the residential subscriber management mechanism rather than a particular service delivery model. For simplicity, the sample consists of one subscriber instance on one SAP, and two types of service offering. Each service offering is available in two classes.

Figure 64-4 Sample configuration



The customer provides a subscriber identification string, the names of the four end-user service packages, and the bandwidth and class requirements for each package. Each package is a combination of HSI and BTV. A 5620 SAM operator creates four queues and four SLA profiles with which the queues are associated, as shown in Table 64-3. Alcatel-Lucent recommends that the 5620 SAM operator give the SLA profiles the same names as the packages to prevent confusion.

Table 64-3 Sample configuration service packages

Subscriber host	Package name	SLA profile name	Associated queues
DH 1	Premium	Premium	HSI Gold, BTV HD
DH 2	Enhanced 2	Enhanced 2	HSI Silver, BTV HD

(1 of 2)

Subscriber host	Package name	SLA profile name	Associated queues
SH 1	Enhanced 1	Enhanced 1	HSI Gold, BTV Classic
SH 2	Basic	Basic	HSI Silver, BTV Classic

(2 of 2)

The customer offers two classes of BTV and HSI services:

- BTV HD: high-definition broadcast television
- BTV Classic: regular-definition broadcast television
- HSI Gold: high-bandwidth broadband Internet access
- HSI Silver: regular broadband Internet access

The following steps, which correspond to the numeric labels in the upper part of Figure 64-4, define the sequence of events for dynamic subscriber hosts that attempt to join the network.

1 Dynamic Host 1 (DH 2) and Dynamic Host 2 (DH 2) each send a DHCP request to the SAP.

2 DHCP relay on the SAP forwards the DHCP requests to the DHCP server.

3 The DHCP server authorizes the requests and responds with a DHCP ACK message for each subscriber host.

4 The subscriber identification policy uses a script to obtain the subscriber identification string, an optional subscriber profile string, and an optional SLA profile string from the Option 82 information in each ACK message. DH 1 and DH 2 provide the same subscriber profile identification string but different SLA profile strings.

5 The NE checks the subscriber identification string values against the entries in the subscriber explicit map and finds no matching entries for the hosts.

6 The NE checks the subscriber profile string and the SLA profile string values for each host against the subscriber identification policy.

7 The NE assigns the same subscriber profile to DH 1 and DH 2 based on the subscriber profile string provided by each host.

8 DH 1 is the first host to join the network, so the scheduling and accounting functions associated with the assigned subscriber profile are instantiated on the SAP.

9 The NE matches the SLA profile string provided by each host to an SLA profile. The NE assigns the Premium SLA profile to DH 1 and the Enhanced 2 SLA profile to DH 2 based on the provided SLA profile strings. These are the first hosts of the subscriber to join the network, so the appropriate queues are instantiated on the SAP based on the SLA profile specifications, and host traffic subsequently flows.

The following steps, which correspond to the numeric labels in the lower part of Figure 64-4, define the sequence of operations for static subscriber hosts that join the network.

1 Static Host 1 (SH 1) turns on the computer, and Static Host 2 (SH 2) turns on the television.

2 The host devices request network access; IP- matching (and optional MAC-matching) anti-spoofing on the SAP checks the static host table on the NE and validates both requests.

3 The NE assigns resources to each static host based on subscriber profile and SLA profile designations, and host traffic subsequently flows.

- The static host table entry for SH1 names a subscriber profile and an SLA profile. Although SH 1 is the first host to use this SLA profile, the queues defined in the profile are already instantiated because of the application of the SLA profiles for DH 1 and DH 2.
- For SH 2, there is no explicit association between the host and a subscriber profile or an SLA profile, so the NE assigns the SAP default subscriber and SLA profiles, which define the most basic service package the customer offers to end users.

64.3 Workflow to manage residential subscribers

1 Create a service that effectively delivers the proposed service offerings.

2 Create ingress and egress scheduler policies for the subscriber hosts in accordance with the customer SLA.

3 Create an accounting policy for the customer.

4 Create access ingress and access egress QoS policies for the different applications, for example, HSI and VoIP, and levels of service, for example, gold, silver, and bronze, that subscriber hosts are to receive. Associate the queues in the QoS policies with the previously created scheduler policies.

5 Create a unique subscriber identification string for the subscriber, according to customer specifications.

6 Create a RADIUS authentication policy for the subscriber, if required.

7 Create a policer control policy for the subscriber, if required.

8 Create SLA profiles that name the previously created QoS policies. See procedure 64-3 for more information.

i Create a different SLA profile for each class of service offering.

ii Use override values to customize the policy values, if required.

iii Use override values to customize the policer values, if required.

9 Create a subscriber profile. See procedure 64-2 for more information.

i Choose the previously created ingress and egress scheduler policies.

ii Choose the previously created accounting policy.

iii Enable accounting.

iv Assign a RADIUS accounting policy, if required.

v Assign ingress and egress policer control policies, if required.

vi Associate one or more of the previously created SLA profiles with the subscriber profile.

10 Assign the subscriber profile and SLA profiles to the service SAPs. See procedure 64-22 for more information.

11 Create primary and backup scripts for extracting subscriber identification strings, such as the one created in step 5, from the DHCP Option 82 information. Place the scripts in network locations that are accessible to the 5620 SAM and the NEs that use the scripts.

12 Create a subscriber identification policy that specifies the URLs for the primary and backup subscriber identification scripts created in step 11. See procedure 64-1 for more information.

13 Create a subscriber explicit map, if required. See procedure 64-15 for more information.

14 Turn up the service.

15 If static subscriber hosts are supported by the configuration, create static host entries on the SAPs using the Anti-Spoofing tab of a SAP configuration form.

i Enable anti-spoofing and specify, as a minimum, an IP-address match criterion.

ii Specify a subscriber identifier, subscriber profile, and SLA profile for each static host, as required, if default values are not configured on the SAP. See procedure 64-24 for more information.

16 Provide the customer with the necessary IP information for provisioning dynamic and static hosts in the customer network.

64.4 Residential subscriber management procedures

Use the following procedures to perform residential subscriber management tasks.

Procedure 64-1 To create or modify a subscriber identification policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a subscriber identification policy.

i Click on the Create button and choose Create Subscriber Identification Policy from the drop-down menu. The Subscriber Identification Policy (Create) form opens.

ii Go to step 3.

b Modify a subscriber identification policy.

Caution — Modifying an active subscriber identification policy is potentially service-affecting. Ensure that you consider the implications of reconfiguring the subscriber identification policy before you proceed.

i Choose Subscriber Identification Policy from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of subscriber identification policies appears.

iii Select a subscriber identification policy and click on the Properties button. The Subscriber Identification Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- Strings From Option
- Primary Script URL
- Primary Script Administrative State
- Secondary Script URL
- Secondary Script Administrative State
- Tertiary Script URL
- Tertiary Script Administrative State

Note 1 — You can designate a subscriber identification policy as the default policy by specifying the case-sensitive name “default” for the Displayed Name parameter. The Displayed Name parameter is configurable only during subscriber identification policy creation.

Note 2 — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Supported Service Models tab button to indicate the intended service model for the subscriber identification policy.

Note — The 5750 SSC requires the specification of a service model for proper interoperation with the 5620 SAM.

5 Configure the parameters:

- VLAN per Subscriber (Routed)
- VLAN per Service (Routed)
- VLAN for all Services (Routed)
- VLAN per ISP per Service (Routed)
- VLAN per Subscriber (Bridged)
- VLAN per Service (Bridged)
- VLAN for all Services (Bridged)
- VLAN per ISP per Service (Bridged)

6 Click on the SLA Profiles tab button. The General tab is displayed.

7 Configure the Use Direct Map as Default parameter.

8 Perform one of the following steps to configure SLA profiles for the subscriber identification policy, if required.

a Assign an SLA profile.

i Click on the Add button. The SLAProfileEntry (Create) form opens.

ii Click on the Select button to choose an SLA profile. The Select SLA Profile form opens.

iii Select an SLA profile and click on the OK button. The Select SLA Profile form closes, and the SLAProfileEntry (Create) form refreshes with the SLA profile information.

iv Configure the SLA Profile String parameter.

v Click on the OK button to close the SLAProfileEntry (Create) form. A dialog box appears.

vi Click on the OK button. The Subscriber Identification Policy (Create) form refreshes with the SLA profile entry.

b Remove an SLA profile.

i Select an SLA profile and click on the Delete button. A dialog box appears.

ii Click on the OK button. The SLA profile is removed from the list.

iii If you want to assign an SLA profile to replace the removed SLA profile, go to step 8 a.

9 Click on the Subscriber Profiles tab button. The General tab is displayed.

10 Configure the Use Direct Map as Default parameter.

11 Perform one of the following steps to configure subscriber profiles for the subscriber identification policy, if required.

a Add a subscriber profile.

i Click on the Add button. The SubscrProfileEntry (Create) form opens.

ii Click on the Select button to choose a subscriber profile. The Select Subscriber Profile form opens.

iii Select a subscriber profile and click on the OK button. The Select Subscriber Profile form closes, and the SubscrProfileEntry (Create) form refreshes with the subscriber profile information.

iv Configure the Subscriber Profile String parameter.

v Click on the OK button to close the SubscrProfileEntry (Create) form. A dialog box appears.

vi Click on the OK button. The Subscriber Identification Policy (Create) form refreshes with the subscriber profile entry.

b Remove a subscriber profile.

i Select a subscriber profile and click on the Delete button. A dialog box appears.

ii Click on the OK button. The subscriber profile is removed from the list.

12 Click on the Application Profiles tab button. The General tab is displayed.

13 Configure the Use Direct Map as Default parameter.

14 Perform one of the following steps to configure application profiles for the subscriber identification policy, if required.

a Add an application profile.

i Click on the Add button. The AppProfileEntry (Create) form opens.

ii Click on the Select button to choose an application profile. The Select Application Profile form opens.

Note 1 — If the subscriber identification policy opened in step 2 is a global policy, global AA group policies are listed. If the subscriber identification policy is a local policy, local AA group policies are listed.

Note 2 — The global AA group policies must be manually distributed to the NE before a global subscriber identification policy using the application profiles can be distributed.

Note 3 — When a new subscriber identification or subscriber explicit map is discovered from the NE, the AA group policy is not automatically resynchronized to the global subscriber identification policy.

iii Select an application profile and click on the OK button. The Select Application Profile form closes, and the AppProfileEntry (Create) form refreshes with the application profile information.

iv Configure the Application Profile String parameter.

v Click on the OK button to close the AppProfileEntry (Create) form. A dialog box appears.

vi Click on the OK button. The Subscriber Identification Policy (Create) form refreshes with the application profile entry.

b Remove an application profile.

i Select an application profile and click on the Delete button. A dialog box appears.

ii Click on the OK button. The application profile is removed from the list.

15 Click on the OK button to close the Subscriber Identification Policy (Create) form. A dialog box appears.

16 Click on the Yes button. The Subscriber Identification Policy (Create) form closes.

17 Close the Manage Subscriber Policies form.

Procedure 64-2 To create or modify a subscriber profile

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a subscriber profile.

i Click on the Create button and choose Create Subscriber Profile from the drop-down menu. The Subscriber Profile (Create) form opens.

ii Go to step 3.

b Modify a subscriber profile.

Caution — Modifying an active subscriber profile is potentially service-affecting. Ensure that you consider the implications of reconfiguring the subscriber profile before you proceed.

i Choose Subscriber Profile from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of subscriber profiles appears.

iii Select a subscriber profile and click on the Properties button. The Subscriber Profile (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description

Note 1 — You can designate a subscriber profile as the default profile by specifying the case-sensitive name “default” for the Displayed Name parameter. The Displayed Name parameter is configurable only during subscriber profile creation.

Note 2 — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

Note 3 — The Egress Aggregate Rate Limit (kbps) and Frame Base Accounting parameters are configurable only when a scheduler is not specified in the Egress Scheduler panel.

4 Click on the Select button in the Accounting Policy panel. The Select Accounting Policy ID - Subscriber Profile form opens.

5 Select an accounting policy and click on the OK button. The Select Accounting Policy ID - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the accounting policy information.

6 Click on the Select button in the ANCP Policy panel. The Select ANCP Policy - Subscriber Profile form opens.

7 Select an ANCP policy and click on the OK button. The Select ANCP Policy - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the ANCP policy information.

8 Click on the Select button in the Host Tracking Policy panel. The Select Host Tracking Policy - Subscriber Profile form opens.

9 Select a host tracking policy and click on the OK button. The Select Host Tracking Policy - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the host tracking policy information.

10 Click on the Select button in the NAT Policy panel. The Select NAT Policy - Subscriber Profile form opens.

11 Select a NAT policy and click on the OK button. The Select NAT Policy - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the NAT policy information.

12 Click on the Select button in the IGMP Policy panel. The Select IGMP Policy - Subscriber Profile form opens.

13 Select an IGMP policy and click on the OK button. The Select IGMP Policy - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the IGMP policy information.

14 Click on the Scheduling tab button.

15 Configure the parameters:

- Egress Aggregate Rate Limit (kbps)
- Average Frame Size
- Encapsulation Offset
- Frame Base Accounting

Note — An additional parameter, Encapsulation Offset Mode, can be configured using OSSI.

16 Perform one of the following steps using the buttons in the Ingress Scheduler and Egress Scheduler panels.

Note — You cannot specify an egress scheduler in a subscriber profile when the Egress Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

a Assign a scheduler.

i Click on the appropriate Select button to choose an ingress or egress scheduler. The ingress or egress Select Scheduler - Subscriber Profile form opens.

ii Select a scheduler and click on the OK button. The Select Policy - Subscriber Profile form closes, and the Subscriber Profile (Create) form refreshes with the chosen scheduler.

b Remove a scheduler.

i Click on the appropriate Clear button to remove an ingress or egress scheduler. The scheduler is removed from the Subscriber Profile (Create) form.

ii If you want to assign a scheduler to replace the removed scheduler, go to step 16a.

17 Click on the RADIUS Accounting tab button to associate a RADIUS-based accounting policy with the subscriber profile or to remove a RADIUS-based accounting policy from the subscriber profile.

18 Perform one of the following steps.

a Assign a RADIUS accounting policy by performing the following steps.

i Click on the Select button in the RADIUS Accounting Information panel. The Select RADIUS Accounting Information - Subscriber Profile form opens.

ii Configure the filter criteria.

iii Click on the Search button. A list of RADIUS accounting policies appears.

iv Select a policy from the list and click on the OK button. The Select RADIUS Accounting Information - Subscriber Profile form closes and the Subscriber Profile (Create) form refreshes with the RADIUS accounting policy information.

b Remove a RADIUS accounting policy.

i Click on the Clear button to remove a RADIUS accounting policy. The policy is removed from the Subscriber Profile (Create) form.

ii If you want to assign a policy to replace the removed policy, go to step 18a.

19 Perform one of the following steps to assign or remove a duplicate RADIUS accounting policy to generate duplicate accounting information for the subscriber profile.

a Assign a duplicate RADIUS accounting policy by performing the following steps.

i Click on the Select button in the Duplicate RADIUS Accounting Information panel. The Select Duplicate RADIUS Accounting Information - Subscriber Profile form opens.

ii Configure the filter criteria.

iii Click on the Search button. A list of RADIUS accounting policies appears.

iv Select a policy from the list and click on the OK button. The Select Duplicate RADIUS Accounting Information - Subscriber Profile form closes and the Subscriber Profile (Create) form refreshes with the duplicate RADIUS accounting policy information.

b Remove a duplicate RADIUS accounting policy.

i Click on the Clear button to remove a duplicate RADIUS accounting policy. The duplicate policy is removed from the Subscriber Profile (Create) form.

ii If you want to assign a duplicate policy to replace the removed duplicate policy, go to step 19a.

20 Click on the SLA Profiles tab button to associate an SLA profile with the subscriber profile or to remove an SLA profile from the subscriber profile. The General tab is displayed.

21 Configure the Use Direct Map as Default parameter.

22 Click on the Profiles tab button.

23 Perform one of the following.

a Assign an SLA profile.

i Click on the Add button. The SLAProfileEntry (Create) form opens.

ii Click on the Select button to choose an SLA profile. The Select SLA Profile form opens.

iii Select an SLA profile and click on the OK button. The Select SLA Profile form closes, and the SLAProfileEntry (Create) form refreshes with the SLA profile information.

iv Configure the SLA Profile String parameter.

v Click on the OK button to close the SLAProfileEntry (Create) form. A dialog box appears.

vi Click on the OK button. The Subscriber Profile (Create) form refreshes with the SLA profile entry.

b Remove an SLA profile.

i Select an SLA profile and click on the Delete button. A dialog box appears.

ii Click on the OK button. The SLA profile is removed from the list.

iii If you want to assign an SLA profile to replace the removed SLA profile, go to step 23 a.

24 Repeat step 23 for each additional SLA profile that you want to associate with the subscriber profile or remove from the subscriber profile.

25 Click on the HSMDA QoS tab button.

26 Configure the parameters:

- Ingress Aggregate Rate Limit (kbps)
- HSMDA Packet Byte Offset (bytes)
- Egress Aggregate Rate Limit (kbps)
- HSMDA Packet Byte Offset (bytes)

27 Perform one of the following.

a Assign an ingress policy.

i Click on the appropriate Select button to choose an ingress policy. The Select Ingress Policy form opens.

ii Select a policy and click on the OK button. The Select Ingress Policy form closes, and the Subscriber Profile (Create) form refreshes with the chosen policy.

b Assign an egress policy.

i Click on the appropriate Select button to choose an egress policy. The Select Egress Policy form opens.

ii Select a policy and click on the OK button. The Select Egress Policy form closes, and the Subscriber Profile (Create) form refreshes with the chosen policy.

28 Click on the Policer Control tab button to configure ingress and egress policer control policies, if required.

i On the Ingress Policer Control Policy panel, configure the Displayed Name parameter.

Click on the Select button next to the Displayed Name field and select a policy from the Select Policer Control Policy form.

ii You can configure local overrides on the selected ingress policer control policy on the Ingress Policer Control Policy Override panel, if required. Enable the Override check box for either of the following parameters, and then configure the parameters:

- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space

iii On the Egress Policer Control Policy panel, configure the Displayed Name parameter.

Click on the Select button next to the Displayed Name field and select a policy from the Select Policer Control Policy form.

iv You can configure local overrides on the selected egress policer control policy on the Egress Policer Control Policy Override panel, if required. Enable the Override check box for either of the following parameters, and then configure the parameters:

- Maximum Frame Based Bandwidth
- Minimum Separation Buffer Space

29 Click on the Override tab button to modify the scheduler parameters for the subscriber profile, if required. The Ingress Schedulers tab is displayed.

30 Perform one of the following.

a Modify the ingress scheduler parameters.

i Click on the Add button. The Ingress Scheduler Entry Override (Create) form opens with the General tab displayed.

ii Click on the Select button. The Select Ingress Scheduler Policy Entry form opens.

iii Select a scheduler policy and click on the OK button. The Select Ingress Scheduler Policy Entry form closes, and the Ingress Scheduler Entry Override (Create) form refreshes with the configured values for the scheduler policy entry.

iv Click on the Override tab button.

v Configure the parameters:

- Summed CIR
- PIR (kbps)
- CIR (kbps)

vi Click on the OK button to close the Ingress Scheduler Entry Override (Create) form.

b Modify the egress scheduler parameters.

i Click on the Egress Schedulers tab button.

ii Click on the Add button. The Egress Scheduler Entry Override (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Egress Scheduler Policy Entry form opens.

iv Select a policy and click on the OK button. The Select Egress Scheduler Policy Entry form closes, and the Egress Scheduler Entry Override (Create) form refreshes with the configured values for the policy entry.

v Click on the Override tab button.

vi Configure the parameters:

- Summed CIR
- PIR (kbps)
- CIR (kbps)

vii Click on the OK button to close the Egress Scheduler Entry Override (Create) form.

c Modify the access ingress HSMDA queue parameters.

i Click on the Access Ingress HSMDA Queue tab button.

ii Click on the Add button. The Access Ingress HSMDA Queue Override (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Access Ingress Policy Queue form opens.

iv Select a policy and click on the OK button. The Select Access Ingress Policy Queue form closes, and the Access Ingress HSMDA Queue Override (Create) form refreshes with the configured values for the policy entry.

v Click on the Override tab button.

vi Configure the parameters:

- Override PIR
- Override CIR
- PIR (kbps)
- CIR (kbps)

vii Click on the Select button. The Select HSMDA Slope Policy form opens.

viii Select a policy and click on the OK button. The Select HSMDA Slope Policy form closes, and the Access Ingress HSMDA Queue Override (Create) form refreshes with the configured values for the policy entry.

ix Click on the OK button to close the Access Ingress HSMDA Queue Override (Create) form.

d Modify the access egress HSMDA queue parameters.

i Click on the Access Egress HSMDA Queue tab button.

ii Click on the Add button. The Access Egress HSMDA Queue Override (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Access Egress Policy Queue form opens.

iv Select a policy and click on the OK button. The Select Access Egress Policy Queue form closes, and the Access Egress HSMDA Queue Override (Create) form refreshes with the configured values for the policy entry.

v Click on the Override tab button.

vi Configure the parameters:

- Override PIR
- Override CIR
- PIR (kbps)
- CIR (kbps)

vii Click on the Select button. The Select HSMDA Slope Policy form opens.

viii Select a policy and click on the OK button. The Select HSMDA Slope Policy form closes, and the Access Egress HSMDA Queue Override (Create) form refreshes with the configured values for the policy entry.

ix Click on the OK button to close the Access Egress HSMDA Queue Override (Create) form.

e Click on the Ingress Policer Level tab button to configure ingress policer priority level overrides, if required. An ingress policer control policy must be configured on the subscriber profile before these steps can be completed.

i Click on the Add button. The Ingress Policer Level Override Create form appears. The configured policer control policy appears in the Displayed Name field.

ii On the Policer Level panel, click on the Select button. The Select Policer Level form appears.

iii Select a policer level from the list and click OK. The Select Policer Level form closes and the selected level appears in the Level field on the Policer Level panel. The current maximum cumulative buffer space value for the policer level is displayed in the Maximum Cumulative Buffer Space field.

iv To override the maximum cumulative buffer space value for the policer level, click on the Override tab button.

v On the Overridden Policer Level panel, enable the Override check box.

vi Either enable the Max check box or configure the Maximum Cumulative Buffer Space parameter.

vii Click OK. The policer level override is applied to the subscriber profile. To configure additional policer level overrides, repeat steps i through vii.

f Click on the Egress Policer Level tab button to configure egress policer priority level overrides, if required. An egress policer control policy must be configured on the subscriber profile before these steps can be completed.

i Click on the Add button. The Egress Policer Level Override Create form appears. The configured policer control policy appears in the Displayed Name field.

ii On the Policer Level panel, click on the Select button. The Select Policer Level form appears.

iii Select a policer level from the list and click OK. The Select Policer Level form closes and the selected level appears in the Level field on the Policer Level panel. The current maximum cumulative buffer space value for the policer level is displayed in the Maximum Cumulative Buffer Space field.

iv To override the maximum cumulative buffer space value for the policer level, click on the Override tab button.

v On the Overridden Policer Level panel, enable the Override check box.

vi Either enable the Max check box or configure the Maximum Cumulative Buffer Space parameter.

vii Click OK. The policer level override is applied to the subscriber profile. To configure additional policer level overrides, repeat steps i through vii.

31 Click on the OK button. The Subscriber Profile (Create) form refreshes with the scheduler override entry.

32 Click on the OK button to close the Subscriber Profile (Create) form. A dialog box appears.

33 Click on the Yes button. The Subscriber Profile (Create) form closes.

34 Close the Manage Subscriber Policies form.

Procedure 64-3 To create or modify an SLA profile

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create an SLA profile.

i Click on the Create button and choose Create SLA Profile from the drop-down menu. The SLA Profile (Create) form opens.

ii Go to step 3.

b Modify an SLA profile.

Caution — Modifying an active SLA profile is potentially service-affecting. Ensure that you consider the implications of reconfiguring the SLA profile before you proceed.

i Choose SLA Profile from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of SLA profiles appears.

iii Select an SLA profile and click on the Properties button. The SLA Profile (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Application
- Description
- Host Limit
- Remove oldest Subscriber Host

The Displayed Name parameter is configurable only during SLA profile creation.

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Select button in the Credit Control Policy panel. The Select Credit Control Policy form opens.

5 Select a credit control policy from the list and click on the OK button. The Select Credit Control Policy form closes.

6 Click on the QoS tab button to choose QoS policies for the SLA profile.

7 Perform one of the following steps using the buttons in the Ingress Policy and Egress Policy panels.

a Assign a policy.

i Click on the appropriate Select button to choose an ingress or egress QoS policy. The ingress or egress Select Policy - SLA Profile form opens.

ii Select a policy and click on the OK button. The Select Policy - SLA Profile form closes, and the SLA Profile (Create) form refreshes with the chosen policy.

iii Configure the ingress queue parameters:

- Use Shared Queue
- Use Multipoint Shared Queue

iv Configure the egress QoS marking parameter:

- Use Egress QoS Marking From SAP

b Remove a policy.

i Click on the Clear button in the Ingress Policy or Egress Policy panel to remove an ingress or egress QoS policy. The policy is removed from the list.

ii If you want to assign a policy to replace the removed policy, go to step 7a.

8 Configure the Scheduler Type parameter.

9 Click on the ACL tab button to assign ingress or egress IP filters to the SLA profile, if required.

i Click on the Select button in the Ingress IP Filter panel to choose an ingress IP filter from the Select Ingress IP Filter - SLA Profile form.

ii Click on the Select button in the Egress IP Filter panel to choose an egress IP filter from the Select Egress IP Filter - SLA Profile form.

iii Click on the Select button in the Ingress IPv6 Filter panel to choose an ingress IPv6 filter from the Select Ingress IPv6 Filter - SLA Profile form.

iv Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress filter from the Select Egress IPv6 Filter - SLA Profile form.

10 Click on the Supported Service Models tab button to indicate the intended service model for the SLA profile.

Note — The 5750 SSC requires the specification of a service model for interoperation with the 5620 SAM.

11 Configure the parameters:

- VLAN per Subscriber (Routed)
- VLAN per Service (Routed)
- VLAN for all Services (Routed)
- VLAN per ISP per Service (Routed)
- VLAN per Subscriber (Bridged)
- VLAN per Service (Bridged)
- VLAN for all Services (Bridged)
- VLAN per ISP per Service (Bridged)

12 Click on the Override tab button to specify local overrides for queue parameters of the QoS policies assigned to the SLA profile, if required. The Access Ingress Policy tab is displayed.

13 Perform either of the following:

a Modify the access ingress queue parameters.

i Click on the Add button. The Access Ingress Queue Override (Create) form opens with the General tab displayed.

ii Go to step 14.

b Modify the access egress queue parameters.

i Click on the Access Egress Queues tab button.

ii Click on the Add button. The Access Egress Queue Override (Create) form opens with the General tab displayed.

14 Choose the policy queue that you want to override.

i Click on the Select button. The policy queue Select form opens.

ii Select a policy queue and click on the OK button. The policy queue Select form closes, and the Queue Override (Create) form refreshes with the configured values for the policy queue.

15 Click on the Override tab button and configure the parameters:

- Override PIR
- Override CIR
- Override Maximum Burst Size
- Override Committed Burst Size
- Override High Priority Reserved
- Override Port Average Overhead
- Default
- PIR (kbps)
- CIR (kbps)
- Maximum Burst Size (bytes)
- Committed Burst Size (KB)
- High Priority Reserved
- Port Average Overhead (%)

The Override Port Average Overhead and Port Average Overhead (%) parameters are configured only for access egress queues.

16 Click on the OK button to close the Queue Override (Create) form. A dialog box appears.

17 Click on the OK button. The SLA Profile (Create) form refreshes with the queue override entry.

18 Specify local overrides for statistics and traffic flow rate parameters of the ingress or egress policers assigned to the SLA profile, if required.

19 Perform either of the following:

a Modify the access ingress policer parameters.

i Click on the Access Ingress Policers tab button.

ii Click on the Add button. The Ingress Policer Override (Create) form opens with the General tab displayed.

iii Go to step 20.

b Modify the access egress policer parameters.

i Click on the Access Egress Policer tab button.

ii Click on the Add button. The Egress Policer Override (Create) form opens with the General tab displayed.

20 Choose the policy policer that you want to override.

i Click on the Select button. The policy policer Select form opens.

ii Select a policy policer and click on the OK button. The policy policer Select form closes, and the Policer Override (Create) form refreshes with the configured values for the policy policer.

21 Click on the Override tab button and configure the parameters:

- Override PIR
- Override CIR
- Override Maximum Burst Size
- Override Committed Burst Size
- Default
- PIR (kbps)
- CIR (kbps)
- Maximum Burst Size (bytes)
- Committed Burst Size (KB)
- Stats Mode
- Packet Byte Offset

22 Click on the OK button to close the Policer Override (Create) form. A dialog box appears.

23 Click on the OK button. The SLA Profile (Create) form refreshes with the policy policer override entry.

24 Click on the OK button. A dialog box appears.

25 Click on the Yes button. The SLA Profile (Create) form closes.

26 Close the Manage Subscriber Policies form.

Procedure 64-4 To create a category map policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.

2 Click on the Create button to open the contextual menu.

3 Choose Category Map Policy from the contextual menu. The Category Map Policy (Create) form appears with the General tab displayed.

4 Configure the parameters:

- Displayed Name
- Description
- Credit Type
- Credit Exhaust Threshold
- Activity Threshold

5 Click on the Category tab button.

6 Click on the Add... button. The Category (Create) form opens with the general tab displayed.

7 Configure the parameters:

- Displayed Name
- Description
- Credit Type Override
- Rating Group
- Out Of Credit Action
- Default Credit Type
- Default Credit Time
- Default Credit Volume
- Default Credit Volume Unit
- PIR

The Rating Group parameter is only configurable when the Use Rating Group checkbox is enabled.

The PIR parameter is configured to its maximum value when the MAX checkbox is enabled.

Note — A maximum of three categories can be created for each category map policy.

8 Click on the Queues tab button.

9 Select any or all of the Ingress and Egress Queues to be defined in the category.

10 Click on the Policers tab button.

11 Select any or all of the Ingress and Egress Policers to be defined in the category.

12 Click on the Credit Exhausting Service Levels tab button.

13 Perform one of the following:

a To define credit exhausting service levels for IP filter entries, go to step 14.

b To define credit exhausting service levels for IPv6 filter entries, go to step 20.

14 Click on the IP Filter Entries tab button.

15 Click on the Add... button. The Exhausted IP Filter Entry (Create) form opens with the General tab displayed.

16 Configure the parameters:

- Filter Direction
- Entry ID
- Displayed Name
- Description

17 Click on the Filter Properties tab button.

18 Configure the parameters:

- Action
- Protocol
- DSCP
- Source IP Address
- Src Mask
- Destination IP Address
- Dst Mask
- Fragment
- IP Option
- IP Opt Mask
- Option Present
- Multiple Option

19 Go to step 25.

20 Click on the IPv6 Filter Entries tab button.

21 Click on the Add... button. The Exhausted IPv6 Filter Entry (Create) form opens.

22 Configure the parameters:

- Filter Direction
- Entry ID
- Displayed Name
- Description

23 Click on the Filter Properties tab button.

24 Configure the parameters:

- Action
- Protocol
- DSCP
- Source IP Address
- Src Mask
- Destination IP Address
- Dst Mask

25 Click on the OK button. A dialog box appears.

26 Click on the OK button. The Category (Create) for reappears with the filter entries information displayed.

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The Category Map Policy (Create) form reappears with the category information displayed.

29 Click on the OK button. The Category Map Policy (Create) form closes.

Procedure 64-5 To create a credit control policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.

2 Click on the Create button to open the contextual menu.

3 Choose Credit Control Policy from the contextual menu. The Credit Control Policy (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Displayed Name
- Description
- Credit Control Server
- Out Of Credit Action
- Error Handling Action

5 Click on the Select button in the Category Map panel. The Select Category Map form opens.

6 Select a category map policy from the list to be used with the credit control policy and click on the OK button. The Select Category Map form closes.

7 If you selected a value of Diameter for the Credit Control Server parameter, click on the Select button in the Diameter Policy panel. The Select Diameter Policy form opens.

8 Select a diameter policy from the list to be used to access the credit control server and click on the OK button. The Select Diameter Policy panel closes.

9 Click on the OK button. The Credit Control Policy (Create) form closes.

Procedure 64-6 To reset credit

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form appears.

2 Choose Residential Subscriber Host from the Object Type drop-down list.

3 Click on the Search button. A list of residential subscriber hosts is displayed.

4 Perform one of the following:

a Select a host from the list and click on the Reset Credit button. Go to step 9.

b Select a host from the list and click on the Properties button. The Subcriber Host form opens.

5 Click on the Credit Control Operational values tab button.

6 Select an entry from the list and perform one of the following:

a Click on the Reset Credit button. Go to step 8.

b Click on the Properties button. A form opens.

7 Close the form after viewing credit control data.

8 Close the Subscriber Host form.

9 Close the Manage Residential Subscribers form.

Procedure 64-7 To create an MSAP policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.

2 In the Manage Residential Subscriber form, choose Global as the Policy scope and right-click on the Create button to open the contextual menu.

3 Choose Create an MSAP Policy from the contextual menu. The MSAP Policy - Global (Create) form appears with the General tab displayed.

4 Configure the parameters in the General tab:

- Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Security tab button and configure the parameters.

i In the DoS Protection Policy area, click on the Select button to open the Select NE DoS Protection form and choose a DoS Protection Policy.

ii If MAC Monitoring is required, select the DoS Protection MAC Monitoring check box.

6 Click on the Subscriber Management tab button and configure the parameters.

- Subscriber Limit
- Default Subscriber Identification Type
- Default Subscriber ID
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id
- Default Subscriber Profile
- Default SLA Profile
- Default Subscriber Identification Policy
- Default Application Profile
- Profiled Traffic Only
- Non-subscriber Traffic Subscriber Identification
- Non-subscriber Traffic Subcriber Profile
- Non-subscriber Traffic SLA Profile
- Non-subscriber Traffic Application Profile

7 Perform the following as required:

a Click on the VPLS Configuration Only tab button and configure the following tabs within the VPLS Configuration Only tab.

i Click on the General tab button and configure the parameters:

- Split Horizon Group Name
- Egress Multicast Group Name
- ARP Reply Agent
- LAG Link Selection

ii Click on the DHCP tab button and configure the parameters:

- Lease Populate
- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- Administrative State
- Emulated Server IP Address
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

iii Click on the IGMP Snooping tab button and configure the parameters:

- IGMP Import Policy
- Fast-leave
- Send Queries
- General query interval (seconds)
- Max. Response interval (seconds)
- Robust count
- IGMP Version
- Max. Response interval group queries (tenths of seconds)
- Name
- Description
- Default Action
- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)
- MVR Source Interface (mvrSource)

b If this policy is for an MSAP on an IES or VPRN, click on the IES VPRN Only Configuration tab button and configure the Anti-Spoofing (antiSpoofing) parameter to be Source IP and MAC Addr.

8 Click on the VPLS Multicast CAC Constraints tab button and configure the parameters as follows:

Note 1 — Up to eight Multicast CAC Level entries can be created for an MSAP policy.

Note 2 — Up to eight Multicast CAC LAG entries can be created for an MSAP policy

Note 3 — The Bandwidth (kbps) range is 1 to 4 294 967 952 for an MSAP policy.

i Click on the Add button in the LAG Port Down tab and configure the following parameters:

- Number of Ports Down
- Level ID

ii Click on the Add button in the Level tab and configure the following parameters:

- Level ID
- Bandwidth (kbps)

9 Click on the Apply button.

10 Click on the OK button.

Procedure 64-8 To create a Capture SAP

Use this procedure to create a Capture SAP, which enables the creation of an MSAP. A Capture SAP must be the default on a port.

Note 1 — A Capture SAP is not intended to carry traffic. The only purpose of the Capture SAP is to trigger the creation of an MSAP.

Note 2 — The MSAPs that are subsequently created will be on the same port as the Capture SAP.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Navigate to the Access Interfaces icon for the required site. The path is VPLS→Site→Access Interfaces.

6 Right-click on Access Interfaces and choose Create VPLS L2 Access Interface. The VPLS L2 Access Interface (Create) form opens with the General tab displayed.

7 Configure the parameters as required for the service.

- SAP Sub Type , choose Capture from the SAP Sub Type drop-down menu.

Note — When you choose Capture as the SAP Sub Type, the displayed form changes to allow configuration of the Capture SAP.

- Description
- Administrative State

8 Click on the Port tab button.

9 Click on the Select button beside the Terminating Port Displayed parameter. The Select Terminating Port form appears.

10 Choose a terminating port from the list in the Select Terminating Port form.

11 Click on the DHCP tab button and add a Subscriber Authentication policy.

i Click on the Select button in the Subscriber Authentication Policy area. The Select Subscriber Authentication Policy - L2 access I/F window appears.

ii Filter the list to the Subscriber Authentication policy that you need.

iii Choose the required Subscriber Authentication policy.

12 Click on the Capture Access Interface tab button.

13 Perform one of the following to configure the Trigger Packet type:

a Select the check box beside one or two of the parameters that you want used to trigger RADIUS authentication. The parameters are:

- DHCP Trigger Packet
- PPPoE Trigger Packet
- ARP Trigger Packet

b Select the check box beside each of the parameters displayed to trigger RADIUS authentication when any or all of the trigger packets are received.

14 Click on the Select button in the MSAP Defaults panel to choose an MSAP Policy Name. The Select MSAP Policy - Capture L2 Access Interface form opens.

15 Configure the filter criteria. A list of available MSAP policies appears.

16 Choose an MSAP policy and click on the OK button. The Select MSAP Policy - Capture L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form appears with the MSAP policy name displayed.

17 Configure the parameters:

- MSAP Service ID
- MSAP Group Interface Name

18 If you need to change the PPPoE Policy, click on the Select button in the PPPoE Policy panel. The Select PPPoE Policy form appears.

i Choose a PPPoE Policy from the Select PPPoE Policy form.

ii If you need to change the existing PPPoE Policy, click on the Properties button in this form and modify the policy.

iii Click on the OK button.

19 Click on the Apply button.

20 Click on the OK button.

Procedure 64-9 To list MSAPs and view MSAP properties

Use this procedure to list MSAPs and view MSAP properties.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Click on the Select Object Type button and choose Access Interface (Service Management) from the list.

3 Perform one of the following to display the MSAPs associated with each service:

- **a** For VPLS MSAPs:
  - **i** Click on the L2 Access Interface (Service Management).
  - **ii** Click on the Abstract L2 Access Interface (VPLS) icon.
  - **iii** Click on the L2 Access Interface (VPLS) icon.
  - **iv** Click on the VPLS L2 Access Interface icon.
  - **v** Choose VPLS MSAP and click on the Search button.
- **b** For IES MSAPs:
  - **i** Click on the Service Access Point icon (Service Management).
  - **ii** Click on the IES Service Access Point (IES) icon.
  - **iii** Choose IES MSAP and click on the Search button.
- **c** For VPRN MSAPs:
  - **i** Click on the Service Access Point icon (Service Management).
  - **ii** Click on the VPRN Service Access Point (VPRN) icon.
  - **iii** Choose VPRN MSAP and click on the Search button.

4 Choose an MSAP from the list and click on the MSAP Properties tab button to view the MSAP properties.

Procedure 64-10 To delete an MSAP policy

Use this procedure to delete any MSAP policy on an MSAP that is an inactive state. Ensure that the MSAP is inactive and that the policy is not associated with other MSAPs that may be used at a later date. Do not attempt to delete MSAP policies on MSAPs that are in an active state.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber form appears.

2 In the Manage Residential Subscriber form, choose the Policy scope.

3 Click on the Select Object Type button and choose MSAP Policy (MSAP Policy). The MSAP Policy (MSAP Policy) list window appears.

4 Click on the Search button in the Manage Residential Subscriber form. The MSAP policies are listed in the MSAP Policy list window.

5 Choose one or more MSAP policies that you need to delete.

6 Click on the Delete button. A dialog box appears.

7 Click on the Yes button in the dialog box. The MSAP policy is deleted.

Procedure 64-11 To modify and re-evaluate an MSAP policy on an MSAP

Use this procedure to re-apply an MSAP policy on an existing MSAP. MSAPs cannot be edited; however, MSAP policies on existing MSAPs can be changed and re-applied.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form appears.

2 Configure the filter criteria. See Procedure 64-9 for more information about configuring the filter to list MSAPs. A list of MSAPs for the service appears.

3 Choose an MSAP and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Click on the MSAP Properties tab button.

5 Click on the Properties button in the Creation MSAP Policy area and enter your required changes.

   i Click on the Apply button.

   ii Click on the OK button.

6 Click on the MSAP Properties tab button.

7 Choose the Do Action option from the Creation MSAP Policy Re-evaluation parameter to apply the policies new parameter values. When you choose Not Applicable, the new parameter values in the policy are not applied but remain in the policy until you choose the Do Action option.

8 Click on the Apply button.

9 Click on the OK button.

Procedure 64-12 To modify an MSAP policy and re-evaluate the MSAPs

Use this procedure to re-apply an MSAP policy on existing MSAPs. MSAPs cannot be edited; however, MSAP policies on existing MSAPs can be changed and re-applied.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form appears.

2 Choose the policy scope as required. The policy scope can be Global or Local.

3 Configure the filter criteria to list MSAPs for the service. Choose MSAP Policy (MSAP Policy) and click on the Search button. A list of MSAP policies appears in the form.

4 Choose an MSAP policy and click on the Properties button. The MSAP Policy (Edit) form appears with the General tab displayed.

5 Enter your required changes.

   i Click on the Apply button.

   ii Click on the OK button.

6 Click on the Reevaluate MSAPs button. The MSAPs are re-evaluated with the changed MSAP policy.

7 Click on the Apply button.

8 Click on the OK button.

Procedure 64-13 To view an MSAP event log, modify the global MSAP log policy, and purge MSAP log records

Use this procedure to view the event log for an MSAP, modify the global MSAP log policy, or purge the log records in an MSAP event log.

1 Perform Procedure 64-9 to list the MSAPs and choose the appropriate MSAP.

2 Click on the Events tab button to display the MSAP event log.

3 If you need to view an event log record, choose a record from the event log and click on the Properties button. The Statistics Record - MSAP Event Log form opens and displays the MSAP record properties.

4 Close the Statistics Record - MSAP Event Log form.

5 If you need to modify the global MSAP event log policy click on the Log Policy button. The Log Policy - Ressubscr. MSap Event Log form opens.

Note — The global MSAP log policy affects all MSAP event logs.

6 Configure the parameters:

- Retention Time (hours)
- Administrative State

7 Click on the Apply button to save the changes.

8 Close the Log Policy - Ressubscr. MSap Event Log form.

9 If you need to purge the MSAP event log records, click on the Purge Log Records button.

10 Click on the OK or Cancel button to close the Log Policy - Ressubscr. MSap Event Log form.

11 Click on the Close button to close the Statistics Record - MSAP Event Log form.

Procedure 64-14 To delete an MSAP

Use this procedure to delete any MSAP that is an inactive state. Verify that the MSAP is in an inactive state. The 5620 SAM prevents attempts to delete an MSAP that is in an active state.

1 Perform Procedure 64-9 to list the MSAPs and choose the appropriate MSAP to delete.

2 Click on the Delete button. A dialog box appears.

3 Click on the Yes button in the dialog box. The MSAP is deleted.

Procedure 64-15 To create or modify a subscriber explicit map

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following.

a Create a subscriber explicit map entry.

i Click on the Create button and choose Create Subscriber Explicit Map Entry from the drop-down menu. The Subscriber Explicit Map Entry (Create) form opens.

ii Go to step 3.

b Modify a subscriber explicit map entry.

Caution — Modifying an active subscriber explicit map entry is potentially service-affecting. Ensure that you consider the implications of reconfiguring the subscriber explicit map entry before you proceed.

i Choose Subscriber Explicit Map Entry from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of subscriber explicit map entries appears.

iii Select a subscriber explicit map entry and click on the Properties button. The Subscriber Explicit Map Entry (Edit) form opens.

3 Configure the parameters:

- Subscriber Identification
- Description
- Subscriber ID Alias

The Subscriber Identification parameter is configurable only during subscriber explicit map creation.

4 Click on the Select button in the Subscriber Profile panel to associate a subscriber profile with the subscriber explicit map. The Select Subscriber Profile form opens.

5 Select a subscriber profile and click on the OK button. The Select Subscriber Profile form closes, and the Subscriber Explicit Map Entry (Create) form refreshes with the subscriber profile.

6 Click on the Select button in the SLA Profile panel to associate an SLA profile with the subscriber explicit map. The Select SLA Profile form opens.

7 Select an SLA profile and click on the OK button. The Select SLA Profile form closes and the Subscriber Explicit Map Entry (Create) form refreshes with the SLA profile.

8 Click on the Select button in the Application Profile panel to associate an application profile with the subscriber explicit map. The Select Application Profile form opens.

9 Select an application profile and click on the OK button. The Select Application Profile form closes and the Subscriber Explicit Map Entry (Create) form refreshes with the application profile.

Note 1 — The global AA group policy must be manually distributed to the NE before a global subscriber identification policy using the application profiles can be distributed.

Note 2 — When a new subscriber identification or subscriber explicit map is discovered from the NE, the AA group policy is not automatically resynchronized to the global subscriber identification policy.

10 Click on the OK button to close the Subscriber Explicit Map (Create) form.

Procedure 64-16 To create or modify an ANCP policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Perform one of the following:

- **a** Create an ANCP policy.
  - **i** Click on the Create button and choose Create ANCP Policy from the drop-down menu. The ANCP (Create) form opens.
  - **ii** Go to step 3.
- **b** Modify an ANCP policy.
  - **i** Choose an ANCP policy from the object drop-down list of the Manage Subscriber Policies form.
  - **ii** Configure the filter criteria and click on the Search button. A list of ANCP policies appears.
  - **iii** Select an ANCP policy and click on the Properties button. The ANCP Policy (Edit) form opens.

3 Configure the Displayed Name parameter.

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Configure the following parameters in the Ingress panel:

- Rate Adjustment
- Rate Reduction (kbps)
- Rate Monitor (kbps)
- Rate Modification
- Rate Monitor Notification
- Rate Modification Scheduler

  The Rate Modification Scheduler parameter is configurable when the Rate Modification parameter is set to Scheduler.

5 Configure the following parameters in the Egress panel:

- Rate Adjustment
- Rate Reduction (kbps)
- Rate Monitor (kbps)
- Rate Modification
- Rate Monitor Notification
- Rate Modification Scheduler

  The Rate Modification Scheduler parameter is configurable when the Rate Modification parameter is set to Scheduler.

6 Configure the following parameters in the Port Down panel:

- Disable SHCV
- Disable SHCV Notification
- Disable SHCV Hold Time (seconds)

7 Click on the OK button to close the ANCP Policy (Create) form.

Procedure 64-17 To create or modify a PPPoE policy

The 5620 SAM supports PPPoE configuration on the 7750 SR and the 7710 SR.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Choose PPPoE Policy (pppoe) from the object drop-down list in the Manage Subscriber Policies form.

3 Perform one of the following:

a Create a PPPoE policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create PPPoE Policy. The PPPoE Policy, Global Policy (Create) form opens.

iii Go to step 4.

b Modify a PPPoE policy.

i Configure the filter criteria and click on the Search button. A list of PPPoE policies appears.

ii Select a PPPoE policy and click on the Properties button. The PPPoE Policy (Edit) form opens.

4 Configure the parameters:

- Displayed Name
- Description
- PPP MTU (octets)
- LCP Keep Alive Interval (seconds)
- LCP Keep Alive Hold Up Multiplier
- Disable AC Cookies
- PADO Delay (100's of milliseconds)
- Maximum Sessions Per MAC
- Enable Reply On PADT

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Apply button. The PPPoE Policy (Edit) form refreshes with the policy configuration mode information.

6 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab button. A list of NEs appears. See Procedure 43-1 for more information about distributing a policy.

7 Click on the Options tab. A list of options appears.

8 Perform one of the following:

a To add an option, go to step 12.

b To edit an existing option, go to step 9.

9 Choose an option from the list.

10 Click on the Properties button. The PPPoE Option (Edit) form opens.

11 Go to step 13.

12 Click on the Add button. The PPPoE Option (Create) form opens.

13 Configure the parameters:

- Option Protocol
- Number
- Option Type
- Option Value
- IP Address

14 Click on the OK button to close the PPPoE Option (Create) form. A dialog box appears.

15 Click on the OK button. The PPPoE Option (Create) form closes.

Procedure 64-18 To create or modify a host tracking policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Choose Host Tracking Policy (Residential Subscriber) from the object drop-down list in the Manage Residential Subscriber Policies form.

3 Perform one of the following:

a Create a host tracking policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create Host Tracking Policy. The Host Tracking Policy, Global Policy (Create) form opens.

iii Go to step 4.

b Modify a host tracking policy.

i Configure the filter criteria and click on the Search button. A list of host tracking policies appears.

ii Select a host tracking policy and click on the Properties button. The Host Tracking Policy (Edit) form opens.

4 Configure the parameters:

- Displayed Name
- Description
- Rate Modification
- Rate Modification Scheduler

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Apply button. The Host Tracking Policy (Edit) form refreshes with the policy configuration mode information.

6 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab button. A list of NEs appears. See Procedure 43-1 for more information about distributing a policy.

7 Close the Host Tracking Policy (Edit) form.

Procedure 64-19 To create or modify an IGMP policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Choose IGMP Policy (Residential Subscriber) from the object drop-down list in the Manage Residential Subscriber Policies form.

3 Perform one of the following:

a Create an IGMP policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create IGMP Policy. The IGMP Policy, Global Policy (Create) form opens.

iii Go to step 4.

b Modify an IGMP policy.

i Configure the filter criteria and click on the Search button. A list of IGMP policies appears.

ii Select an IGMP policy and click on the Properties button. The IGMP Policy (Edit) form opens.

4 Configure the parameters:

- Displayed Name
- Description
- Import Policy
- Maximum Number of Groups
- Administrative Version
- Fast Leave

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Apply button. The IGMP Policy (Edit) form refreshes with the policy configuration mode information.

6 Click on the Static Group/Source tab button. A list of multicast static group/static source address pairs appears.

7 Perform one of the following:

a Select an address pair from the list and click on the Properties button. The IGMP Policy Static (Edit) form appears. Go to step 8.

b Click on the Add button. The IGMP Policy Static (Create) form appears. Go to step 8.

8 Configure the parameters:

- Static Multicast Group
- Static Source

9 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab button. A list of NEs appears. See Procedure 43-1 for more information about distributing a policy.

10 Close the IGMP Policy (Edit) form.

Procedure 64-20 To configure a BGP Peering policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Choose BGP Peering Policy (Residential Subscriber) from the object drop-down list in the Manage Residential Subscriber Policies form.

3 Perform one of the following:

a Create a BGP Peering policy.

i Click on the Create button. A drop down menu appears.

ii Choose Create BGP Peering Policy. The BGP Peering Policy, Global Policy (Create) form opens.

iii Go to step 4.

b Modify a BGP Peering policy.

i Configure the filter criteria and click on the Search button. A list of BGP Peering policies appears.

ii Select a BGP Peering policy and click on the Properties button. The BGP Peering Policy (Edit) form opens.

4 Configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Displayed Name
- Description
- Cluster ID
- Local Address
- BGP Keychain
- MED Source
- MED Value

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

5 Click on the Apply button. The BGP Peering Policy (Edit) form refreshes with the policy configuration mode information.

6 Click on the Behavior tab button and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Preference
- Local Preference
- Multi Hop
- Loop Detect
- Aggregator ID Zero
- Damping
- Disable Client Reflect
- Min Route Advertisement (seconds)
- Disable Standard Communities
- Disable Extended Communities
- Disable Fast External Failover
- Advertise Inactive Routes
- Peer Type
- Passive
- Next Hop Self
- Minimum TTL Value
- Connect Retry Time (seconds)
- Keep-Alive (seconds)
- Hold Time (seconds)
- Prefix Limit

7 Click on the AS Properties tab button and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Peer AS
- Min Origination AS (seconds)
- Disable 4Byte ASN
- AS Override
- Local AS
- Remote Private AS

8 Click on the Import Policies tab button and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Import Policy 1
- Import Policy 2
- Import Policy 3
- Import Policy 4
- Import Policy 5

9 Click on the Export Policies tab button and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- Export Policy 1
- Export Policy 2
- Export Policy 3
- Export Policy 4
- Export Policy 5

10 Click on the Authentication tab button and configure the parameters:

If the Inherit Value box is enabled for a parameter, the parameter value is inherited from the parent BGP object.

- MD5 Authentication
- Authentication Key

11 To distribute the policy to an NE, if a local definition does not exist, click on the Local Definitions tab button. A list of NEs appears. See Procedure 43-1 for more information about distributing a policy.

12 Close the BGP Peering Policy (Edit) form.

Procedure 64-21 To configure a diameter policy

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Residential Subscriber Policies form opens.

2 Perform one of the following.

a Create a diameter policy.

i Click on the Create button and choose Diameter Policy from the drop-down menu. The Diameter Policy (Create) form appears with the General tab displayed.

ii Go to step 3.

b Modify a diameter policy.

Caution — Modifying an active diameter policy is potentially service-affecting. Ensure that you consider the implications of reconfiguring the diameter policy before you proceed.

i Choose Diameter Policy from the object drop-down list.

ii Configure the filter criteria and click on the Search button. A list of diameter policies appears.

iii Select a diameter policy and click on the Properties button. The Diameter Policy (Edit) form opens.

3 Configure the parameters:

- Name
- Description

4 On the Connection Origin panel, configure the Virtual Router Type parameter.

If you specified VPRN Service as the Virtual Router Type, you must also configure the Service Name parameter on the VPRN Service panel. Click on the Select button and choose a VPRN service from the Select VPRN Service - Diameter Policy form.

5 Configure the timer parameters:

- Watchdog Timer (seconds)
- Connection Timer (seconds)
- Transaction Timer (seconds)

6 Click on the DCAA Parameters tab button.

7 Configure the parameters:

- Failover Support
- Failure Handling
- Tx Timer (seconds)
- Service Context ID
- RADIUS Called-Station-Id
- Include RADIUS User
- Origin Subscription ID
- Subscription ID Type

8 Click on the Peers tab button.

9 Click on the Add button. The Diameter Peer - Diameter Policy (Create) form appears with the General tab displayed.

10 Configure the parameters:

- Name
- Description
- Administrative State
- Preference
- IP Address
- Port Number
- Protocol
- Destination Host
- Destination Realm

11 If you want to specify local override settings for any of the timer settings for the peer, deselect the Inherit Value check box and then specify a value for any of the following timer parameters:

- Watchdog Timer (seconds)
- Connection Timer (seconds)
- Transaction Timer (seconds)

Note — When the Inherit Value check box is selected for a timer parameter on a peer object, the timer value is inherited from the parent diameter policy.

12 Click on the OK button on Diameter Peer - Diameter Policy (Create) form. The Diameter Policy (Create) form reappears with the new peer displayed on the Peers tab.

13 Click on the OK button in the Diameter Policy (Create) form. The Manage Residential Subscriber Policies form reappears with the new diameter policy displayed in the list.

14 Close the Manage Residential Subscriber Policies form.

Procedure 64-22 To manage residential subscriber management components on a SAP

Perform this procedure to manage the subscriber configuration on one or more SAPs. You can configure the subscriber-related SAP parameters and assign one or more of the following residential subscriber management components:

- subscriber identification policy
- default subscriber identification string
- default subscriber profile
- default SLA profile
- non-subscriber traffic subscriber profile
- non-subscriber traffic SLA profile

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Click on the Components tab button.

5 Navigate to the Access Interfaces icon below a site. The path is *service_type*→Site→Access Interfaces.

6 Click on the Access Interfaces icon to display the site SAPs.

7 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.

Note 1 — You can configure subscriber management on multiple SAPs at once from any list of SAP search results that the 5620 SAM generates. For simplicity, the procedure uses the term SAP to mean one or more SAPs, and focuses only on SAPs that belong to the same service site.

Note 2 — The 5620 SAM commits changes to a SAP configuration only when subscriber management is enabled on all SAPs that you are configuring.

8 Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

9 Click on the Profiles tab button.

10 Perform one of the following steps for a component.

a Associate a component with the SAP.

i Click on the Select button beside the component in the Policies panel. The component Select Default form opens.

ii Select a component and click on the OK button. The component Select Default form closes, and the Policies panel refreshes with the component name.

b Remove a component, or replace an existing component with a new component.

Caution — Removing or replacing a residential subscriber management component on a SAP that is in use by subscriber hosts can be service-affecting to hosts that attempt to join the network. Ensure that removing the component does not affect the subscriber hosts before you proceed.

i Click on the Clear button beside the component in the Policies panel. The 5620 SAM removes the component from the Policies panel.

ii If you want to choose a component to replace the removed component, go to step 10 a.

11 Click on the OK button. The SAP configuration form closes.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The service configuration form closes.

14 Close the Manage Services form.

Procedure 64-23 To enable or disable residential subscriber management on a SAP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Click on the Components tab button.

5 Navigate to the Access Interfaces icon below a site. The path is *service_type*→Site→Access Interfaces.

6 Click on the Access Interfaces icon to display the site SAPs.

7 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.

8 Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

9 Click on the Profiles tab button.

10 Configure the Admin Status parameter by performing one of the following.

a Set the parameter to Enabled to enable residential subscriber management on the SAP.

b Set the parameter to Disabled to disable residential subscriber management on the SAP.

11 Click on the OK button. The SAP configuration form closes.

12 Click on the OK button. A dialog box appears.

13 Click on the Yes button. The service configuration form closes.

14 Close the Manage Services form.

Procedure 64-24 To create a static host for residential subscriber management on a SAP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Click on the Components tab button.

5 Navigate to the SAPs that support subscriber management. Perform one of the following, depending on the type of service that you are configuring:

a For an IES, the path is IES→Site→Subscriber Interfaces→*subscriber interface*→*group interface*→Service Access Points→*SAP*.

b For a VPLS, the path is VPLS→Site→Access Interfaces→*SAP*.

c For a VPRN service, the path is VPRN→Site→Subscriber Interfaces→*subscriber interface*→*group interface*→Service Access Points→*SAP*.

6 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.

7 Click on the Anti-Spoofing tab button. The General tab is displayed.

8 Configure the Anti-Spoofing parameter.

Note — You must set the Anti-Spoofing parameter to IP-address matching or to IP- and MAC-address matching before you can enable subscriber management for the static hosts on a SAP.

9 Click on the Static Hosts tab button.

10 Click on the Add button. The Access Interface Anti-Spoofing Static Host (Create) form opens with the General tab displayed.

11 Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification
- Use SAP ID as Subscriber ID
- ANCP String
- Intermediate Destination ID

Note — To enable residential subscriber management for a static host, you must specify values for the IP Address and Subscriber Identification parameters.

12 Configure the Administrative State parameter.

13 Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with a list of available subscriber profiles.

Note — To enable residential subscriber management for a static host, you must specify a subscriber profile.

14 Select a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

15 Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host, if required. The Select SLA Profile - AntiSpoofingStaticHosts form opens with a list of available SLA profiles.

Note — To enable residential subscriber management for a static host, you must specify an SLA profile.

16 Select an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

17 Click on the Select button in the Application Profile panel to choose an application profile for the static host, if required. The Select Application Profile - AntiSpoofingStaticHosts form opens with a list of local application profiles.

18 Select an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

19 Click on the OK button.

Note — The Administrative State parameter must be set to Up, to enable validation of Subscriber Identification, Subscriber Profile, and Application Profile.

Partially configured Static Hosts can be configured if the Administrative State parameter is set to Down.

20 Click on the Managed Routes tab button.

21 Click on the Add button.

22 The Access Interface Anti-Spoofing Static Host Managed Route Display (Create)form opens.

23 Configure the parameters:

- IP Address
- Prefix Length

24 Click on the OK button. A dialog box appears.

25 Click on the OK button.The Access Interface Anti-Spoofing Static Host Managed Route Display (Create) form closes.

Note — The creation of 16 managed routes is supported for each static host on IES and VPRN SAPs on the 7750 SR, 7450 ESS, and 7710 SR, Release 6.1 or later.

26 Click on the Apply button if you want to create an additional static host entry. A dialog box appears. Otherwise go to step 28.

27 Repeat steps 11 to 25 for each additional static host entry that you want to create.

28 Click on the OK button. A dialog box appears.

29 Click on the OK button. The Access Interface Anti-Spoofing Static Host (Create) form closes, and the SAP configuration form refreshes with the new static host entries.

30 Click on the OK button. The SAP configuration form closes.

31 Click on the OK button. A dialog box appears.

32 Click on the Yes button. The service configuration form closes.

33 Close the Manage Services form.

Procedure 64-25 To configure a MEP on a SAP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Click on the Components tab button.

5 Perform one of the following steps.

a To create a MEP on an Access Interface SAP, navigate to the Access Interfaces icon below a site. The path is *service_type*→Site→Access Interfaces.

b To create a Down MEP on a Subscriber Group Interface SAP, navigate to the Subscriber Group Interfaces icon below a site. The path is *service_type*→Site→Subscriber Interfaces→Group Interfaces. Go to step 7.

Note 1 — MEPs can be configured on an Access Interface SAP for VPLS, VPRN, IES, and VLL Epipe services.

Note 2 — Down MEPs can be configured on a Subscriber Group Interface SAP for VPRN and IES.

6 Click on the Access Interfaces icon to display the site SAPs. Go to step 8.

7 Click on the Group Interfaces icon to display the site SAPs.

8 Select one or more SAPs, right-click, and choose Properties. The SAP configuration form opens with the General tab displayed.

9 Click on the MEP tab button.

10 Click on the Add button. The MEP (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Auto-Assign ID
- ID
- Site ID
- Direction
- Administrative State
- CCM Messages
- Control MEP
- Priority Level for CCM Messages
- Low-priority Defect
- Mac Address
- Fault Propagation
- Type
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

The Control MEP parameter is only displayed if the SAP, BINDING or PATH ENDPOINT parameter is set to Ethernet Tunnel Path Endpoint.

Note — When configuring a Down MEP on a Subscriber Group Interface SAP, the Direction parameter cannot be configured.

12 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step 16.

13 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

14 Click on the AIS tab button.

15 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

16 Click on the OK button. A dialog box appears.

17 Click on the OK button. The MEP (Create) form closes.

18 Close the Manage Services form.

Procedure 64-26 To configure a MEP on an SDP Binding

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Click on the Components tab button.

5 Navigate to the Spoke SDP Bindings icon below a site. The path is *service_type*→Site→Spoke SDP Bindings.

Note — MEPs can be configured on a SDP Binding for VPLS, VPRN, and VLL Epipe services.

6 Click on the Spoke SDP Bindings icon to display the site Spoke SDP Bindings.

7 Select one or more Spoke SDP Bindings, right-click, and choose Properties. The Spoke SDP Bindings configuration form opens with the General tab displayed.

8 Click on the Meps tab button.

9 Click on the Add button. The MEP (Create) form opens.

10 Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

11 Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

12 Configure the parameters:

- Auto-Assign ID
- ID
- Site ID
- Direction
- Administrative State
- CCM Messages
- Priority Level for CCM Messages
- Low-priority Defect
- Mac Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

13 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step 17.

14 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

15 Click on the AIS tab button.

16 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

17 Click on the OK button. A dialog box appears.

18 Click on the OK button. The MEP (Create) form closes.

19 Close the Manage Services form.

Procedure 64-27 To modify the primary subscriber identification script or URL

This procedure allows a 5620 SAM operator to modify the primary subscriber identification script without service disruption. Perform this procedure only when the primary script and URL are operational.

Caution — Modifying the primary subscriber identification script is potentially service-affecting if no functional backup script is administratively enabled. Modifying a backup (secondary or tertiary) subscriber identification script is unlikely to be service-affecting if the other backup script (secondary or tertiary) functions properly and is administratively enabled. Ensure that at least one administratively enabled backup script is accessible to the 5620 SAM and the NEs to which it applies before you proceed.

1 Choose Policies→Residential Subscriber from the 5620 SAM main menu. The Manage Subscriber Policies form opens.

2 Choose Subscriber Identification Policy from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of subscriber identification policies appears.

4 Select a subscriber identification policy and click on the Properties button. The Subscriber Identification Policy (Edit) form opens with the General tab displayed.

5 Copy the operational primary script URL to the secondary position. This action ensures that an operational backup script is in place in the event that there is a problem with the new primary script or URL.

   i Set the Secondary Script Administrative State parameter to disabled.

   ii Click on the Apply button. A dialog box appears.

   iii Click on the Yes button. The 5620 SAM administratively disables the secondary script.

   iv Configure the Secondary Script URL parameter with the value of the Primary Script URL parameter.

   v Set the Secondary Script Administrative State parameter to enabled.

vi Click on the Apply button. A dialog box appears.

vii Click on the Yes button. The 5620 SAM administratively enables the secondary script.

Note — You must administratively disable and enable a script URL to cause the NEs to which the subscriber identification policy applies to load the script using the URL.

6 Modify a renamed copy of the former primary script or create a replacement script, as required; record the new or modified script URL.

7 Configure the new URL as the primary script URL.

i Set the Primary Script Administrative State parameter to Disabled.

ii Click on the Apply button. A dialog box appears.

iii Click on the Yes button. The 5620 SAM administratively disables the primary script. The secondary (former primary) script is the active script.

iv Configure the Primary Script URL parameter with the new URL value.

v Set the Primary Script Administrative State parameter to Enabled.

vi Click on the Apply button. A dialog box appears.

vii Click on the Yes button. The 5620 SAM administratively enables the primary script. The new primary script is the active script.

Note — You must administratively disable and enable a script URL to cause the NEs to which the subscriber identification policy applies to load the script using the URL.

8 Click on the OK button. A dialog box appears.

9 Click on the Yes button. The Subscriber Identification Policy (Edit) form closes.

10 Close the Manage Subscriber Policies form.

Procedure 64-28 To configure NE SHCV event handling

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Click on the View SHCV button. The Subscriber Host Connectivity Verification form opens.

3 Choose Network Element SHCV from the object drop-down list.

4 Configure the filter criteria and click on the Search button. A list of NEs appears.

5 Select an NE and click on the Properties button. The Network Element SHCV (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Trap Dropped Raises Alarm
- Rate Exceeded Raises Alarm
- Maximum Host Lost Connectivity Rate (traps per second)

7 Click on the OK button. The Network Element SHCV (Edit) form closes, and a dialog box appears.

8 Click on the Yes button.

9 Close the Subscriber Host Connectivity Verification form.

10 Close the Manage Residential Subscribers form.

Procedure 64-29 To rename a subscriber

Perform this procedure to change the identification of a subscriber, for example, when you no longer want hosts on the SAP to use the SAP ID as the subscriber ID.

Caution 1 — Renaming a subscriber can be service-affecting because it changes the subscriber identification string of all associated subscriber hosts. Before you proceed, ensure that no subscriber hosts require the subscriber identification string associated with this subscriber.

Caution 2 — Renaming a subscriber changes the SAP default subscriber identification strings that are associated with it.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscribers appears.

4 Select a residential subscriber and click on the Modify button. The Residential Subscriber (Edit) form opens with the General tab displayed.

5 Configure the New Subscriber Identification parameter.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The 5620 SAM renames the subscriber.

8 Close the Manage Residential Subscribers form.

Procedure 64-30 To view SHCV log events

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Click on the View SHCV button. The Subscriber Host Connectivity Verification form opens.

3 Choose SHCV Event Log from the object drop-down list.

4 Configure the filter criteria and click on the Search button. A list of NE SHCV event logs appears.

5 Select a log entry and click on the Properties button. The SHCV Log Entry form opens.

6 View the log entry.

7 Close the SHCV Log Entry form.

8 Close the Subscriber Host Connectivity Verification form.

9 Close the Manage Residential Subscribers form.

Procedure 64-31 To view or configure active residential subscriber hosts on a SAP

Note — The 5620 SAM does not automatically display a list of all active hosts on a SAP because the number of hosts on a SAP is potentially large and may take a long time to retrieve. You must request the list of hosts on a SAP. The 5620 SAM prompts you for confirmation before retrieving the list of hosts.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a service and click on the Properties button. The service configuration form opens with the General tab displayed.

4 Click on the Components tab button.

5 Navigate to the Access Interfaces icon below a site. The path is *service_type*→Site→Access Interfaces.

6 Click on the Access Interfaces icon to display the site SAPs.

7 Select a SAP, right-click, and choose Properties. The SAP configuration (Edit) form opens with the General tab displayed.

8 Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

9 Click on the Subscriber Hosts tab button.

10 Click on the Find button. A confirmation prompt appears.

11 Click on the Yes button. The list of subscriber hosts refreshes with the active subscriber host entries.

12 To view the information for a subscriber host, select the host entry and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed.

13 If the subscriber host is a static host, go to step 20.

14 Configure the Subscriber Profile String parameter for the dynamic host or PPPoE host, if required. Click on the Select button to choose a subscriber profile string from the Subscriber Profile String - Subscriber Host form.

Caution — Changing the subscriber profile string directly on a subscriber host is potentially service-affecting to all hosts on all SAPs that belong to the subscriber. Because a subscriber is associated with only one subscriber profile, when you change the subscriber profile string for one host, all dynamic or PPPoE hosts associated with the subscriber on all SAPs are automatically configured with the new subscriber profile.

15 Configure the SLA Profile String parameter for the dynamic host or PPPoE host, if required. Click on the Select button to choose an SLA profile from the SLA Profile - Subscriber Host form.

16 Configure the Application Profile parameter for the dynamic host PPPoE host, if required. Click on the Select button to choose an application profile string from the Application Profile String - Subscriber Host form.

Caution — Changing the application profile string directly on a subscriber host is potentially service-affecting to all hosts on all SAPs that belong to the subscriber. Because a subscriber is associated with only one application profile, when you change the application profile string for one host, all dynamic or PPPoE hosts associated with the subscriber on all SAPs are automatically configured with the new application profile.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The Subscriber Host form closes.

19 Go to step 21.

20 Click on the Cancel button to close the Subscriber Host form.

21 Click on the OK button. The SAP configuration form closes.

22 Close the Manage Services form.

Procedure 64-32 To perform DHCP lease management for a subscriber host

DHCP is used to assign IP addresses to hosts or workstations on the network. This function is usually performed by a DHCP server. Essentially, it “leases” out addresses for specific times to the various hosts. If a host does not use a specific address for a set period of time, that IP address can then be assigned to another machine by the DHCP server.

In order to allow the DHCP client to lease out address for specific times, the 5620 SAM allows an operator to force the DHCP client to change its state by sending a renewal command. Upon receipt of the renewal command from the 5620 SAM, the DHCP client changes to the renewal state and then negotiates with the DHCP server for lease times.

Conversely, an operator can also terminate (clear) a lease for a particular host from within the Residential Subscriber Host form of 5620 SAM.

Note — The DHCP lease renewal and termination are supported only on dynamic hosts, not on static hosts or subscriber hosts.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Select Residential Subscriber Host from the object drop-down list.

3 Click on the Search Subscriber Host Information from Last Resynch radio button.

4 Click on the Select button beside Site ID to specify an NE. The Select an ESM Capable Network Element form opens.

5 Select an NE in the list and click on the OK button. The Select an ESM Capable Network Element form closes and the NE system IP address is displayed on the Manage Residential Subscribers form.

6 Configure the Service ID parameter.

7 Click on the Select button beside Port to specify a port. The Select Port form opens.

8 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed on the Manage Residential Subscribers form.

9 Configure the Inner Encapsulation Value and Outer Encapsulation Value parameters.

Note — The Outer Encapsulation Value parameter is configurable only when the port encapsulation type is Dot1 Q or Q in Q. The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is Q in Q.

10 Click on the Search button. A list of subscriber hosts is displayed.

11 Select one or more entries in the list.

Note — You can renew a lease for multiple entries. However, you can perform a lease termination for only one host at a time.

12 Perform one of the following steps.

a To renew the lease, click on the Force Renew button.

b To terminate the lease, click on the Clear Lease State button.

13 A dialog box appears. Click on the Yes button. The action is completed.

14 Close the Manage Residential Subscribers form.

Procedure 64-33 To view subscriber host information

ESM Dynamic Host Persistence provides persistence of subscriber host information of properties that bind a host to a SAP, an IP address or a MAC address. This provides troubleshooting functionality while avoiding unnecessary and unscalable network queries. Only the properties of the subscriber host which are required to tie the host to other objects for troubleshooting, since there are no statistics and no OAM tests for subscriber hosts, are persisted.

Note — Only IPoE (DHCP and ARP) and IPOE-DHCP6 hosts can be persisted in the 5620 SAM.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Host from the object list.

3 Click on the Search Subscriber Host Information from Last Resynch radio button.

4 View the available read-only attributes.

5 If required, click on the Resync Subscriber Host Table button. The ESM Capable Network Element form opens.

6 Select one or more NEs. Click on the OK button. A dialog box opens.

7 Click on the check box. Click on the Yes button.

8 The Select an ESM Capable Network Element form closes.

9 To retrieve the SAPs on which a subscriber host with an IP address resides, perform the following steps:

Note — You can also retrieve DHCP, PPPoE sessions, and ARP host information on demand from the Manage→Residential Subscribers→Manage Residential Subscriber form menu options.

i Click on the Search Current Subscriber Host Information radio button.

ii Click on the Select button beside Site ID to specify an NE. The Select an ESM Capable Network Element form opens.

iii Select an NE in the list and click on the OK button. The Select an ESM Capable Network Element form closes and the NE system IP address is displayed on the Manage Residential Subscribers form.

iv Configure the Service ID parameter.

v Click on the Select button beside Port to specify a port. The Select Port form opens.

vi Select a port in the list and click on the OK button. Configure the Inner Encapsulation Value and Outer Encapsulation Value parameters. The Select Port form closes and the port identifier is displayed on the Manage Residential Subscribers form.

vii Click on the Search button.

viii View the available read-only attributes.

ix Close the Manage Residential Subscribers form.

Procedure 64-34 To configure a local user database

A local user database is used by a local DHCP server to authenticate DHCP clients that request IP addresses. A group interface uses the local user database to authenticate a PPPoE clients that request IP addresses.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Local User Database (localuserdb) from the object drop-down list.

3 Perform one of the following steps:

a To create a local user database, click on the Create Local User Database button. A Local User Database (Create) window opens with the General tab displayed. Go to step 6.

b To modify an existing database, click on the Search button. A list of existing databases is displayed. Go to step 4.

4 Choose a database from the list.

5 Click on the Properties button. The Local User Database (Edit) form opens with the General tab displayed.

6 Click on the Select button in the Site panel to specify an NE. The Select a Local User Database Capable Network Element form opens.

7 Select an NE in the list and click on the OK button. The Select a Local User Database Capable Network Element form closes and the NE system address is displayed on the Local User Database (Create) form.

8 Configure the parameters.

- Displayed Name
- Description
- Administrative State

9 Click on the DHCP tab button. The DHCP Match List form is displayed.

10 Configure the parameters.

- Match Type DHCP 1
- Match Type DHCP 2
- Match Type DHCP 3
- Match Type DHCP 4

11 Click on the Masks tab button.

12 Click on the Add button. The Local User Database Dhcp Mask form is displayed.

13 Configure the parameters:

- Match Type
- Prefix String
- Prefix Length
- Suffix String
- Suffix Length

14 Click on the Hosts tab button.

15 Click on the Add button. The Local User DB DHCP Host (Create) form opens with the General tab displayed.

16 Configure the parameters:

- Host Name
- Administrative State
- Domain Name
- Server Address

17 Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - Local User DB DHCP Host form opens.

18 Configure the filter criteria. A list of available policies appears.

19 Select a policy and click on the OK button. The Select Subscriber Authentication Policy - Local User DB DHCP Host form closes, and the Local User DB DHCP Host (Create) form reappears with the policy name information displayed.

20 Click on the Select button in the MSAP Defaults panel to choose an MSAP Policy Name. The MSAP Policy - Local User DB DHCP Host form opens.

Note — You can also enter text in the fields next to the MSAP Policy Name, MSAP Service ID, and MSAP Group Interface Name parameters.

21 Configure the filter criteria. A list of available MSAP policies appears.

22 Select an MSAP policy and click on the OK button. The MSAP Policy - Local User DB DHCP Host form closes, and the Local User DB DHCP Host (Create) form appears with the MSAP policy name displayed.

23 Click on the Select button in the MSAP Defaults panel to choose an MSAP Service ID. The Service - Local User DB DHCP Host form opens with a list of services displayed.

24 Select a service and click on the OK button. The Service - Local User DB DHCP Host form closes, and the Local User DB DHCP Host (Create) form appears with the service information displayed.

25 Click on the Select button in the MSAP Defaults panel to choose an MSAP Group Interface Name. The Group Interface - Local User DB DHCP Host form opens with a list of group interfaces displayed.

26 Select a group interface and click on the OK button. The Group Interface - Local User DB DHCP Host form closes, and the Local User DB DHCP Host (Create) form appears with the group interface information displayed.

27 Click on the Address tab button. Configure only one of the following parameters.

- IP Address
- Use GI Address
- IP Address Pool name
- Use Client Pool

28 Configure the IPv6 addressing parameters, if required:

- IPv6 Address
- IPv6 Prefix
- IPv6 Prefix Length

29 Click on the Host Identification tab button. Configure 4 of the following parameters.

- Circuit ID Format
- Circuit ID
- MAC Address
- Option 60
- Remote ID Format
- Remote ID
- SAP ID
- Service ID
- DHCP String
- System ID

30 Click on the Identification Strings tab button. Configure the Option Number parameter. The window is refreshed with additional parameters.

31 Configure the parameters.

- ANCP String
- Application Profile String
- Intermediate Destination ID
- SLA Profile String
- Subscriber Profile String
- Subscriber ID

32 Click on the Options tab button. The Options form is displayed.

33 Click on the Add button. A Local User Database DHCP Option form opens.

34 Configure the Option parameter. Depending on the Option Value different parameters must be configured for each option.

35 Perform one of the following steps:

a Configure Custom Option, Subnet Mask, Default Routers, DNS Name Servers, and Netbios Name Server options. Go to step 36.

- Number
- Type
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

b Configure Lease Time, Lease Renew Time and Lease Rebind Time options. Go to step 36.

- Days
- Hours
- Minutes
- Seconds

c To configure the Domain Name option, configure the Option Value parameter. Go to step 36.

d To configure Netbios Node Type option, configure the Netbios Node Type parameter. Go to step 36.

36 Click on the OK button. A confirmation dialog box appears.

37 Click on the OK button. The Local User Database DHCP Option window closes and the Local User DB DHCP Host (Create) window is refreshed with the new options.

38 Click on the OK button.

39 Click on the PPPoE tab button. The PPPoE Match List form opens.

40 Configure the parameters.

- Match Type PPPoE 1
- Match Type PPPoE 2
- Match Type PPPoE 3

41 Click on the Masks tab button.

42 Click on the Add button. The Local User Database PPPoE Mask form opens.

43 Configure the parameters.

- Match Type
- Prefix String
- Prefix Length
- Suffix String
- Suffix Length

Note — You must configure the Mask Type parameter before you configure the remaining parameters on the Local User Database PPPoE Mask form.

44 Click on the Hosts tab button.

45 Click on the Add button. The Local User DB PPPoE Host (Create) form opens with the General tab displayed.

46 Configure the parameters.

- Host Name
- Administrative State
- Retail Service ID
- PADO Delay

47 Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - Local User DB PPPoE Host form opens.

48 Configure the filter criteria. A list of available policies appears.

49 Choose a policy and click on the OK button. The Select Subscriber Authentication Policy - Local User DB PPPoE Host form closes, and the Local User DB PPPoE Host (Create) form reappears with the policy name displayed.

50 Click on the Select button in the MSAP Defaults panel to choose an MSAP Policy Name. The MSAP Policy - Local User DB PPPoE Host form opens.

Note — You can also enter text in the fields next to the MSAP Policy Name, MSAP Service ID, and MSAP Group Interface Name parameters.

51 Configure the filter criteria. A list of available MSAP policies appears.

52 Select an MSAP policy and click on the OK button. The MSAP Policy - Local User DB PPPoE Host form closes, and the Local User DB PPPoE Host (Create) form appears with the MSAP policy name displayed.

53 Click on the Select button in the MSAP Defaults panel to choose an MSAP Service ID. The Service - Local User DB PPPoE Host form opens with a list of services displayed.

54 Select a service and click on the OK button. The Service - Local User DB PPPoE Host form closes, and the Local User DB PPPoE Host (Create) form appears with the service information displayed.

55 Click on the Select button in the MSAP Defaults panel to choose an MSAP Group Interface Name. The Group Interface - Local User DB PPPoE Host form opens with a list of group interfaces displayed.

56 Select a group interface and click on the OK button. The Group Interface - Local User DB PPPoE Host form closes, and the Local User DB PPPoE Host (Create) form appears with the group interface information displayed.

57 Click on the Address tab button. Configure one of the following parameters:

Note — If more than one IP address parameter is configured, the 5620 SAM displays an error message.

- IP Address
- Use GI Address
- IP Address Pool name
- Use Client Pool

58 Click on the Host Identification tab button. Configure only 3 of the following parameters:

Note 1 — Circuit ID Format and Circuit ID are considered one parameter.

Note 2 — User Name Format and User Name are considered one parameter.

- Circuit ID Format
- Circuit ID
- MAC Address
- Remote ID Format
- Remote ID
- Service Name
- User Name Format
- User Name

59 Configure the following parameters:

- Password Type
- Password

60 Click on the Identification Strings tab button. Configure the Option Number parameter. The window is refreshed with additional parameters.

61 Configure the parameters.

- ANCP String
- Application Profile String
- Intermediate Destination ID
- SLA Profile String
- Subscriber Profile String
- Subscriber ID

62 Click on the L2TP tab button. A list of available tunnel groups appears.

Note — L2TP configuration is required on an NE that has the LAC role if RADIUS authentication is not used for PPPoE clients.

63 Click on the Select button next to the Group Name parameter to choose a tunnel group name. The Select Tunnel Group Name - Local User DB PPPoE Host form opens.

64 Configure the filter criteria and click on the Search button. A list of available tunnels is displayed.

65 Choose a tunnel group and click on the OK button. The Select Tunnel Group Name - Local User DB PPPoE Host form closes, and the Local User DB PPPoE Host (Create) form reappears with the Group Name displayed.

66 Click on the Options tab button.

67 Click on the Add button. A Local User DB PPPoE Option form opens.

68 Configure the parameters:

- Option
- Number
- Type
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Option Value parameter is configurable when the Type parameter is set to ASCII string or Hex String.

69 Click on the OK button. A confirmation dialog box opens.

70 Click on the OK button. The Local User DB PPPoE Host (Create) form is refreshed with the new options.

71 Close the Local User DB PPPoE Host (Create) form.

72 Click on the following tab buttons to view information:

- Local DHCP Servers
- Group Interfaces
- Subscriber Authentication Policies
- Faults

73 Close the Local User Database (Edit) form.

Procedure 64-35 To view a subscriber and the associated subscriber hosts

Note — You can use the 5620 SAM GUI to display the object model associated with 5750 SSC residential subscriber services. See chapter 80 for more information.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscribers appears.

4 Select a residential subscriber and click on the Properties button. The Residential Subscriber (View) form opens with the General tab displayed.

5 View a list of the residential subscriber instances for the subscriber, if required.

i Click on the Residential Subscriber Instances tab button.

ii Select a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

iii View the instance information.

The Residential Subscriber State panel displays the following subscriber status information:

- Active
- Residential Subscriber Creation
- Last Active State Change

iv Close the Residential Subscriber Instance (Edit) form.

6 List and view the active hosts for the subscriber, if required.

i Click on the Subscriber Hosts tab button.

ii Click on the Find button. A confirmation prompt appears.

iii Click on the Yes button. The list of subscriber hosts refreshes with the active subscriber host entries.

iv To view the information for a subscriber host, select the host and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed. Otherwise, go to step 7.

v View the subscriber host information.

vi Close the Subscriber Host form.

7 Close the Residential Subscriber (View) form.

8 Close the Manage Residential Subscribers form.

Procedure 64-36 To view a subscriber instance and the associated subscriber hosts

Note — You can use the 5620 SAM GUI to display the object model associated with 5750 SSC residential subscriber services. See chapter 80 for more information.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Instance from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscriber instances appears.

4 Select a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

The Residential Subscriber State panel displays the following subscriber status information:

- Active
- Residential Subscriber Creation
- Last Active State Change

5 List and view the active hosts for the subscriber instance, if required.

i Click on the Subscriber Hosts tab button.

ii Click on the Find button. A confirmation prompt appears.

iii Click on the Yes button. The list of subscriber hosts refreshes with the active subscriber host entries.

iv To view the information for a subscriber host, select the host and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed. Otherwise, go to step 7.

v View the subscriber host information.

vi Click on the Cancel button to close the Subscriber Host form.

6 List and view the subscriber hosts for which a DHCP lease has been manually terminated, if required.

i Click on the Clear Status tab button.

ii To view the information for a subscriber host, select the host and click on the Properties button. The Subscriber Host form opens with the subscriber host information displayed. Otherwise, go to step 7.

iii View the subscriber host DHCP lease information.

iv Click on the Cancel button to close the Subscriber Host form.

7 View the collected statistics for the subscriber instance, if required.

i Click on the Statistics tab button.

ii Choose a statistics class from the object drop-down list.

iii Click on the Collect button to collect the statistics for the chosen class, or click on the Collect All button to collect the statistics for all classes.

iv Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

v View the statistics information.

vi Click on the Close button to close the statistics record form.

vii Repeat steps ii to vi for each statistics class that you want to view.

8 Click on the Cancel button to close the Residential Subscriber Instance (Edit) form.

9 Close the Manage Residential Subscribers form.

Procedure 64-37 To delete an inactive residential subscriber instance

Use this procedure to remove the record of an inactive residential subscriber instance from the 5620 SAM database. Residential subscriber instances become inactive in the 5620 SAM when the subscriber is deleted from the NE.

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Instance from the object drop-down list.

3 Configure the filter criteria and click on the Search button. A list of residential subscriber instances appears.

The Active property indicates the status of each residential subscriber instance in the list. An inactive residential subscriber instance has no check mark under the Active heading.

4 Select the inactive residential subscriber instance you want to delete and click on the Delete button. The inactive residential subscriber instance is removed from the list.

5 Close the Manage Residential Subscribers form.

Procedure 64-38 To collect, view, and clear host tracking statistics and information

Use this procedure to perform one or more of the following:

- collect, view, and clear on-demand host tracking statistics and information for a residential subscriber instance
- collect, view, and clear on-demand host tracking statistics and information for a VPLS L2 access interface
- collect, view, and clear on-demand host tracking statistics and information for an IES service access point
- collect, view, and clear on-demand host tracking statistics and information for a VPRN service access point
- clear statistics and host tracking information for a VPLS, VPRN, or IES service site
- clear statistics and host tracking information for a residential subscriber host

1 To collect, view, and clear on-demand host tracking statistics and information for a residential subscriber instance.

i Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

ii Choose Residential Subscriber Instance (Residential Subscriber) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of residential subscriber instances appears.

iv Choose a residential subscriber instance and click on the Properties button. The Residential Subscriber Instance (Edit) form opens with the General tab displayed.

v Click on the Statistics tab button.

vi Choose Host Tracking Stats (Residential Subscriber) from the object drop-down list.

vii Click on the Collect button to collect the statistics.

viii Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

ix View the statistics information.

x Click on the Close button to close the statistics record form.

xi Repeat steps viii to x for each statistics record that you want to view.

xii Click on the Host Tracking Info tab button.

xiii Configure the filter criteria and click on the Search button. Host tracking data for the residential subscriber instance appears.

xiv Click on the Clear button. A dialog box appears.

xv If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? checkbox.

xvi Click the Yes button. An information box appears.

xvii Click the OK button. The data is deleted from the NE.

xviii Click the Clear Status tab button to view a list of host tracking information clear results.

xix Choose a request and click on the Properties button to view information about the request, if required.

xx Close the Residential Subscriber Instance (Edit) form.

xxi Close the Manage Residential Subscribers form.

2 To collect, view, and clear on-demand host tracking statistics and information for a VPLS L2 access interface.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPLS Service (VPLS) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPLS services appears.

iv Select a service and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

v Click on the Components tab button.

vi Right click on an access interface and click on the Properties menu item. The VPLS L2 Access Interface (Edit) form opens.

vii Click on the Statistics tab button.

viii Choose Host Tracking Stats on SAP (Residential Subscriber) from the object drop-down list.

ix Click on the Collect button to collect the statistics.

x Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

xi View the statistics information.

xii Click on the Close button to close the statistics record form.

xiii Repeat steps x to xii for each statistics record that you want to view.

xiv Click on the Subscriber Management tab button.

xv Click on the Host Tracking Info tab button.

xvi Configure the filter criteria and click on the Search button. Host tracking data for the L2 access interface appears.

xvii Click on the Clear button. A dialog box appears.

xviii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? checkbox.

xix Click the Yes button. An information box appears.

xx Click the OK button. The data is deleted from the NE.

xxi Repeat steps xvii to xx for each host that you need to clear.

xxii Click the Clear Status tab button to view a list of host tracking information clear results.

xxiii Choose a request and click on the Properties button to view information about the request, if required.

xxiv Close the VPLS L2 Access Interface (Edit) form.

xxv Close the VPLS Service (Edit) form.

xxvi Close the Manage Services form.

3 To collect, view, and clear on-demand host tracking statistics and information for an IES service access point.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose IES Service (IES) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of IES services appears.

iv Select a service and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

v Click on the Components tab button.

vi Right click on a service access point and click on the Properties menu item. The IES Service Access Point (Edit) form opens.

vii Click on the Statistics tab button.

viii Choose Host Tracking Stats on SAP (Residential Subscriber) from the object drop-down list.

ix Click on the Collect button to collect the host tracking statistics.

x Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

xi View the statistics information.

xii Click on the Close button to close the statistics record form.

xiii Repeat steps x to xii for each statistics record that you want to view.

xiv Click on the Subscriber Management tab button.

xv Click on the Host Tracking Info tab button.

xvi Configure the filter criteria and click on the Search button. Host tracking data for the IES service access point appears.

xvii Click on the Clear button. A dialog box appears.

xviii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? checkbox.

xix Click the Yes button. An information box appears.

xx Click the OK button. The data is deleted from the NE.

xxi Repeat steps xvii to xx for each host that you need to clear.

xxii Click the Clear Status tab button to view a list of host tracking information clear results.

xxiii Choose a request and click on the Properties button to view information about the request, if required.

xxiv Close the IES Service Access Point (Edit) form.

xxv Close the IES Service (Edit) form.

xxvi Close the Manage Services form.

4 To collect, view, and clear on-demand host tracking statistics and information for a VPRN service access point.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPRN Service (VPRN) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPRN services appears.

iv Select a service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

v Click on the Components tab button.

vi Right click on a service access point and click on the Properties menu item. The VPRN Service Access Point (Edit) form opens.

vii Click on the Statistics tab button.

viii Choose Host Tracking Stats on SAP (Residential Subscriber) from the object drop-down list.

ix Click on the Collect button to collect the host tracking statistics.

x Select a statistics record and click on the Properties button to view the record. The statistics record form opens.

xi View the statistics information.

xii Click on the Close button to close the statistics record form.

xiii Repeat steps vii to xii for each statistics record that you want to view.

xiv Click on the Subscriber Management tab button.

xv Click on the Host Tracking Info tab button.

xvi Configure the filter criteria and click on the Search button. Host tracking data for the VPRN service access point appears.

xvii Click on the Clear button. A dialog box appears.

xviii If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? checkbox.

xix Click the Yes button. An information box appears.

xx Click the OK button. The data is deleted from the NE.

xxi Repeat steps xvii to xx for each host that you need to clear.

xxii Click the Clear Status tab button to view a list of host tracking information clear results.

xxiii Choose a request and click on the Properties button to view information about the request, if required.

xxiv Close the VPRN Service Access Point (Edit) form.

xxv Close the VPRN Service (Edit) form.

xxvi Close the Manage Services form.

5 To clear on-demand host tracking statistics and information for a VPLS service site.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPLS Service (VPLS) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPLS services appears.

iv Select a service and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

v Click on the Components tab button.

vi Right click on a site and click on the Properties menu item. The VPLS Site (Edit) form opens with the General tab displayed.

vii Click on the IGMP Host Tracking tab button.

viii Click on the Clear button. A dialog box appears.

ix If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? checkbox.

x Click the Yes button. An information box appears.

xi Click the OK button. The service site data is deleted from the NE.

xii Click the Clear Status tab button to view a list of site host tracking information clear results.

xiii Choose a request and click on the Properties button to view information about the request, if required.

xiv Close the VPLS Site (Edit) form.

xv Close the VPLS Service (Edit) form.

xvi Close the Manage Services form.

6 To clear on-demand host tracking statistics and information for an IES service site.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose IES Service (IES) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of IES services appears.

iv Select a service and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

v Click on the Components tab button.

vi Right click on a site and click on the Properties menu item. The IES Site (Edit) form opens with the General tab displayed.

vii Click on the IGMP Host Tracking tab button.

viii Click on the Clear button. A dialog box appears.

ix If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? checkbox.

x Click the Yes button. An information box appears.

xi Click the OK button. The service site data is deleted from the NE.

xii Click the Clear Status tab button to view a list of site host tracking information clear results.

xiii Choose a request and click on the Properties button to view information about the request, if required.

xiv Close the IES Site (Edit) form.

xv Close the IES Service (Edit) form.

xvi Close the Manage Services form.

7 To clear on-demand host tracking statistics and information for a VPRN service site.

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose VPRN Service (VPRN) from the object drop-down list.

iii Configure the filter criteria and click on the Search button. A list of VPRN services appears.

iv Select a service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

v Click on the Components tab button.

vi Right click on a site and click on the Properties menu item. The VPRN Site (Edit) form opens with the General tab displayed.

vii Click on the IGMP Host Tracking tab button.

viii Click on the Clear button. A dialog box appears.

ix If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? checkbox.

x Click the Yes button. An information box appears.

xi Click the OK button. The service site data is deleted from the NE.

xii Click the Clear Status tab button to view a list of site host tracking information clear results.

xiii Choose a request and click on the Properties button to view information about the request, if required.

xiv Close the VPRN Site (Edit) form.

xv Close the VPRN Service (Edit) form.

xvi Close the Manage Services form.

8 To clear on-demand host tracking statistics and information for a residential subscriber host.

i Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

ii Choose Residential Subscriber Host (Residential Subscriber) from the object drop-down list.

iii Select the Search Current Subscriber Host Information option.

iv Click on the Select button beside Site ID to specify an NE. The Select an ESM Capable Network Element form opens.

v Select an NE in the list and click on the OK button. The Select an ESM Capable Network Element form closes and the NE system IP address is displayed on the Manage Residential Subscribers form.

vi Configure the Service ID parameter.

vii Click on the Select button beside Port to specify a port. The Select Port form opens.

viii Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed on the Manage Residential Subscribers form.

ix Click the Search button. A list of hosts appears.

x Choose a host from the list and click the Clear Host Tracking button. A dialog box appears.

xi If you only need to clear the host tracking statistics, enable the Clear only Host Tracking Statistics? checkbox.

xii Click the Yes button. An information box appears.

xiii Click the OK button. The residential subscriber host data is deleted from the NE.

xiv You can view a list of the residential host clear results by clicking on the Clear Status button on the residential subscriber instance form.

xv Repeat steps x to xiv for each host that you need to clear.

xvi Close the Manage Residential Subscribers form.

Procedure 64-39 To list and manage subscriber management SAPs

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Select one of the available SAP types from the object drop-down list:

- IES Service Access Point (ies)
- L2 Access Interface (mvpls)
- L2 Access Interface (vpls)
- VPRN Service Access Point (vprn)

3 Click on the Select button to choose a site.

4 Click on the Search button. A list of SAPs for the selected service type appears.

5 To view or manage the information for a particular SAP, select the entry from the list and click on the Properties button. The SAP Properties form opens on the General tab. You can view SAP information or make changes to a variety of parameters on the various tabs of the form.

6 Click on the OK button to implement any changes you have made.

7 Close the Properties form.

8 Close the Manage Residential Subscribers form.

Procedure 64-40 To configure DHCP event monitoring for a SAP

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Select one of the available SAP types from the object drop-down list:

- IES Service Access Point (ies)
- L2 Access Interface (mvpls)
- L2 Access Interface (vpls)
- VPRN Service Access Point (vprn)

3 Click on the Select button to choose a site.

4 Click on the Search button. A list of SAPs appears.

5 To configure DHCP monitoring for a particular SAP, select the entry from the list and click on the Create Monitored SAP button. The Monitored Access Interface (Create) form opens with the General tab displayed.

Note — A maximum of five hosts or five SAPs can be monitored simultaneously. If more than the maximum number of hosts is selected and configured for monitoring an error message will be displayed.

6 Configure the parameters:

- Monitoring Period
- Units

7 Click on the OK button to close the Monitored Access Interface (Create) form.

Note — You must complete Procedure 64-41 to enable and schedule SAP monitoring.

8 Close the Manage Residential Subscribers form.

Procedure 64-41 To monitor DHCP events for a SAP

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Monitored Access Interface from the object drop-down list.

3 Configure the filter criteria at the top-right panel of the form, if required.

4 Click on the Search button. A list of Monitored SAPs appears.

5 To initiate or view DHCP monitoring for a particular SAP, select the entry from the list and click on the Properties button. The Monitored Access Interface (Edit) form opens on the General tab.

6 You can perform one or more of the following on this form:

   a To start monitoring the chosen SAP, click on the Start Monitor button.

   b To stop monitoring the chosen SAP, click on the Stop Monitor button.

   c To remove monitoring of the chosen SAP, click on the Delete button.

   d To change the Monitoring Period, click on the Stop Monitor button, enter the desired value into the field, and select an appropriate Unit from the adjacent drop-down menu.

7 To view DHCP events for the chosen SAP, click on the Events tab. The DHCP Events list is displayed.

8 Select an event from the list and click on the Properties button to view detailed information about the event.

9 Click on the OK button to close the Monitored Access Interface form.

10 Close the Manage Residential Subscribers form.

Procedure 64-42 To configure DHCP event monitoring for a subscriber host

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Residential Subscriber Hosts from the object drop-down list.

3 Click on the Select button beside Site ID to specify an NE. The Select an ESM Capable Network Element form opens.

4 Select an NE in the list and click on the OK button. The Select an ESM Capable Network Element form closes and the NE system IP address is displayed on the Manage Residential Subscribers form.

5 Configure the Service ID parameter.

6 Click on the Select button beside Port to specify a port. The Select Port form opens.

7 Select a port in the list and click on the OK button. The Select Port form closes and the port identifier is displayed on the Manage Residential Subscribers form.

8 Configure the Inner Encapsulation Value and Outer Encapsulation Value parameters.

Note — The Outer Encapsulation Value parameter is configurable only when the port encapsulation type is Dot1 Q or Q in Q. The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is Q in Q.

9 Click on the Search button. A list of subscriber hosts appears.

10 To configure DHCP monitoring for a particular subscriber host, select the entry from the list and click on the Create Monitored Host button. The Monitored Subscriber Host form opens.

Note — A maximum of five hosts or five SAPs can be monitored simultaneously. If more than the maximum number of hosts is selected and configured for monitoring an error message will be displayed.

11 Configure the parameters:

- Monitoring Period
- Units
- Polling Interval

12 Click on the OK button to close the Monitored Subscriber Host form.

Note — You must complete Procedure 64-43 to enable and schedule subscriber host monitoring.

13 Close the Manage Residential Subscribers form.

Procedure 64-43 To monitor DHCP events for a subscriber host

1 Choose Manage→Residential Subscribers from the 5620 SAM main menu. The Manage Residential Subscribers form opens.

2 Choose Monitored Subscriber Host from the object drop-down list.

3 Configure the filter criteria at the top right panel of the form, if required.

4 Click on the Search button. A list of monitored subscriber hosts appears.

5 To initiate or view DHCP monitoring for a particular subscriber host, select the entry from the list and click on the Properties button. The Monitored Subscriber Host (Edit) form opens with the General tab displayed.

6 You can perform one or more of the following on this form:

   a To start monitoring the chosen subscriber host, click on the Start Monitor button.

   b To stop monitoring the chosen subscriber host, click on the Stop Monitor button.

   c To remove monitoring of the chosen subscriber host, click on the Delete button.

   d To change the Monitoring Period, click on the Stop Monitor button, enter the desired value into the field, and select an appropriate Unit from the adjacent drop-down menu.

   e To change the Polling Interval, click on the Stop Monitor button and then select the desired value from the drop-down menu.

7 To view DHCP events for the chosen subscriber host, click on the Events tab. The DHCP Events list is displayed.

8 Select an event from the list and click on the Properties button to view detailed information about the event.

9 Click on the OK button to close the Monitored Subscriber Interface form.

10 Close the Manage Residential Subscribers form.

65 — VLAN service management

65.1 VLAN service management overview

The 5620 SAM supports the creation of VLAN services using 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, or OmniSwitch devices that are configured as PE devices. Table 65-1 lists the types of VLAN services that are supported by each device:

Table 65-1 Device VLAN support

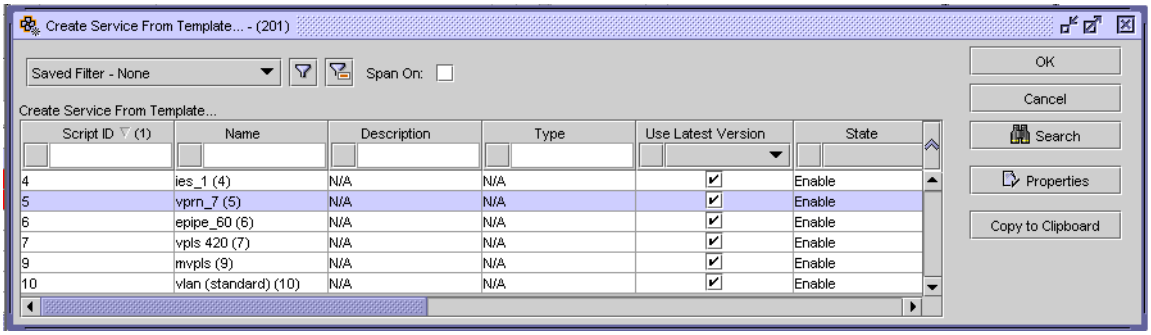
Device	Supported VLAN types
7250 SAS 7250 SAS-ES 7250 SAS-ESA Telco	• standard VLAN • management VLAN • L2 VPN (TLS/VLAN-Stacking) VLAN • Broadcast TV (MVR/IPMV) VLAN • Internet Access (Super VLAN)
OmniSwitch	• standard VLAN • L2 VPN (TLS/VLAN-Stacking) VLAN • Broadcast TV (MVR/IPMV) VLAN

Several 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch VLAN services can be interconnected through a backbone VPLS.

The 5620 SAM supports end-to-end VLAN configuration using the following methods:

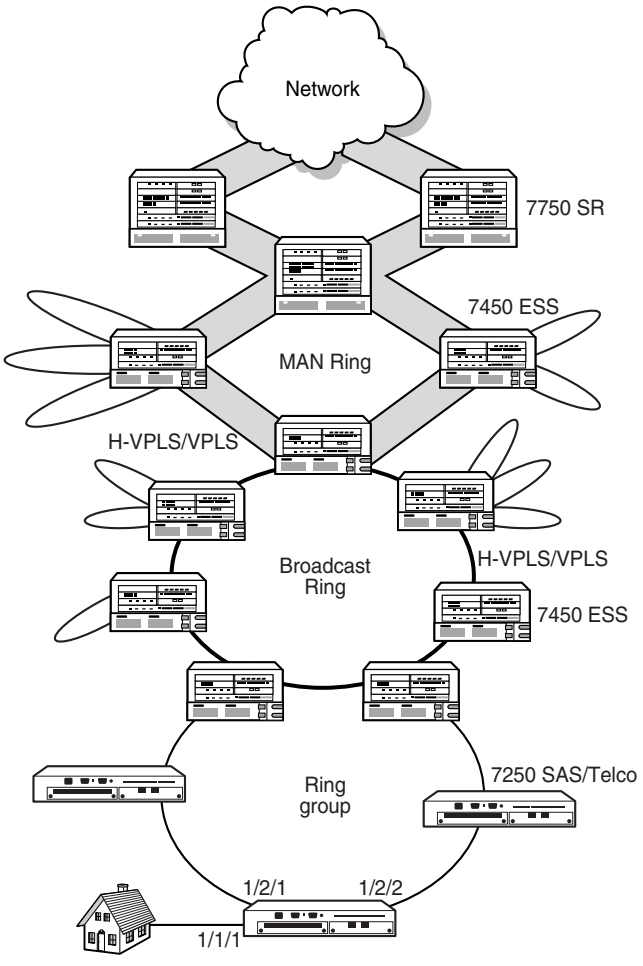
- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Pre-configured template. Figure 65-1 shows the Create Service From Template form. A user that is assigned the template management role can create a service template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

Figure 65-1 Create Service From Template form



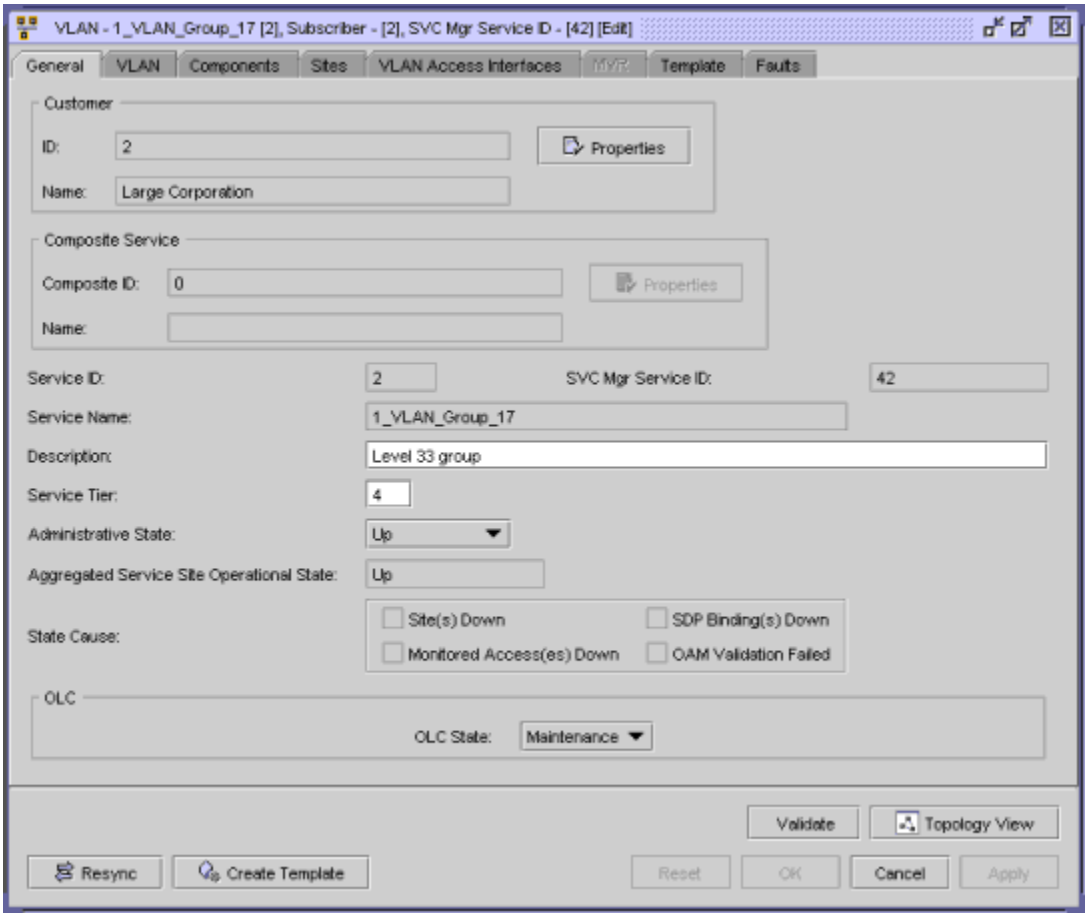
VLAN ring groups are used to send traffic across an Ethernet ring using copper or fiber optic connections from the source traffic device, for example, from a 7450 ESS, to all devices in the ring. STP configuration on OmniSwitch, 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco devices ensures that there is a constant stream of traffic in either direction by rerouting traffic around breaks in the physical links between the devices. Figure 65-2 shows an example of a ring group that is part of a larger metropolitan area network. The scenario shown in Figure 65-2 also supports OmniSwitch NEs instead of the 7250 SAS/Telco NEs shown.

Figure 65-2 Ring in a metropolitan and broadcast network



The General tab of the 5620 SAM service management form displays useful information about the operational state of the service and its sites through the Aggregated Operational State and State Cause parameters, as shown in Figure 65-3.

Figure 65-3 VLAN service management form - General



You can run the OAM Validation test suite (7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco only) for the service by clicking on the Validate button. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. In addition, the Validation Result tab on the Tests tab displays more detailed information about the OAM test result. See chapter 75 for more information about how to configure OAM validation test suites.

The Aggregated Service Site Operational State parameter has four possible values. The value is derived from the operational states of the sites that are part of the service, as follows:

- Up—all sites are operationally up
- Partially Down—at least one site is operationally down
- Down—all sites are operationally down
- Unknown—the service has no provisioned sites

When the Aggregated Service Site Operational State parameter is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator. You can view alarms on the Faults page.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology map views. See chapter 72 for more information about the hierarchical organization of composite services.

Telco policies

Policies can be assigned to ports on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices. Policies are defined at a global level and then applied to components of the service, such as a port.

Note — The 5620 SAM supports the distribution of policies on the 7450 ESS, 7750 SR, 7710 SR, Release 6.3 or earlier Telco devices, and on the 7250 SAS and 7250 SAS-ES, prior to Release 2.0.

The policy on the component is then a local version of the global policy. The following policies are common to VLAN services:

- QoS policies define ingress classification, policing, shaping, and marking on the device. QoS policies are configured using the Telco Qos Node Level Policy Manager.
- Filter policies control network traffic into or out of an interface or device based on IP or MAC matching criteria. Filter policies are configured using the Telco ACL Standard IP Filter Manager, the Telco ACL Extended IP Filter Manager, and the Telco ACL MAC Filter Manager.
- Multicast policies define the available broadcast addresses (BTV channels) for a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco ring. ACL IGMP filters specify the filters that are applied for end users to the channels to ensure that only the subscribed channels are delivered. Multicast polices and filters are configured using the Multicast Package Policy Manager and the Telco ACL IGMP Filter Manager, and are applied during service creation.

See chapter 43 for more information about policies.

OmniSwitch policies

Policies can be assigned to ports on an OmniSwitch. Policies are defined at a global level and then applied to components of the service, such as a port.

The policy on the component is then a local version of the global policy. The following policies are common to VLAN services:

- QoS policies define ingress classification, policing, shaping, and marking on the device.
- UNI policies define how control frames that are received on a port are processed. UNI policies are applied to a port that is used as a SAP in a stacked VLAN.
- SAP policies define traffic engineering parameters for bandwidth sharing, rate limiting, CVLAN translation (or double-tagging), and priority bit mapping. SAP policies are applied to the service access multi-point.
- Filter policies control network traffic into or out of an interface or device based on IP or MAC matching criteria.

See chapter 43 for more information about policies.

Default VLANs

By default, 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and OmniSwitch devices are configured with a default VLAN that uses VLAN ID 1. In addition, access ports on the 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA are untagged and configured for access mode as members of VLAN ID 1.

Note — The 5620 SAM does not manage VLAN 1 on an OmniSwitch.

Before you create a VLAN on a 7250 SAS, 7250 SAS-ES, or 7250 SAS-ESA, device using untagged ports, ensure the following.

- Renumber the default VLAN (ID 1) with the new VLAN ID that you want to use.
- Remove all untagged access ports that are not members of the new VLAN.
- Do not share untagged ports between VLANs, as there can only be one default VLAN for each untagged port.

See section 15.17 for more information about tagged and untagged ports.

7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch network management

The 5620 SAM manages the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch devices using SNMP and CLI messages. The devices support termination of all VLAN types on Ethernet ports. The 7250 SAS, 7250 SAS-ES, and 7250 SAS-ESA supports the termination of standard VLANs and L2 VPN VLANs on CES ports with dot1q encapsulation.

When using 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices to ensure the latest management view of the network, a management VLAN must be created on devices that belong to a ring group. This is done by:

- ensuring ports are configured to allow management message traffic
- making the 7450 ESS part of a management VPLS, used to relay SNMP and CLI messages to the devices

Spanning tree protocols

The STP configuration on a 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device in a ring group or an OmniSwitch device in a VLAN group detects loops in the topology and ensures that there is a constant stream of traffic by rerouting traffic around breaks in the physical links between the devices. The 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch devices support STP, MSTP and RSTP.

Spanning tree on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices

Spanning tree protocols are a global configuration, and only one protocol can be enabled at a time. For example, if you enable RSTP while STP is already running, the 7250 SAS disables STP and runs RSTP. You can disable STP per port when MSTP or RSTP is enabled globally. Spanning tree protocols must be configured before the 5620 SAM manages the device.

Spanning tree on OmniSwitch devices

The OmniSwitch can operate in the following spanning tree modes:

- flat
- 1 x 1

The flat mode provides a CST instance that applies across all VLANs and supports STP (802.1D), RSTP (802.1w), and MSTP. MSTP allows the mapping of one or more VLANs to a single spanning tree instance.

The 1x1 mode is an Alcatel-Lucent proprietary implementation that automatically calculates a separate spanning tree instance for each VLAN configured on the switch. This mode only supports the use of the STP and RSTP.

By default, an OmniSwitch runs in the 1x1 mode and uses the 802.1D protocol.

The 5620 SAM supports the configuration of Spanning Tree protocols and modes.

See the OmniSwitch user documentation for more information about Spanning Tree modes.

STP

STP is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. Fault-tolerant internetworks must have a loop-free path between all the nodes in a network. The spanning tree algorithm calculates the best loop-free path through a switched Layer 2 network. Switches send and receive STP frames at regular intervals but do not forward these frames.

See the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch user documentation for more information about device-specific STP CLI commands and parameters.

RSTP

RSTP uses point-to-point wiring to provide rapid convergence of the spanning tree. With RSTP, the spanning tree may be reconfigured in less than 1 s, as compared to 50 s required with the default STP settings. This is critical in networks that carry voice, video, and other delay-sensitive traffic.

RSTP assigns port roles and determines the active topology to provide rapid convergence of the spanning tree. RSTP selects the switch with the highest switch priority.

See the 7250 SAS, Telco, and OmniSwitch user documentation for more information about device-specific RSTP CLI commands and parameters.

MSTP

MSTP allows you to group and associate VLANs to multiple spanning tree instances, or forwarding paths. MSTP allows up to 16 RSTP instances to be run and associates a VLAN with a specific MST instance. This reduces link convergence time and enables load balancing over a large number of VLANs.

Each MST instance can have its own independent topology. Multiple forwarding paths improve network fault tolerance because when one instance fails, data flow is unaffected over the remaining forwarding paths. You can manage large networks and use redundant paths more easily by allocating different VLAN and spanning tree instance assignments to different parts of the network.

See the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch user documentation for more information about device-specific RSTP CLI commands and parameters.

MSTP fast ring (7250 SAS and Telco only)

The MSTP fast ring mode shortens the MSTP convergence time in a ring topology when a disconnection occurs. To use MSTP fast ring, you must select one bridge to be the root bridge by setting its priority to the lowest value. All of the user ports must be configured as MSTP edge ports.

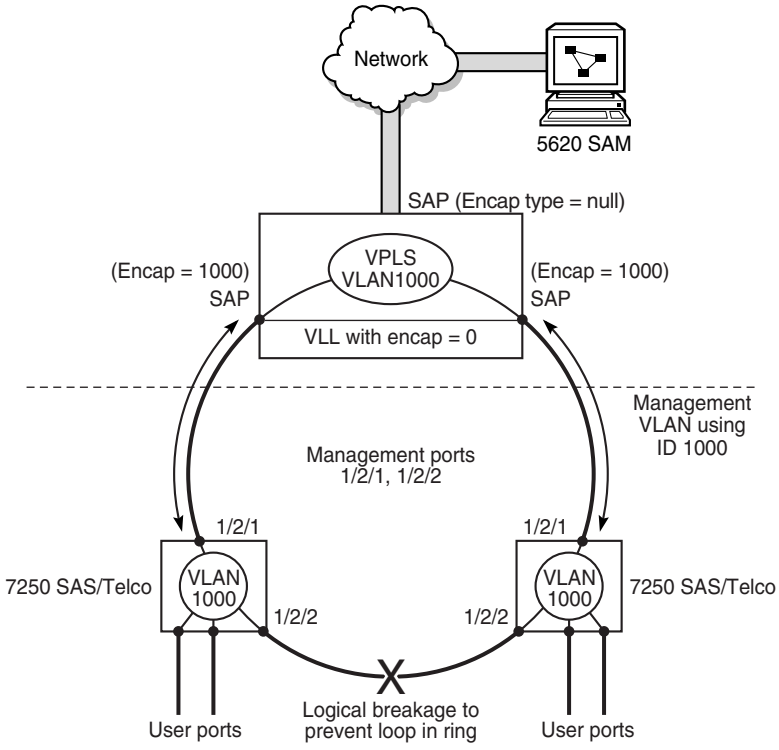
To optimize the performance of your network, increment the priority of the bridges as you draw away from the root bridge.

See the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco user documentation for information about configuring the MSTP fast ring.

65.2 Sample management VLAN configuration

Figure 65-4 shows a sample management VLAN service configuration. The configuration depends on the specific network requirements.

Figure 65-4 Sample management VLAN



The following high-level steps describe the configuration of the sample management VLAN.

1 Choose a management VLAN ID to be used in the ring, for example, ID 1000.

2 Create a VPLS on the 7450 ESS that has the SAPs in the VPLS set with encapsulation 1000. See chapter 68 for more information about creating a VPLS.

3 The port to which the 5620 SAM is connected to the network is added to the VPLS without encapsulation.

4 Create a management VLAN on each 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, or Telco device; for example, by using CLI:

- config vlan
- create mgt_1000
- config mgt_1000
- add ports 1/2/1, 1/2/2 tagged

5 Exclude all other VLANs from being management VLANs, for example, by using CLI:

- config vlan
- no management 1-999,1001-4094 (for a Telco) no management 1-999, 1001-4092 (for a 7250 SAS)

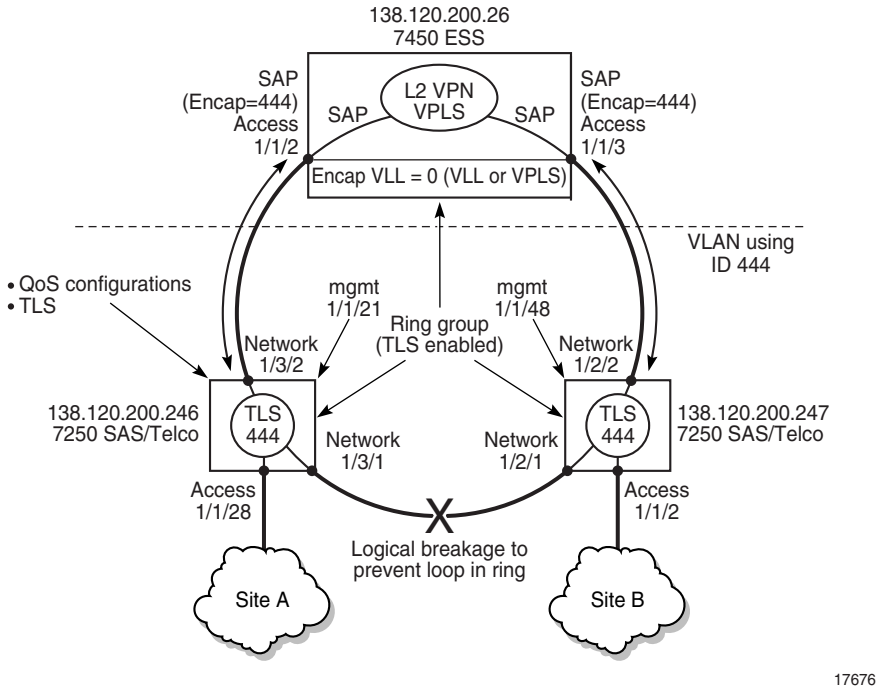
6 Ensure only the uplink ports from the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices have device management capabilities to ensure user ports cannot access CLI, SNMP, or FTP functionality, for example, by using CLI:

- config
- no port management 1/1/1-1/1/24

65.3 Sample VLAN configuration for L2 VPNs

Figure 65-5 shows a sample VLAN L2 VPN service configuration. Transparent LAN services such as a L2 VPN are used to transport large numbers of customer VLANs while keeping the traffic in each VLAN segregated. The configuration depends on the specific network requirements.

Figure 65-5 Sample VLAN configuration for L2 VPNs



Verify that the following preconfigurations are complete.

- Ensure that the appropriate preconfigurations have been performed on the 7250 SAS or Telco devices.
  - pre-discovery CLI modifications
  - discovery including mediation configuration with the CLI user names and passwords
  - configure protocol to manage topology loops, such as MSTP or RSTP
- Ensure that the TLS VPLS that feeds the ring VLAN service is configured on the 7450 ESSs. The encapsulation of the SAPs that belong to the VPLS on the 7450 ESSs must match the VLAN ID of the ring VLAN.

- Configure the 7250 SAS or Telco ports as access (ports that are part of the VLAN) and network (ports that are used for uplinks), as required, from the navigation tree.
- Configure the bridge instances for the 7250 SAS or Telco devices from the network view in the navigation tree.
- Devices that belong to the ring, and the 7450 ESS that the ring connects to, should be added to the ring group.
- Ensure that the appropriate preconfigurations have been performed on the 7450 ESS.
  - A VLL is created with 0 encapsulation between the SAPs (1/1/2 and 1/1/3) on the 7450 ESS
  - The SAPs on the 7450 ESS that are part of the VPLS use the same encapsulation as the VLAN ID for the ring group
  - A L2 VPN VPLS is created on the 7450 ESS.

Table 65-2 lists the high-level tasks that are required to configure this sample VLAN L2 VPN service.

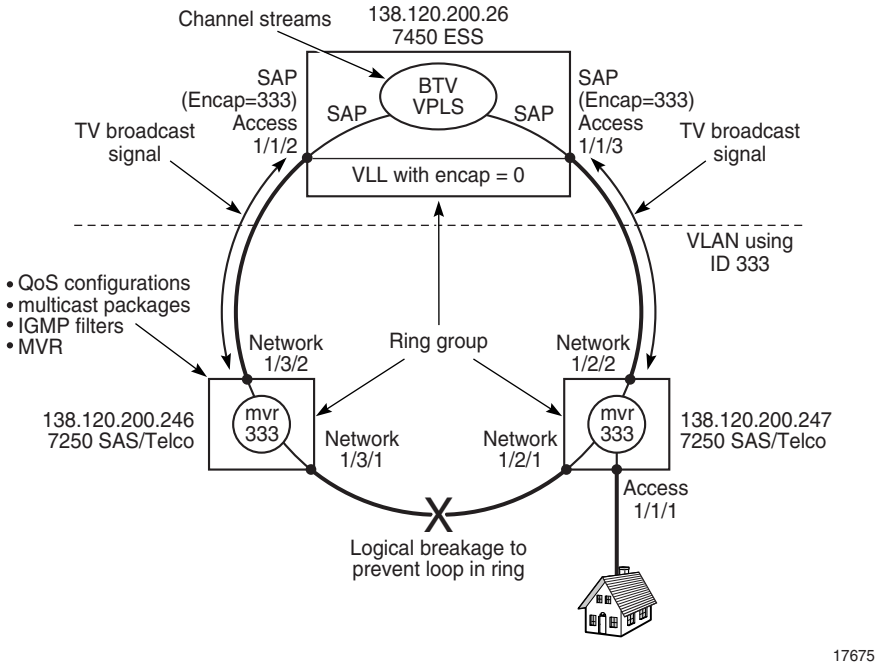
Table 65-2 Sample VLAN L2 VPN service configuration

Task	Description
1. Manage and configure devices	Ensure that the required configurations are completed to equipment, including configuring access and network ports, enabling CLI configuration on managed 7250 SAS and Telco devices, and the creating of ring groups that are enabled to receive TLS (L2 VPN) streams: • The ring group contains all three devices. • TLS is enabled for the ring group. • Ports 1/3/1 and 1/3/2 on the device connected to Site A and 1/2/1 and 1/2/2 connected to Site B are configured as network to act as uplinks. • Ports 1/1/2 and 1/1/3 are configured as access on the 7450 ESS, and the encapsulation matches the VLAN ID (444). • Ports 1/1/2 and 1/1/28 on the 7250 SAS and Telco devices are configured as access ports.
2. Configure policies as required	Policies should be configured before you create a service. The following key policies can be applied to resources that are part of a VLAN. • QoS policies for the 7250 SAS and Telco devices and ports • scheduling policies • filter policies, including IGMP filter policies to create and deploy access control lists on the 7250 SAS and Telco devices in the ring
3. Distribute policies to devices	Distribute configured policies to the devices. The policies are used during the creation of VLAN services.
4. Create VLAN services	Create VLAN services using a series of configuration forms. Ensure that the VLAN created for the ring group uses ID 444.
5. Add access interfaces	Associate access interfaces (similar to SAPs) with VLAN services, that are the physical ports to which end users connect. Use the L2 Interfaces tab button on the VLAN properties form to associate VLAN services with the ports used by end users.

65.4 Sample VLAN configuration for BTV

Figure 65-6 shows a sample VLAN broadcast service configuration. BTV VLANs are shared VLANs, where the multicast broadcast channels or pay per view channels are available across the ring, and based on subscriptions and privileges determined using IGMP snooping, the user gains or is denied access. The configuration depends on the specific network requirements.

Figure 65-6 Sample VLAN configuration for BTV



Verify that the following preconfigurations are complete.

- Ensure that the appropriate preconfigurations have been performed on the 7250 SAS and Telco devices:
  - pre-discovery CLI modifications
  - SNMP trap forwarding to the 5620 SAM
  - discovery, including mediation configuration with the CLI user names and passwords
  - configure protocols to manage topology loops, such as MSTP or RSTP
- Ensure that the BTV VPLS that feeds the ring VLAN service is configured on the 7450 ESSs. The encapsulation of the SAPs that belong to the VPLS on the 7450 ESSs should match the VLAN ID of the ring VLAN.
- Configure 7250 SAS and Telco ports as access (ports that are part of the VLAN) and network (ports that are used for uplinks), as required, from the navigation tree.
- Configure the bridge instances for the 7250 SAS and Telco devices from the network view in the navigation tree.

- Enable IGMP snooping on the bridge instance for the 7250 SAS and Telco devices included in the broadcast TV VLAN.
- 7250 SAS and Telco devices that belong to the ring, and the 7450 ESS that the ring connects to, should be added to the ring group.
- Ensure that the appropriate preconfigurations have been performed on the 7450 ESS.
  - A VLL is created with 0 encapsulation between the SAPs (1/1/2 and 1/1/3) on the 7450 ESS
  - The SAPs on the 7450 ESS that are part of the VPLS use the same encapsulation as the VLAN ID for the ring group
  - A BTV VPLS is created on the 7450 ESS.
- Create and manage the necessary broadcast TV policies, including multicast package and IGMP filtering.

Table 65-3 lists the high-level tasks that are required to configure this sample VLAN broadcast TV service.

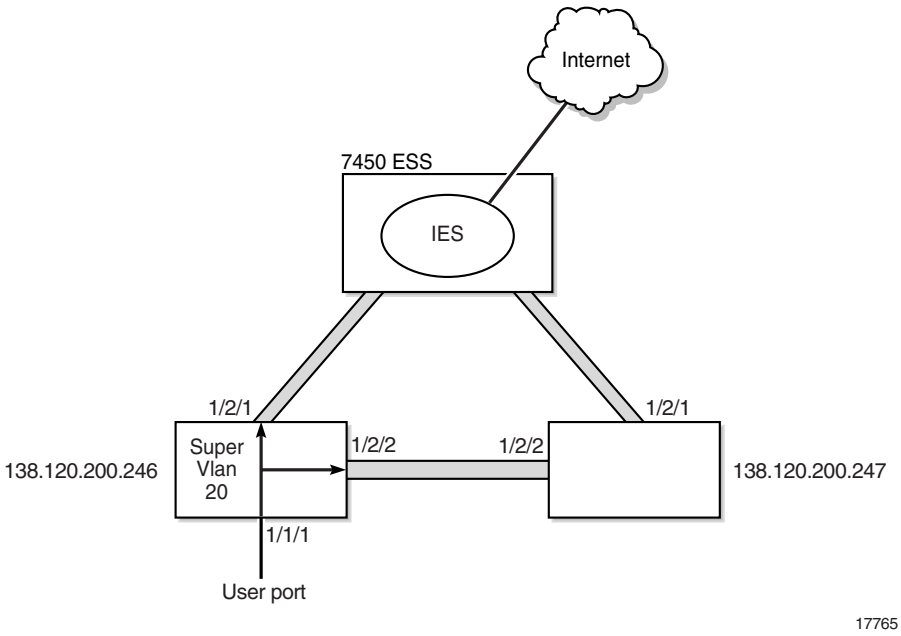
Table 65-3 Sample VLAN broadcast TV service configuration

Task	Description
1. Manage and configure devices	Ensure that the required configurations are completed to equipment, including configuring access and network ports, enabling CLI configuration on managed 7250 SAS and Telco devices, and the creation of ring groups: • The ring group contains all three devices. • Ports 1/3/1 and 1/3/2 on the device with the IP address 138.120.200.246 and ports 1/2/1 and 1/2/2 on the device with the IP address 138.120.200.247 are configured as network to act as uplinks. • Ports 1/1/2 and 1/1/3 are configured as access on the 7450 ESS with an encapsulation matching the VLAN ID (333). • Port 1/1/1 on device 138.120.200.247 is configured as access.
2. Configure policies as required	Policies should be configured before you create a service. The following key policies can be applied to resources that are part of a VLAN BTV service. • QoS policies for the 7250 SAS and Telco devices and ports • scheduling policies • filter policies, including IGMP filter policies to create and deploy access control lists on the 7250 SAS and Telco devices in the ring • multicast package policies to determine the content of the broadcast streams that are sent to the 7250 SAS and Telco devices in the ring
3. Distribute policies to devices	Distribute configured policies to the devices. Policies are used during the creation of VLAN services.
4. Create VLAN services	Create VLAN services using a series of configuration forms: Ensure that the VLAN created for the ring group uses ID 333.
5. Add access interfaces	Associate access interfaces (similar to SAPs) with VLAN services, that are the physical ports to which end users connect. You use the L2 Interfaces tab button on the VLAN properties form to associate VLAN services with the ports used by end users.

65.5 Sample configuration for super VLAN

Figure 65-7 shows a sample super VLAN configuration. Super VLANs are used to restrict traffic that arrives on the user port to the uplink port. This disallows traffic between user ports. This application is often used for public Internet access services. The configuration depends on the specific network requirements.

Figure 65-7 Sample configuration for super VLAN



Verify that the following preconfigurations are complete.

- Ensure that the appropriate preconfigurations have been performed on the 7250 SAS and Telco devices:
  - pre-discovery CLI modifications
  - SNMP trap forwarding to the 5620 SAM
  - discovery, including mediation configuration with the CLI user names and passwords
  - configure protocol to manage topology loops, such as MSTP or RSTP
- Ensure that the 7450 ESS is configured to support super VLAN Internet access.
- Create an IES on the 7450 ESS.
- Configure 7250 SAS and Telco ports as access (ports that are part of the VLAN) and network (ports that are used for uplinks), as required, from the navigation tree.
- 7250 SAS and Telco devices that belong to the ring, and the 7450 ESS that the ring connects to, should be added to the ring group.

Table 65-4 lists the high-level tasks that are required to configure this sample super VLAN service.

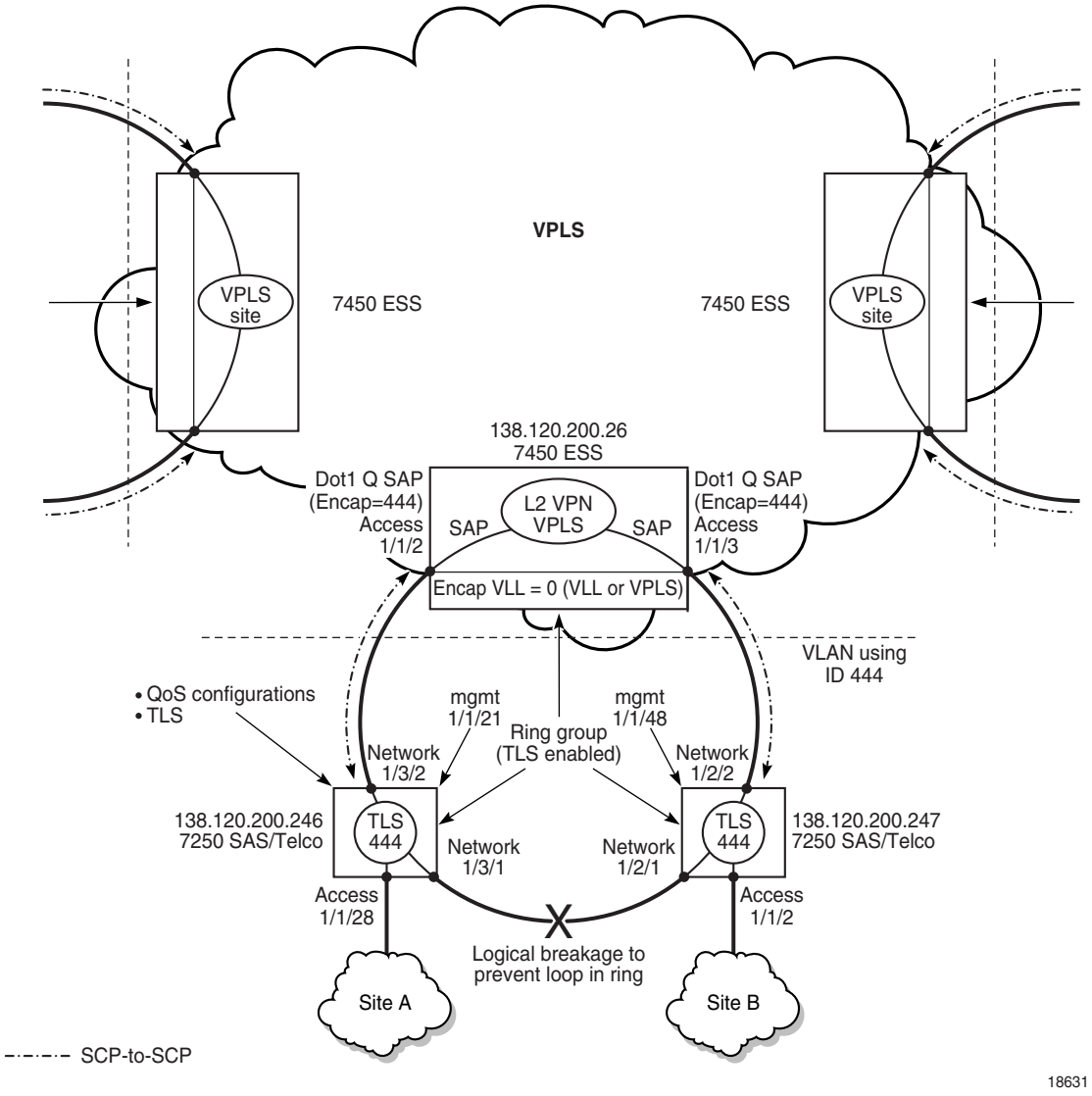
Table 65-4 Sample configuration for super VLAN

Task	Description
1. Manage and configure devices	Ensure that the required configurations are completed to equipment, including configuring access and network ports, enabling CLI configuration on managed 7250 SAS and Telco devices, and the creation of ring groups: • The ring group contains all three devices. • Ports 1/2/1 and 1/2/2 on the device with the IP address 138.120.200.246 and ports 1/2/1 and 1/2/2 on the device with the IP address 138.120.200.247 are configured as network to act as uplinks. • Port 1/1/1 on device 138.120.200.246 is configured as access.
2. Configure policies as required	Policies should be configured before you create a service. The following key policies can be applied to resources that are part of a super VLAN service. • QoS policies for the 7250 SAS and Telco devices and ports • scheduling policies
3. Distribute policies to devices	Distribute configured policies to the devices. Policies are used during the creation of VLAN services.
4. Create VLAN services	Create VLAN services using a series of configuration forms: • The super VLAN created for the ring group uses ID 20.
5. Add access interfaces	Associate access interfaces (similar to SAPs) with VLAN services, that are the physical ports to which end users connect. Use the L2 Interfaces tab button on the VLAN properties form to associate VLAN services with the ports used by end users.

65.6 Sample VLAN interconnection configuration

Figure 65-8 shows a sample configuration of an interconnection of VLANs across a VPLS backbone.

Figure 65-8 Sample VLAN interconnection



Verify that the following preconfigurations are complete:

- Ensure that the appropriate preconfigurations have been performed on the 7250 SAS and Telco devices.
  - pre-discovery CLI modifications
  - SNMP trap forwarding to the 5620 SAM
  - discovery including mediation configuration with the CLI user names and passwords
  - ports are configured as access (ports that are part of the VLAN) and network (ports that are used for uplinks)
  - configure protocol to manage topology loops, such as MSTP or RSTP, using CLI

- Configure 7250 SAS and Telco ports as access and network, as required, from the navigation tree.
- 7250 SAS and Telco devices that belong to the ring, and the 7450 ESS that the ring connects to, should be added to the ring group.

Table 65-5 lists the high-level tasks that are required to configure this sample interconnection of VLAN services.

Table 65-5 Sample VLAN interconnection configuration

Task	Description
1. Manage and configure	Ensure that the required configurations are completed to equipment as described in Table 65-2, including the following. • configuring access and network ports • enabling CLI configuration on managed 7250 SAS and Telco devices • creating ring groups that are enabled to receive TLS (L2 VPN) streams • configuring and distributing policies
2. Create VLAN services	Create VLAN services using a series of configuration forms. Ensure that the VLAN created for the ring group uses ID 444.
3. Configure VPLS	Ensure that the encapsulation value of the ports that contain the SAPs on the 7450 ESS matches the VLAN ID of each VLAN service in the ring group. Ensure that the encapsulation value of the ports that contain the SAPs on the 7450 ESS at each VPLS site is Dot1 Q. See chapter 68 for more information about creating a VPLS.
4. Create composite service	Create a composite service to interconnect the VLAN services with the VPLS. • Create the composite service. • Define general properties for the composite service. • Specify the services that are participating in the composite service. You can specify multiple services in one operation. • Create SCP-to-SCP connectors to link the Dot1 Q-encapsulated VPLS SAP and the adjacent L2 switch uplinks of the VLAN ring group. See chapter 72 for more information about creating composite services.

65.7 Workflow to create a VLAN service (7250 SAS and Telco)

1 Ensure that the appropriate preconfigurations have been performed on the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices:

- pre-discovery CLI modifications
- discovery including mediation configuration with CLI user name and password
- creation of a management VLAN for all devices that belong to a ring group.
- configuration of protocol to manage topology loops, such as MSTP or RSTP.

2 Ensure the TLS or BTV VPLS that feeds the ring VLAN service is configured on the 7450 ESSs. The encapsulation of the SAPs that belong to the VPLS on the 7450 ESSs should match the VLAN ID of the ring VLAN.

For super VLAN services, ensure the IES that provides Internet access to the ring VLAN service is configured on the 7450 ESSs.

3 Configure 7250 SAS and Telco ports as access and network, as required, from the navigation tree.

4 Configure device- or port-wide QoS policies, as required.

5 Configure the bridge instances for the 7250 SAS and Telco devices from the network view in the navigation tree, as described in chapter 28.

6 Create and add devices connected to the 7450 ESS as part of a ring group, as described in chapter 17.

7 For BTV VLAN services:

   i Manage the multicast addresses of television channels using the Multicast Package Manager, as described in chapter 43.

   ii Configure and manage IGMP filters using the IGMP Policy Manager to specify the multicast channels that end users can access from the ring that is delivering the broadcast streams.

   iii Distribute the policies to the managed devices.

8 Provision the service.

   i Set up customers or associate existing customers with the new service.

   ii Create the VLAN and associate the customer with the VLAN.

   iii Add the physical access interface of the end user for the service from the L2 Interface tab.

   iv Associate IP access groups with the port used for the customer.

9 Turn up the service.

65.8 Workflow to create a standard VLAN service (OmniSwitch)

1 Ensure that the appropriate preconfigurations have been performed on the OmniSwitch:

- pre-discovery CLI modifications
- discovery including mediation configuration with CLI usernames and passwords
- addition of the OmniSwitches that participate in the VLAN to a VLAN group

2 Configure OmniSwitch network ports, as required, from the navigation tree. The Automatic VLAN Binding parameter associated with a network port or LAG must be enabled before the 5620 SAM can identify the network port or LAG as a network interface.

3 Configure QoS policies, as required.

4 Configure the bridge instances for the OmniSwitches from the network view in the navigation tree.

5 Provision the service.

i Set up customers or associate existing customers with the new service.

ii Create the VLAN and associate a customer with the VLAN. Set the application parameter to Standard VLAN.

iii Add sites that are participating in this VLAN. Configure STP and VLAN properties if required.

iv Create VLAN access interfaces to be used for this service. Specify the access port to be used by each interface and whether the access is tagged.

6 Turn up the service.

Network interface VLAN bindings are created between the newly created VLAN and all of the network ports on the node.

65.9 Workflow to create a stacked VLAN service (OmniSwitch)

1 Ensure that the appropriate preconfigurations have been performed on the OmniSwitches:

- pre-discovery CLI modifications
- discovery including mediation configuration with CLI user name and password
- addition of the OmniSwitches that participate in the VLAN to a VLAN group

2 Configure OmniSwitch network ports, as required, from the navigation tree.

3 Configure QoS policies, as required.

4 Configure the bridge instances for the OmniSwitches from the network view in the navigation tree.

5 Provision the service.

i Set up customers or associate existing customers with the new service.

ii Create the VLAN and associate a customer with the VLAN. Set the application parameter to L2-VPN (TLS/VLAN-Stacking).

iii Add devices connected as part of a VLAN group, to the VLAN.

iv Add sites that are participating in this VLAN. Configure STP and VLAN properties if required.

v Create Ethernet services. Enter the names of the services that you need to associate with the SVLAN created in the previous steps.

vi Create one or more service access multipoints. SAPs, CVLANs, and a SAP policy are associated with a service access multipoint. A service access multipoint is assigned a user-selected or auto-generated ID when the multipoint is created

vii Create SAPs. Specify the port to be used as a customer-facing port (UNI).

viii Create CVLANs to associate customer traffic with a VLAN-stacking SAP. CVLANs identify the type of customer traffic that is received on the SAP UNI ports.

6 Turn up the service.

65.10 Workflow to create an IP multicast VLAN service (OmniSwitch)

In an IP multicast VLAN, the stacked VLAN network port corresponds to the sender port, which also receives multicast data for a configured multicast group. The stacked VLAN port corresponds to the receiver port of the IP multicast VLAN.

1 Ensure that the appropriate preconfigurations have been performed on the OmniSwitches:

- pre-discovery CLI modifications
- discovery including mediation configuration with CLI usernames and passwords
- addition of the OmniSwitches that participate in the VLAN to a VLAN group

2 Configure OmniSwitch network ports, as required, from the navigation tree.

3 Configure QoS policies, as required.

4 Configure the bridge instances for the OmniSwitches from the network view in the navigation tree.

5 Provision the service.

i Set up customers or associate existing customers with the new service.

ii Create the VLAN and associate a customer with the VLAN. Set the application parameter to Broadcast TV (MVR/IPMV).

iii Add devices connected as part of a VLAN group, to the VLAN.

iv Create an L2 access interface. The interface acts as the receiver port on the IPMV. The port that is selected must already be used as a SAP in a SVLAN.

v Create Ethernet services. Enter the names of the services that you need to associate with the SVLAN created in the previous steps.

vi Create one or more service access multipoints. SAPs, CVLANs, and a SAP policy are associated with a service access multipoint. A service access multipoint is assigned a user-selected or auto-generated ID when the multipoint is created.

vii Create SAPs. Specify the port to be used as a customer-facing port (UNI). The UNI port must already be configured as a receiver port on the IP multicast VLAN.

viii Create CVLANs that will be used to associate customer traffic with a VLAN stacking SAP. CVLANs identify the type of customer traffic received on the SAP UNI ports. The service processes and tunnels the traffic through the SVLAN

ix Add multicast group addresses to the IP multicast VLAN site.

x Add CVLAN tags to the IP multicast VLAN site. CVLAN tags are used to bind IP multicast VLANs to a receiver port.

6 Turn up the service.

65.11 VLAN service management procedures

Use the following procedures to perform VLAN creation and management tasks.

Procedure 65-1 To create a BTV VLAN service

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the BTV VLAN. The Select Customer - VLAN form opens.

3 Select a customer for the BTV VLAN and click on the OK button. The Select Customer - VLAN form closes and the VLAN (Create) form reappears with the customer information displayed in the General tab.

4 Configure the parameters.

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Administrative State
- OLC State

The OLC State parameter is configurable after you click on the Apply button.

Disable the Auto-Assign ID parameter and set the VLAN ID using the Service ID parameter. If the Auto-Assign ID parameter is enabled, the 5620 SAM chooses the VLAN ID.

5 Click on the VLAN tab button.

6 Set the Application parameter to Broadcast TV (MVR/IPMV).

7 Click on the Select button in the Group panel to choose a group to associate with the BTV VLAN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 Click on the MVR tab button.

10 Configure the parameters.

- Mode
- Query Response Time (seconds)

11 Click on the Select button in the Multicast Package panel to choose a multicast package for the BTV VLAN. The Select Multicast Package - MvrConfiguration form opens.

12 Select a multicast package and click on the OK button. The Select Multicast Package - MvrConfiguration form closes and the VLAN (Create) form reappears with the multicast package information displayed.

13 Click on the Components tab button.

14 Right-click on VLAN and choose Create Site. The Select Network Elements - VLAN form opens.

15 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the site information displayed on the General tab.

16 Configure the parameters.

- Description
- Administrative State
- Monitor Access Interface Operational State

17 Click on the MVR tab button to configure the Mode parameter, if required.

18 Click on the Components tab button.

19 Right-click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

20 Configure the parameters.

- Description
- Administrative State

21 Click on the Port tab button.

22 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

23 Use the configurable filter and Search button to choose a port for user-side access to the BTV VLAN, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

24 Configure the remaining parameters, if required.

25 Click on the VLAN tab button.

26 Configure the VLAN Tagging parameter.

You can only configure this parameter after you create a SAP. After the SAP is created, the VLAN Tagging parameter cannot be modified. If you need to change the value of the parameter, you must first delete the SAP and then create a SAP that matches the new requirements.

27 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

28 Click on the OK button. The Site (Create) form reappears.

29 Repeat steps 19 to 28 for each access interface to be created on the site.

30 Click on the OK button. The Site (Create) form closes, and a dialog box appears.

31 Click on the OK button. The VLAN (Create) form reappears with the site information displayed in the service components tree.

32 Click on the OK button to close the VLAN (Create) form.

Procedure 65-2 To create an L2 VPN TLS VLAN service

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the L2 VPN. The Select Customer - VLAN form opens.

3 Select a customer for the L2 VPN and click on the OK button. The Select Customer - VLAN form closes and the VLAN (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters.

- Auto-Assign ID
- Service Name
- Description
- Service Tier
- Administrative State
- OLC State

  The OLC State parameter is configurable after you click on the Apply button.

Disable the Auto-Assign ID parameter and set the VLAN ID using the Service ID parameter. If the Auto-Assign ID parameter is enabled, the 5620 SAM chooses the VLAN ID.

5 Click on the VLAN tab button.

6 Set the Application parameter to L2-VPN (TLS/VLAN-Stacking).

7 Click on the Select button in the Group panel to choose a group to associate with the L2 VPN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 Click on the Components tab button.

10 Right-click on VLAN and choose Create Site. The Select Network Elements - VLAN form opens.

11 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the site information displayed in the General tab.

12 Configure the parameters.

- Description
- Administrative State
- Monitor Access Interface Operational State

13 Click on the Components tab button.

14 Right-click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

15 Configure the parameters.

- Description
- Administrative State

16 Click on the Port tab button.

17 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

18 Use the configurable filter and Search button to choose a port for user-side access to the L2 VPN service, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

19 Configure the remaining parameters, if required.

20 Click on the VLAN tab button.

21 Configure the VLAN Tagging parameter. This parameter must be set to Tagged on CES interfaces.

You can only configure this parameter when you create a SAP. After the SAP is created, the parameter cannot be modified. If you need to change the value of this parameter, you must first delete the SAP and then create a SAP that matches the new requirements.

22 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

23 Click on the OK button. The Site (Create) form reappears.

24 Repeat steps 14 to 23 for each access interface to be created on the site.

25 Click on the OK button. The Site (Create) form closes, and a dialog box appears.

26 Click on the OK button. The VLAN (Create) form reappears with the new site information displayed in the service components tree.

27 Click on the OK button to close the VLAN (Create) form.

Procedure 65-3 To create a super VLAN service

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the super VLAN. The Select Customer - VLAN form opens.

3 Select a customer for the super VLAN and click on the OK button. The Select Customer - VLAN form closes and the VLAN (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters.

- Auto-Assign ID
- Service Name
- Description
- Service Tier
- Administrative State
- OLC State

  The OLC State parameter is configurable after you click on the Apply button.

Disable the Auto-Assign ID and set the VLAN ID using the Service ID parameter. If the parameter is enabled, the 5620 SAM chooses the VLAN ID.

5 Click on the VLAN tab button.

6 Configure the Application parameter. Choose the Internet Access (Super-VLAN) option.

7 Click on the Select button in the Group panel to choose a group to associate with the super VLAN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 Click on the Components tab button.

10 Right-click on VLAN and choose Create Site. The Select Network Elements - VLAN form opens.

11 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form reappears with the site information displayed on the General tab.

12 Configure the parameters.

- Description
- Administrative State
- Monitor Access Interface Operational State

13 Click on the Components tab button.

14 Right-click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

15 Configure the parameters.

- Description
- Administrative State

16 Click on the Port tab button.

17 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

18 Use the configurable filter and Search button to choose a port for user-side access to the super VLAN, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

19 Configure the remaining parameters, if required.

20 Click on the VLAN tab button.

21 Configure the parameter.

- VLAN Tagging

You can only configure this parameter when you create a SAP. After the SAP is created the parameter cannot be modified. If you need to change the value of this parameter you must first delete the SAP and create a new one that matches the new requirements.

The VLAN Tagging parameter should always be set to Tagged on CES interfaces.

22 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

23 Click on the OK button. The Site (Create) form reappears.

24 Repeat steps 14 to 23 for each access interface to be created on the site.

25 Click on the OK button. The Site (Create) form closes, and a dialog box appears.

26 Click on the OK button. The VLAN (Create) form reappears with the new site information displayed in the service components tree.

27 Click on the OK button to close the VLAN (Create) form.

Procedure 65-4 To create a standard VLAN service

Perform the following procedure to create a standard VLAN service on OmniSwitch, 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco devices.

Note — Alcatel-Lucent recommends that you specify the OmniSwitch ports that will be network interfaces before you configure a standard VLAN service.

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VLAN. The Select Customer - VLAN form opens.

3 Select a customer for the VLAN and click on the OK button. The Select Customer - VLAN form closes and the VLAN (Create) form reappears with the customer information displayed in the General tab.

4 Configure the parameters.

- Auto-Assign ID
- Service Name
- Description
- Service Tier
- Administrative State
- OLC State

  The OLC State parameter is configurable after you click on the Apply button.

Disable the Auto-Assign ID parameter and set the VLAN ID using the Service ID parameter. If the Auto-Assign ID parameter is enabled, the 5620 SAM chooses the VLAN ID.

5 Click on the VLAN tab button.

6 Set the Application parameter to Standard VLAN.

7 Click on the Select button in the Group panel to choose a group to associate with the VLAN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 Click on the Components tab button.

10 Right-click on VLAN and choose Create Site. The Select Network Elements - VLAN form opens.

11 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form appears with the site information displayed on the General tab.

12 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

13 Perform one of the following actions:

a If you are configuring a standard VLAN on an OmniSwitch, go to step 14.

b If you are configuring a standard VLAN on a 7250 SAS or Telco device, go to step 16.

14 Click on the VLAN tab button.

15 Configure the parameters:

- Enable Mobile-Tag
- Enable Authentication

16 Click on the Components tab button.

17 Right-click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

18 Configure the parameters.

- Description
- Administrative State

19 Click on the Port tab button.

20 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

21 Use the configurable filter and Search button to choose a port for user-side access to the VLAN, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

22 Click on the VLAN tab button.

23 Configure the VLAN Tagging parameter. The parameter must be set to Tagged on CES interfaces.

You can only configure this parameter when you create a SAP. After the SAP is created, the parameter cannot be modified. If you need to change the value of this parameter, you must first delete the SAP and create a SAP that matches the new requirements.

24 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

25 Click on the OK button. The Site (Create) form reappears.

26 Repeat steps 16 to 25 for each access interface that you need to create on the site.

27 Perform one of the following actions:

- If you are configuring a standard VLAN on an OmniSwitch, go to step 28.
- If you are configuring a standard VLAN on a 7250 SAS or Telco device, go to step 26.

28 Click on the STP tab button.

29 Configure the parameters:

- Enable STP
- Enable Flat STP
- Enable 1x1 STP

30 Click on the DHCP Snooping tab button if you need to enable DHCP snooping on the VLAN. The DHCP Snooping General tab is displayed.

31 Click on the Add button. The VLAN Level DHCP Snooping (Create) form opens.

32 Configure the parameters:

- VLAN Level Option-82 Data Insertion
- VLAN Level MAC Address Verification

These parameters are automatically enabled when DHCP snooping is enabled on a VLAN.

33 Click on the OK button. The VLAN Level DHCP Snooping (Create) form closes, and a dialog box appears.

34 Click on the OK button. The DHCP Snooping General tab reappears.

35 Click on the Binding Database tab button if you need to add a static entry to the DHCP binding table.

36 Click on the Add button. The DHCP Snooping Binding Database (Create) form opens.

37 Configure the MAC Address parameter.

38 Click on the Select button to choose a port. The Select Port - DHCP Snooping Binding Database form opens.

39 Choose a port from the list and click on the OK button.

40 The DHCP Snooping Binding Database (Create) form reappears.

41 Configure the parameters:

- IP Address
- Lease Time

42 Click Apply to add the static entry to the table. A warning dialogue box appears.

43 Click on the OK button.

44 Repeat steps 35 to 43 for each static entry that you need to add to the binding table.

45 Click the Cancel button to close the DHCP Snooping Binding Database (Create) form.

46 Click on the OK button. The Site (Create) form reappears.

47 Click on the OK button. The VLAN (Create) form reappears with the new site information displayed.

48 Click on the OK button to close the VLAN (Create) form.

Procedure 65-5 To create a management VLAN service

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the management VLAN. The Select Customer - VLAN form opens.

3 Select a customer for the management VLAN and click on the OK button. The Select Customer - VLAN form closes and the VLAN (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters.

- Auto-Assign ID
- Service Name
- Description
- Service Tier
- Administrative State
- OLC State

The OLC State parameter is configurable after you click on the Apply button.

Disable the Auto-Assign ID parameter and set the VLAN ID using the Service ID parameter. If the Auto-Assign ID parameter is enabled, the 5620 SAM chooses the VLAN ID.

5 Click on the VLAN tab button.

6 Set the Application parameter to Management VLAN.

7 Click on the Select button in the Group panel to choose a group to associate with the management VLAN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

9 Click on the Components tab button.

10 Right-click on VLAN and choose Create Site. The Select Network Elements - VLAN form opens.

11 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form reappears with the site information displayed on the General tab.

12 Configure the parameters.

- Description
- Administrative State
- Monitor Access Interface Operational State

13 Click on the Components tab button.

14 Right-click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

15 Configure the parameters.

- Name
- Description
- Administrative State

16 Click on the Port tab button.

17 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

18 Use the configurable filter and Search button to choose a port for user-side access to the management VLAN, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

19 Configure the remaining parameters, if required.

20 Click on the VLAN tab button.

21 Configure the VLAN Tagging parameter. This parameter must be set to Tagged on CES interfaces.

You can only configure this parameter when you create a SAP. After the SAP is created the parameter cannot be modified. If you need to change the value of this parameter you must first delete the SAP and create a new one that matches the new requirements.

22 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

23 Click on the OK button. The Site (Create) form reappears.

24 Repeat steps 14 to 23 for each access interface to be created on the site.

25 Click on the OK button. The Site (Create) form closes, and a dialog box appears.

26 Click on the OK button. The VLAN (Create) form reappears with the new site information displayed in the service components tree.

27 Click on the OK button to close the VLAN (Create) form.

Procedure 65-6 To create an OmniSwitch stacked VLAN service

Note 1 — The TLS Mode must be set to Ethernet Service before a stacked VLAN service can be created on an OmniSwitch. See Procedure 28-51 to configure the TLS Mode.

Note 2 — Alcatel-Lucent recommends that you configure OmniSwitch network ports before you configure a stacked VLAN service.

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VLAN. The Select Customer - VLAN form opens.

3 Choose a customer for the VLAN and click on the OK button. The Select Customer - VLAN form closes and the VLAN (Create) form reappears with the customer information.

4 Configure the parameters.

- Auto-Assign ID
- Service Name
- Description
- Service Tier
- Administrative State
- OLC State
  The OLC State parameter is configurable after you click on the Apply button.

Disable the Auto-Assign ID parameter and set the VLAN ID using the Service ID parameter. If the Auto-Assign ID parameter is enabled, the 5620 SAM chooses the VLAN ID.

5 Click on the VLAN tab button.

6 Set the Application parameter to L2-VPN (TLS/VLAN-Stacking).

7 Click on the Select button in the Group panel to choose a group to associate with the VLAN. The Select Group - VLAN Service form opens.

8 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form opens with the group information displayed.

9 Click on the Components tab button.

10 Right-click on VLAN and choose Create Site. The Select Network Elements - VLAN form opens.

11 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the General tab displayed.

12 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

13 Click on the Components tab button.

14 Right-click on Ethernet Services and choose Create Ethernet Service. The Ethernet Service (Create) form opens with the General tab displayed.

15 Configure the Ethernet Service Name parameter.

16 Click on the Components tab button.

17 Right-click on Ethernet Service and choose Create Service Access Multipoint. The Service Access MultiPoint (Create) form opens with the General tab displayed

18 Configure the parameters:

- Auto-Assign ID
- Service Access Multi-Point ID

19 If you need to apply a SAP policy other than the default one, click on the Clear button to clear the default SAP policy from the SAP Profile panel. Otherwise, go to step 22.

20 Click on the Select button to choose a SAP profile to associate with the service access multipoint. The Select SAP Profile - Service Access MultiPoint form opens.

21 Choose a SAP profile and click on the OK button. The Select SAP Profile - Service Access MultiPoint form closes and the Service Access Multipoint (Create) form reappears with the selected SAP profile information displayed.

22 Click on the Components tab button.

23 Right-click on Service Access Points and choose Create VLAN Service Access Point. The VLAN Service Access Point (Create) form opens with the General tab displayed.

24 Configure the parameters:

- Name
- Description

25 Click on the Port tab button.

26 Click on the Select button to choose a port for the VLAN SAP. The Select Terminating Port - VLAN Service Access Point form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

27 Use the configurable filter and Search button to choose a port for the VLAN SAP, and click on the OK button. The Select Terminating Port - VLAN Service Access Point form closes, and the VLAN Service Access Point (Create) form displays the port information.

28 Click on the Apply button if you need to add another VLAN SAP. A dialog box appears. Otherwise go to step 32.

29 Click on the OK button. The VLAN SAP appears in the list of service access points in the Components tab.

30 Click on the General tab button.

31 Repeat steps 24 to 29 to add an additional VLAN service access point.

32 Click on the OK button. The VLAN Service Access Point (Create) form closes and a dialog box appears.

33 Click on the OK button. The Service Access MultiPoint (Create) form reappears.

34 Click on the Customer VLANs tab button.

35 Click on the Add button to add a customer VLAN to the service access multipoint. The Customer VLAN (Create) form opens.

36 Configure the parameters:

- Customer VLAN ID
- Map Type

37 Click on the Apply button if you need to add another customer VLAN. A dialog box appears. Otherwise, go to step 40.

38 Click on the OK button.

39 Repeat steps 36 to 38 to add another customer VLAN.

40 Click on the OK button. The Customer VLAN (Create) form closes, and a dialog box appears.

41 Click on the OK button. The Service Access Multipoint (Create) form reappears with the customer VLAN information displayed.

42 Click on the OK button. The Service Access Multipoint (Create) form closes and a dialog box appears.

43 Click on the OK button. The Ethernet Service (Create) form reappears.

44 Repeat steps 17 to 43 to add another service access multipoint to the Ethernet service.

45 Click on the OK button. The Ethernet Service (Create) form closes and a dialog box appears.

46 Click on the OK button. The Site (Create) form reappears.

47 Repeat steps 14 to 46 to add another Ethernet service to the site.

48 Click on the STP tab button.

49 Configure the parameters:

- Enable STP
- Enable Flat STP
- Enable 1x1 STP

50 Click on the DHCP Snooping tab button if you need to enable DHCP snooping on the VLAN. The DHCP Snooping General tab is displayed.

51 Click on the Add button. The VLAN Level DHCP Snooping (Create) form opens.

52 Configure the parameters:

- VLAN Level Option-82 Data Insertion
- VLAN Level MAC Address Verification

These parameters are automatically enabled when DHCP snooping is enabled on a VLAN.

53 Click on the OK button. The VLAN Level DHCP Snooping (Create) form closes, and a dialog box appears.

54 Click on the OK button. The DHCP Snooping General tab reappears.

55 Click on the Binding Database tab button if you need to add a static entry to the DHCP binding table.

56 Click on the Add button. The DHCP Snooping Binding Database (Create) form opens.

57 Configure the MAC Address parameter.

58 Click on the Select button to choose a port. The Select Port - DHCP Snooping Binding Database form opens.

59 Choose a port from the list and click on the OK button.

60 The DHCP Snooping Binding Database (Create) form reappears.

61 Configure the parameters:

- IP Address
- Lease Time

62 Click Apply to add the static entry to the table. A warning dialogue box appears.

63 Click on the OK button.

64 Repeat steps 55 to 63 for each static entry that you need to add to the binding table.

65 Click the Cancel button to close the DHCP Snooping Binding Database (Create) form.

66 Click on the OK button. A dialog box appears.

67 Click on the OK button. The VLAN (Create) form reappears.

68 Click on the OK button to close the VLAN (Create) form.

Procedure 65-7 To create an OmniSwitch IP multicast VLAN service

1 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VLAN. The Select Customer - VLAN form opens.

3 Choose a customer for the VLAN and click on the OK button. The Select Customer - VLAN form closes and the VLAN (Create) form reappears with the customer information.

4 Configure the parameters.

- Auto-Assign ID
- Service Name
- Description
- Service Tier
- Administrative State
- OLC State

  The OLC State parameter is configurable after you click on the Apply button.

Disable the Auto-Assign ID parameter and set the VLAN ID using the Service ID parameter. If the Auto-Assign ID parameter is enabled, the 5620 SAM chooses the VLAN ID.

5 Click on the VLAN tab button.

6 Set the Application parameter to Broadcast TV (MVR/IPMV).

7 The IPMVLAN panel appears. In the panel, configure the Type parameter.

8 Click on the Select button in the Group panel to choose a group to associate with the VLAN. The Select Group - VLAN Service form opens.

9 Choose a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form opens with the group information displayed.

10 Click on the Components tab button.

11 Right-click on VLAN and choose Create Site. The Select Network Elements - VLAN form opens.

12 Choose a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the site information displayed in the General tab displayed.

13 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

14 Click on the Components tab button.

15 Right click on Access Interfaces and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed. The VLAN access interface serves as a receiver port on the IP multicast VLAN.

16 Configure the Description parameter.

17 Click on the Port tab button.

18 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

19 Use the configurable filter and Search button to choose a port for the VLAN access interface, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

Note — To configure an access interface, a stacked VLAN user port must be created. See Procedure 65-6.

20 Click on the VLAN tab button.

21 Configure the VLAN Tagging parameter.

22 Click on the Apply button if you need to add another VLAN access interface and the VLAN access interface appears in the list of access interfaces on the Components tab. A dialog box appears. Otherwise, go to step 26.

23 Click on the OK button.

24 Click on the General tab button.

25 Repeat steps 16 to 23 for each additional VLAN access interface to be added to the site.

26 Click on the OK button. A dialog box appears.

27 Click on the OK button. The VLAN Access Interface (Create) form closes.

28 Right-click on Ethernet Services and choose Create Ethernet Service. The Ethernet Service (Create) form opens with the General tab displayed.

29 Configure the Ethernet Service Name parameter.

30 Click on the Components tab button.

31 Right-click on Ethernet Service and choose Create Service Access MultiPoint. The Service Access MultiPoint (Create) form opens with the General tab displayed.

32 Configure the parameters:

- Auto-Assign ID
- Service Access Multi-Point ID

33 If you need to apply a SAP policy other than the default one, click on the Clear button to clear the default SAP policy from the SAP Profile panel. Otherwise, go to step 36.

34 Click on the Select button to choose a SAP profile to associate with the service access multi-point. The Select SAP Profile - Service Access MultiPoint form opens.

35 Choose a SAP profile and click on the OK button. The Select SAP Profile - Service Access MultiPoint form closes and the Service Access Multipoint (Create) form reappears with the selected SAP profile information displayed.

36 Click on the Components tab button.

37 Right-click on Service Access Points and choose Create VLAN Service Access Point. The VLAN Service Access Point (Create) form opens with the General tab displayed.

38 Configure the parameters:

- Name
- Description

39 Click on the Port tab button.

40 Click on the Select button to choose a port for the VLAN SAP. The Select Terminating Port - VLAN Service Access Point form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrids. After you do this, the port is listed when you click on the Search button.

41 Use the configurable filter and Search button to choose a port for the VLAN SAP, and click on the OK button. The Select Terminating Port - VLAN Service Access Point form closes, and the VLAN Service Access Point (Create) form displays the port information.

42 Click on the Apply button if you need to add another VLAN SAP. A dialog box appears. Otherwise, go to step 46.

43 Click on the OK button. The VLAN service access point appears in the list of Service Access Points on the Components tab.

44 Click on the General tab button.

45 Repeat steps 37 to 43 to add an additional VLAN SAP.

46 Click on the OK button. The VLAN Service Access Point (Create) form closes and a dialog box appears.

47 Click on the OK button. The Service Access MultiPoint (Create) form reappears.

48 Click on the Customer VLANs tab button.

49 Click on the Add button to add a customer VLAN to the service access multipoint. The Customer VLAN (Create) form opens.

50 Configure the parameters:

- Customer VLAN ID
- Map Type

51 Click on the Apply button if you need to add another customer VLAN. A dialog box appears. Otherwise, go to step 54.

52 Click on the OK button.

53 Repeat steps 50 to 52 to add another customer VLAN.

54 Click on the OK button. The Customer VLAN (Create) form closes, and a dialog box appears.

55 Click on the OK button. The Service Access Multipoint (Create) form reappears with the customer VLAN information displayed.

56 Click on the OK button. The Service Access Multipoint (Create) form closes and a dialog box appears.

57 Click on the OK button. The Ethernet Service (Create) form reappears.

58 Repeat steps 31 to 57 if you need to add another service access multipoint to the Ethernet service.

59 Click on the OK button. The Ethernet Service (Create) form closes and a dialog box appears.

60 Click on the OK button. The Site (Create) form reappears.

61 Repeat steps 28 to 60 if you need to add another Ethernet service to the site.

62 Click on the STP tab button.

63 Configure the parameters:

- Enable STP
- Enable Flat STP
- Enable 1x1 STP

64 Click on the DHCP Snooping tab button if you need to enable DHCP snooping on the VLAN. The DHCP Snooping General tab is displayed.

65 Click on the Add button. The VLAN Level DHCP Snooping (Create) form opens.

66 Configure the parameters:

- VLAN Level Option-82 Data Insertion
- VLAN Level MAC Address Verification

These parameters are automatically enabled when DHCP snooping is enabled on a VLAN.

67 Click on the OK button. The VLAN Level DHCP Snooping (Create) form closes, and a dialog box appears.

68 Click on the OK button. The DHCP Snooping General tab reappears.

69 Click on the Binding Database tab button if you need to add a static entry to the DHCP binding table.

70 Click on the Add button. The DHCP Snooping Binding Database (Create) form opens.

71 Configure the MAC Address parameter.

72 Click on the Select button to choose a port. The Select Port - DHCP Snooping Binding Database form opens.

73 Choose a port from the list and click on the OK button.

74 The DHCP Snooping Binding Database (Create) form reappears.

75 Configure the parameters:

- IP Address
- Lease Time

76 Click Apply to add the static entry to the table. A warning dialogue box appears.

77 Click on the OK button.

78 Repeat steps 69 to 77 for each static entry that you need to add to the binding table.

79 Click the Cancel button to close the DHCP Snooping Binding Database (Create) form.

80 Click on the Multicast Groups tab button.

81 Click on the Add button to add a multicast group address to the site. The Multicast Group (Create) form opens.

82 Configure the Multicast Address parameter.

83 Click on the Apply button if you need to add another multicast address. A dialog box appears. Otherwise, go to step 86.

84 Click on the OK button. The multicast address information appears on the Site (Create) form.

85 Repeat steps 82 to 84 to add another multicast address to the site.

86 Click on the OK button.

87 Click on the Customer VLAN Tags tab button.

88 Click on the Add button to add a customer VLAN tag to the site. The Customer VLAN Tag (Create) form opens.

89 Configure the Customer VLAN Tag parameter.

90 Click on the Apply button if you need to add another customer VLAN tag. The customer VLAN tag information appears on the Site (Create) form. A dialog box appears. Otherwise, go to step 93.

91 Click on the OK button.

92 Repeat steps 89 to 91 to add another customer VLAN tag to the site.

93 Click on the OK button.

94 Click on the OK button to the close the Site (Create) form. A dialog box appears.

95 Click on the OK button. The Site (Create) form closes.

96 Click on the OK button to close the VLAN (Create) form.

Procedure 65-8 To create a 9500 MPR Dot1Q VLAN service (ETSI only)

1 Right-click on a 9500 MPR in the navigation tree and choose Properties from the contextual menu. The 9500 MPR properties form opens.

2 Set the Bridge Type parameter to 802.1Q.

3 Close the 9500 MPR properties form.

4 Choose Create→Service→VLAN from the 5620 SAM main menu. The VLAN (Create) form opens with the General tab displayed.

5 Click on the Select button to choose a customer to associate with the 9500 Dot1Q VLAN service. The Select Customer - VLAN form opens.

6 Select a customer for the 9500 MPR Dot1Q VLAN service and click on the OK button. The Select Customer - VLAN form closes and the VLAN (Create) form reappears with the customer information displayed on the General tab.

7 Configure the parameters.

- Auto-Assign ID
- Service Name
- Description
- Service Tier
- Administrative State
- OLC State

  The OLC State parameter is configurable after you click on the Apply button.

Disable the Auto-Assign ID parameter and set the Service ID using the Service ID parameter. If the Auto-Assign ID parameter is enabled, the 5620 SAM chooses the VLAN ID.

8 Click on the VLAN tab button.

9 Set the Application parameter to 9500 VLAN.

10 Click on the Select button in the Group panel to choose a group to associate with the 9500 MPR Dot1Q VLAN service. The Select Group - VLAN Service form opens.

11 Select a group and click on the OK button. The Select Group - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

12 Configure the Auto-Assign ID parameter.

Disable the Auto-Assign ID parameter to set the VLAN ID using the VLAN ID parameter. If the Auto-Assign ID parameter is enabled, the 5620 SAM chooses the VLAN ID.

13 Perform one of the following:

a Enable the Specify VLAN Path parameter.

b Disable the Specify VLAN Path parameter to specify a VLAN path by clicking on the Select button in the VLAN path panel. Go to step 16.

14 Click on the Select button in the VLAN Path panel to choose a VLAN Path to associate with the 9500 MPR Dot1Q VLAN service. The Select VLAN Path - VLAN Service form opens.

15 Select a VLAN Path and click on the OK button. The Select VLAN Path - VLAN Service form closes and the VLAN (Create) form reappears with the group information displayed.

Note — The VLAN Path can consist of consecutive physical links, non-consecutive physical links, or radio links, spanning NEs.

16 Click on the Components tab button.

17 Right-click on VLAN and choose Create Site. The Select Network Elements - VLAN form opens.

Note — The Components tab will be auto-populated with Sites corresponding to the hops in the previously specified VLAN Path.

18 Select a site and click on the OK button. The Select Network Elements - VLAN form closes and the Site (Create) form opens with the site information displayed in the General tab.

19 Configure the parameters.

- Description
- Administrative State
- Monitor Access Interface Operational State

20 Click on the OK button. The Site (Create) form closes, and a dialog box appears.

21 Click on the OK button. The VLAN (Create) form reappears with the new site information displayed in the service components tree.

22 Click on the OK button to close the VLAN (Create) form.

Procedure 65-9 To associate a VLAN service with an access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Use the configurable filter and Search button to choose the VLAN service to be associated with an interface, and click on the Properties button. The VLAN - *Service Name* (Edit) form opens.

3 Click on the Components tab button.

4 Scroll through the service components tree to find the site for the new access interface.

5 Right-click on the Access Interfaces branch of the tree that is connected to the site and choose Create VLAN Access Interface. The VLAN Access Interface (Create) form opens with the General tab displayed.

6 Configure the parameters.

- Description
- Administrative State

7 Click on the Port tab button.

8 Click on the Select button to choose a port for the VLAN access interface. The Select Terminating Port - VLAN Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

9 Use the configurable filter and Search button to choose a port for the VLAN access interface, and click on the OK button. The Select Terminating Port - VLAN Access Interface form closes, and the VLAN Access Interface (Create) form displays the port information.

10 Configure the remaining parameters, if required.

11 Click on the OK button. The VLAN Access Interface (Create) form closes, and a dialog box appears.

12 Click on the OK button. The VLAN - *Service Name* (Edit) form reappears with the new interface displayed in the service components tree under Access Interfaces for the site specified in step 4.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button to confirm the action and close the dialog box. The Manage Services form reappears.

15 Click on the Close button to close the Manage Services form.

Procedure 65-10 To add a MEP to an OmniSwitch VLAN service access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Use the configurable filter and Search button to choose the VLAN service and click on the Properties button. The VLAN - *Service Name* (Edit) form opens.

3 Click on the Components tab button.

4 Scroll through the service components tree to find the access interface.

5 Right-click on the access interface and click on Properties. The VLAN Access Interface (Edit) form opens with the General tab displayed.

6 Click on the MEPs tab button.

7 Click on the Add button.

8 Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

9 Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

10 Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages
- Priority Level for CCM Messages
- Low-priority Defect

11 Click on the OK button. The VLAN Access Interface (Edit) form reappears.

12 Click on the Refresh button to update the MEP list.

13 Repeat steps 7 to 12 to add additional MEPs.

14 Close the VLAN Access Interface (Edit) form to return to the VLAN Service (Edit) form.

15 Close the VLAN Service (Edit) form.

16 Close the Manage Services form.

Procedure 65-11 To configure IGMP on an OmniSwitch VLAN site

OmniSwitch IGMP parameters can be configured globally and per VLAN site. You can configure VLAN site IGMP parameters only after you create the VLAN. VLAN IGMP configuration settings override global IGMP settings. See Procedure 28-37 for information about configuring global OmniSwitch IGMP parameters.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an OmniSwitch VLAN service.

4 Click on the Properties button. The VLAN *Service Name* (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Sites tab button.

6 Choose a site from the list and click on the Properties button. The Site (Edit) form opens with the General tab displayed.

7 Click on the IGMP tab button.

8 Choose an entry from the list and click on the Properties button. The IGMP (Edit) form opens with the General tab displayed.

9 Configure the following parameters, if required:

- Administrative State
- Querying
- Spoofing
- Proxying
- Query Interval (seconds)
- Last Member Query Interval (tenths of seconds)
- Query Response Interval (tenths of seconds)
- Robust Count
- Querier Forwarding
- Zapping
- Max Group Action
- Max Group
- Protocol Version
- Router Timeout (seconds)
- Source Timeout (seconds)
- Unsolicited Report Interval (seconds)

10 Click on the Multicast Group tab button to create a static IGMP group.

11 Click on the Add button. The Group (Create) form opens.

12 Click on the Select button to choose a terminating port. The Select Port - Group form opens with a list of available ports.

13 Choose a port from the list and click on the OK button. The Select Port - Group form closes and the selected port is displayed on the Group (Create) form.

14 Configure the Multicast Group IP Address parameter.

15 Click on the OK button. The Select Port - Group form closes, the multicast group appears in the listing, and a dialog box appears.

16 Click on the OK button.

17 Repeat steps 11 to 16 for each multicast group that you need to add.

18 Click on the Multicast Neighbor tab button to create a static IGMP neighbor.

19 Click on the Add button. The Neighbor (Create) form opens.

20 Click on the Select button to choose a terminating port. The Select Port - Neighbor form opens with a list of available ports.

21 Choose a port from the list and click on the OK button. The Select Port - Neighbor form closes and the selected port is displayed on the Neighbor (Create) form.

22 Click on the OK button. The Select Port - Neighbor form closes, the multicast neighbor appears in the listing, and a dialog box appears.

23 Click on the OK button.

24 Repeat steps 19 to 23 for each multicast neighbor that you need to add.

25 Click on the Multicast Querier tab button to create a static IGMP querier.

26 Click on the Add button. The Querier (Create) form opens.

27 Click on the Select button to choose a terminating port. The Select Port - Querier form opens with a list of available ports.

28 Choose a port from the list and click on the OK button. The Select Port - Querier form closes and the selected port is displayed on the Querier (Create) form.

29 Click on the OK button. The Select Port - Querier form closes, the multicast querier appears in the listing, and a dialog box appears.

30 Click on the OK button.

31 Repeat steps 26 to 30 for each multicast querier that you need to add.

32 Click on the OK button to close the IGMP (Edit) form.

33 Click on the OK button to close the Site (Edit) form

34 Click on the OK button to close the VLAN (Edit) form

35 Click on the Yes button to confirm the action. The VLAN *Service Name* (Edit) form closes and the Manage Services form reappears.

36 Click on the Close button to close the Manage Services form.

Procedure 65-12 To modify a VLAN service

Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VLAN service.

4 Click on the Properties button. The VLAN *Service Name* (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs contain non-configurable parameter information for the service:

- VLAN tab—displays information about the VLAN type
- MVR tab—displays multicast package policy information for the service

The MVR tab button is not selectable for some types of VLAN.

The following tabs list the service elements that can be individually or collectively selected and configured:

- Components tab—lists the various service components in a tree format
- Sites tab—lists the sites that are included in the service
- VLAN Access Interfaces tab—lists the L2 access interfaces that are included in the service
- Ethernet Services—lists the Ethernet services
- Template tab — displays the template used to create the mirror service, if applicable.
- Faults tab—displays the faults associated with the service

The Ethernet Services tab button is not selectable for some types of VLAN.

Note — Users with the administrator scope of command role can click on the Select button on the Templates tab to associate a service template with the service object, if required.

5 Modify the parameters for the service as required.

To configure items in the Components tab, right-click on the items and choose Properties from the contextual menu.

To configure items in the tabs that contain lists of service elements, choose the items and click on the Properties button.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button to confirm the action. The VLAN *Service Name* (Edit) form closes and the Manage Services form reappears.

8 Click on the Close button to close the Manage Services form.

Procedure 65-13 To view the service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VLAN (Edit) form opens.

4 View the Aggregated Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab button to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab button to view the aggregated alarms for the object. The Aggregated Alarms tab is displayed.

8 Close the VLAN (Edit) form.

9 Click on the Close button to close the Manage Services form.

Procedure 65-14 To run an OAM validation test

A validator test suite must be created for the tested entity. See chapter 75 for more information about how to create a validator test suite.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VLAN (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If a validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

   i Click on the OK button to associate the service with an existing validator test suite. The Choose Validator Test Suite form appears.

   ii Configure the filter criteria. A list of validator test suites appears.

   iii Select a validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark beside the OAM Validation Failure indicator.

6 Click on the Tests tab button.

7 Click on the Validation Result tab button.

8 Select an entry and click on the Properties button. The Tested Entity Result form opens and displays information about the validation test.

9 Close the Tested Entity Result form.

10 Close the VLAN (Edit) form.

11 Close the Manage Services form.

Procedure 65-15 To view the service topology

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VLAN service and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - *Service Name* map opens.

   See chapter 4 for more information about service topology views.

Procedure 65-16 To delete a VLAN service

Caution — Do not delete any VLANs that are used for network management, otherwise connectivity between the 5620 SAM and the 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, OmniSwitch, or Telco devices is lost.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a VLAN service from the list.

4 Click on the Delete button. A dialog box appears and prompts you to confirm that you understand the implications of deleting the service.

5 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

6 Click on the Close button to close the Manage Services form.

66 — VLAN groups and paths

66.1 VLAN groups and paths overview

The 5620 SAM supports the configuration and provisioning of VLAN groups and paths.

Note — Service provisioning using VLAN groups and paths is available for ETSI NEs only.

VLAN groups are used to do the following:

- Manage the VLAN IDs that are assigned to 9500 MPR VLAN group members.
- Logically group OmniSwitch and 9500 MPR devices to represent a typical network topology; an OmniSwitch and a 9500 MPR cannot belong to the same VLAN group.

A VLAN path is a bidirectional transport-tunnel service that is created on a 9500 MPR. VLAN paths use a tree or mesh topology. A path is defined by specifying the number of hops from a source 9500 MPR to a destination 9500 MPR. Each hop in the path is a 9500 MPR, and must belong to the same VLAN group.

9500 MPR VLAN paths can span NEs connected via both physical links and radio links.

66.2 Workflow to configure VLAN groups and paths

1 Create VLAN groups and add members to each group as required.

2 Create the VLAN paths that are required between the 9500 MPR group members. The paths are used when you create services on a 9500 MPR.

You can create 9500 MPR services and associate each service with a VLAN path. The 5620 SAM creates cross-connects on each 9500 MPR in the VLAN path that is used by a service. Each cross-connect for the same service uses the same VLAN ID.

66.3 VLAN groups and paths procedures

Use the following 5620 SAM procedures to manage VLAN groups and paths.

Procedure 66-1 To create a VLAN group

1 Choose Manage→VLAN→VLAN Group from the 5620 SAM main menu. The Manage VLAN Groups form opens.

2 Click on the Create button. The VLAN Group (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Group Name
- Description
- Node Type
- Technology
- Topology

You can configure the VLAN Space Management by SAM parameter when the Node Type parameter value is set to 9500.

You can configure the Head Ends parameter when the Node Type parameter value is set to OMNI.

4 Click on the Apply button.

5 Click on the Group Members tab button.

6 Click on the Add button. The Select Network Elements form opens and a list of available NEs is displayed. Only NE types specified by the Node Type parameter are displayed in the list.

7 Choose one or more NEs from the list and click on the OK button. A dialog box appears.

8 Click on the OK button. The selected NEs are listed on the VLAN Group (Edit) form.

9 If you enabled the Head Ends parameter, you can add head end NEs to the group. Otherwise, go to step 13.

10 Click on the Add Headend Node button. The Select Network Elements form opens and a list of available NEs is displayed. Only 7750 SR, 7710 SR, and 7450 ESS NE types are displayed in the list.

11 Choose one or more NEs from the list and click on the OK button. A dialog box appears.

12 Click on the OK button. The selected NEs are listed on the VLAN Group (Edit) form.

13 If you need to apply a span of control to a group, other than the default, click on the Spans tab button. Otherwise, go to step 14.

i Click on the Add button. The Select Span(s) - VLAN Group form opens with a list of available spans.

ii Choose one or more spans of control to apply to the VLAN group.

iii Click on the OK button. The Select Span(s) - VLAN Group form closes and a dialog box appears.

iv Click on the OK button.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The VLAN Group (Edit) form closes.

16 A list of VLAN groups is displayed in the Manage VLAN Groups form.

17 Close the Manage VLAN Groups form.

Procedure 66-2 To delete a VLAN group or group member

Note 1 — You must delete all of the members from a group before you can delete the group.

Note 2 — A 9500 MPR group member cannot be deleted if it is part of a VLAN path.

1 Choose Manage→ VLAN→VLAN Group from the 5620 SAM main menu. The Manage VLAN Groups form opens.

2 Apply a filter, or create and apply a filter, and click on the Search button. A list of VLAN groups is displayed.

3 Choose a VLAN group from the list.

4 Click on the Properties button. The VLAN Group (Edit) form opens with the General tab displayed.

5 Click on the Group Members tab button.

6 If the group does not contain any members, go to step 9. Otherwise go to step 7.

7 Choose one or more members of the VLAN group and click on the Delete button. A dialog box appears.

8 Click on the OK button to delete the group members.

9 Close the VLAN Group (Edit) form. The Manage VLAN Groups form is displayed.

10 Choose the VLAN group that you need to delete from the displayed list.

11 Click on the Delete button. A dialog box appears.

12 Click on the Yes button to delete the VLAN group.

13 Close the Manage VLAN Groups form.

Procedure 66-3 To create a VLAN path

1 Choose Manage→VLAN→Paths from the 5620 SAM main menu. The Manage VLAN Paths form opens.

2 Click on the Create button. The Create VLAN Path form opens with the Identification step displayed.

3 Configure the parameters.

- Name
- Description

4 Click on the Next button. The Define Source Site step is displayed.

5 Perform one of the following actions to specify a starting 9500 MPR.

a Choose an NE from a list.

i Click on the Select button. The Select a Network Element - Define Source Site form opens.

ii Choose a 9500 MPR in the list and click on the OK button. The management IP address of the 9500 MPR is displayed as the starting NE of the VLAN path.

b Enter the management IP address of the starting 9500 MPR.

6 Click on the Next button. The Define the Provisioned Path step is displayed.

7 Click on the Insert Hop button to insert a VLAN path hop. The Hop for New VLAN Path (Create) form opens.

8 Perform one of the following actions.

a Enter a 9500 MPR IPv4 address manually.

b Choose a 9500 MPR from a list.

i Click on the Select button. The Select a Network Element - New VLAN Path form opens.

ii Choose a 9500 MPR in the list and click on the OK button. The Select a Network Element - New VLAN Path form closes and the management IP address of the 9500 MPR is displayed on the New VLAN Path (Create) form.

9 Click on the Apply button if you need to add an additional hop. Click on the OK button after you add all of the hops.

10 Close the Hop for New VLAN Path (Create) form.

11 To change the hop sequence, choose a hop and click on the Move Up or Move Down button. The first hop in the list is the source hop and the last hop in the list is the final destination site when the form changes are saved.

12 Click on the Finish Button to save the configuration.

13 Click on the Close button. The Create VLAN Path form closes.

14 Close the Manage VLAN Paths form.

Procedure 66-4 To delete a VLAN path

Note — You cannot delete a VLAN path if it is being used by a service.

1 Choose Manage→VLAN→Paths from the 5620 SAM main menu. The Manage VLAN Paths form opens.

2 Apply a filter, or create and apply a filter, and click on the Delete button. The VLAN path and all of the associated hops are deleted.

3 Close the Manage VLAN Paths form.

67 — VLL service management

67.1 VLL service management overview

The 5620 SAM supports the provisioning of VLL services on edge devices. A VLL service is an L2 point-to-point service that connects access interfaces. A VLL service is completely transparent to customer or subscriber data and to control protocols. Because of this, the device performs no MAC learning in a VLL service.

The 5620 SAM supports multiple variations of VLL services. See "VLL types" in this section for more information.

A VLL service that connects access interfaces on one device is called a local VLL service. As there is no need for signaling between devices, a local VLL service uses no SDPs.

A VLL service that connects access interfaces on two devices is called a distributed VLL service. Subscriber or customer data enters a distributed VLL service through access interfaces on different edge devices. The VLL service encapsulates the data and transports it across a service provider IP/MPLS network through GRE or MPLS service tunnels.

Packets that arrive at an edge device are associated with a VLL service based on the access interface on which they arrive. An access interface is uniquely identified using these parameters:

- physical port or POS port and channel
- encapsulation type
- encapsulation identifier (if required, depending on encapsulation type)

A VLL service uses T-LDP signaling, and uses MPLS or GRE as the service tunnel transport.

A new or existing VLL can be configured as the spoke of an HVPLS. See "HVPLS" in section 68.1 and chapter 72 for more information.

The 5620 SAM supports end-to-end VLL configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Preconfigured template. A user that is assigned the template management role can create a service template. The template management user can also configure and bind site, circuit, and L2 interface templates to the service template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

Common to all device services, such as VLL, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces or circuits, when the service is configured or modified. The following policies are common to all device services:

- QoS policies define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy form, the Access Egress Policy form, and the ATM QoS Policy form. Because a VLL service is a point-to-point service, ingress QoS policies create only the unicast queues that are defined in the policy and not the multicast queues.
- (Epipe service only) Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy and HSMDA Scheduler Policy forms.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy form.
- Filter policies control network traffic into or out of an interface or circuit based on IP or MAC matching criteria. Filter policies are configured using the ACL IP Filter form and the ACL MAC Filter form.
- Accounting policies measure the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy form.
- ANCP policies provide status and control information based on port-up and port-down messages and changes to the current access line rate between the edge device and the access node. ANCP policies are configured using the Manage Subscriber Policies form.
- Time of day suites specify time and day restriction policies that are assigned to QoS policies and schedulers, ACL filters, and aggregation schedulers. Time of day suites and time range policies are configured using the Time of Day Suite form and Time Range form, respectively.

See chapter 43 for more information about policies.

OAM diagnostics can be performed on a per-service basis. See chapter 35 for more information.

The General tab of the VLL service management form displays information about the operational state of the service and its sites through the Operational State and State Cause indicators.

The Operational State indicator identifies the states of the sites that are part of the service, as follows:

- Up—one operational path in both directions (end-to-end)
- Down—path is not operationally complete

When the Operational State is Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator.

You can run the OAM Validation test suite for the service by clicking on the Validate button. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. In addition, the Validation Result tab on the Tests tab displays detailed information about the OAM test result. See chapter 75 for more information about how to configure OAM validation test suites.

The 5620 SAM also monitors the status of a peer SAP after a VLL has been created and put into service. Status information includes faults detected on the service tunnel, and access and network SAP transmissions and receptions. The States tab of the Spoke SDP Binding form displays indicators of failure in the VLL in the State Cause panel.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default Service Tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology views. See chapter 72 for more information about the hierarchical organization of composite services.

VLL types

The 5620 SAM supports the creation of the following VLL service types:

- Apipe, or ATM VLL service
- Epipe, or Ethernet VLL service
- Fpipe, or frame relay VLL service
- Ipipe, or IP interworking VLL service
- Cpipe, or circuit emulation VLL service

Apipe (ATM VLL)

An Apipe, or ATM VLL service, provides a point-to-point ATM service between users who connect to 7750 SR, 7710 SR, 7705 SAR, or 7450 ESS NEs in an IP/MPLS network directly or through an ATM access network. One endpoint of an Apipe uses ATM encapsulation and the other endpoint uses ATM or frame relay encapsulation. An ATM PVC—for example, a VC or a VP—is configured on the managed device. As a result, the ATM switches at the service endpoints appear to be directly connected over an ATM link. The 5620 SAM supports VPI/VCI translation in an Apipe and supports local cross-connecting when the Apipe endpoints are on the same managed device.

An Apipe encapsulates standard UNI/NNI cells that ingress the ATM SAP into a pseudowire packet using N:1 cell mode encapsulation or AAL-5 SDU mode encapsulation. When using N:1 cell mode encapsulation, an Apipe supports cell concatenation into a pseudowire packet and the setup of both VC- and VP-level connections.

For ATM and frame relay interworking, an Apipe provides a point-to-point service between a user who connects to an existing ATM network and another user who connects to a PE in an IP/MPLS network. An ATM AAL-5 SDU pseudowire or a frame relay 1-to-1 mode pseudowire connects the nodes. The PE performs an FRF.5 interworking function to join the ingress and egress data paths.

An ATM VT SAP on a PE is identified by the physical port and VPI range. Cells that arrive on a specified port and are within the specified VPI range go into a single pseudowire for transport through the IP/MPLS network. A user can configure the whole ATM port as a VT and does not need to specify a VPI range. There is no ingress or egress VPI/VCI translation or loss of cell order.

Epipe (Ethernet VLL)

An Epipe, or Ethernet VLL service, provides a point-to-point Ethernet service. One endpoint of an Epipe uses Ethernet encapsulation, and the other endpoint uses Ethernet, ATM, frame relay encapsulation, or CEM encapsulation. An Epipe effectively provides ATM and frame relay bridged encapsulation termination for interworking. The 5620 SAM supports local cross-connecting when the Epipe endpoints are on the same device. The device supports these Epipe connectivity scenarios:

- a frame relay or ATM user in an ATM network communicating with an Ethernet user on an IP/MPLS network
- a frame relay or ATM user who connects to a PE device in an IP/MPLS network and communicates with an Ethernet user who connects to another PE device in the same network

ATM users connect through a UNI using AAL-5 or bridged Ethernet PDUs, and use the VCI/VPI as the ATM SAP identifier. Frame relay users connect through a UNI that uses Multiprotocol Interconnect over frame relay or bridged Ethernet PDUs, or over an Ethernet UNI interface. The DLCI is the frame relay SAP identifier. The VCI/VPI and DLCI identifier tags are transparent to the service and remain unaffected during transport.

The 5620 SAM supports the following Ethernet SAP encapsulations for an Epipe service:

- null
- dot1q
- SONET/SDH BCP-null
- SONET/SDH BCP-dot1q

Epipe services allow you to designate a dot1q encapsulated SAP as the default SAP for a specific port. For more information about how you can use default SAPs on an Ethernet port, see "Default SAPs" in section 68.1.

A default SAP can co-exist with other SAPs on a port, but it cannot be implemented on a null encapsulated port. Through the SAM 5620 interface, you can create a default SAP by specifying an outer encapsulation value of 4095 or * to a SAP. If OSSI is used, the outer encapsulation value is always 4095.

Fpipe (frame relay VLL)

An Fpipe, or frame relay VLL service, provides a point-to-point frame relay service between users who connect to PE 7750 SR, 7710 SR, or 7450 ESS NEs in an IP/MPLS network. Both endpoints of an Fpipe use frame relay encapsulation. An Fpipe connects users through frame relay PVCs. An Fpipe receives standard Q.922 core frames on the frame relay SAP and encapsulates them in a pseudowire packet according to the 1-to-1 frame relay encapsulation mode. This is the VC type used on the SDP by default. The 5620 SAM does not support the many-to-one, or port encapsulation, mode. Fpipe creation supports local cross-connecting when the endpoints are on the same managed device.

Ipipe (IP interworking VLL)

An Ipipe, or IP interworking VLL service, uses the IP/MPLS network to provide Layer 3 connectivity between different Layer 2 technologies. An Ipipe service provides point-to-point IP connectivity between a user on a frame relay, ATM, cHDLC, or PPP access circuit with routed PDU IPv4 encapsulation and a user on an Ethernet interface. The Ethernet SAP interface can terminate on a 7705 SAR, 7750 SR, 7450 ESS, or 7710 SR.

Table 67-1 summarizes the supported SAP types.

Table 67-1 Supported SAP types

SAP Types	Frame relay	ATM	PPP/IPCP	cHDLC	Ethernet
Frame relay	✓	✓			✓
ATM	✓	✓			✓
PPP/IPCP			✓		✓
cHDLC				✓	✓
Ethernet	✓	✓	✓	✓	✓

In an Ipipe service, both CE devices appear to be on the same IP interface. The PE devices must therefore resolve Layer 2 addresses when different resolution protocols are used on either SAP. Each PE device is manually configured with the IP addresses of both CE devices, or alternatively, can be set to automatically discover the IP addresses of the CE routers. The PE device maintains an ARP cache context for each IP interworking VLL, and responds to ARP request messages received on the Ethernet SAP. The PE device responds with the Ethernet SAP configured MAC address as a proxy for an ARP request for the frame relay, ATM, or PPP user access circuit IP address, and silently discards any ARP request message received on the Ethernet SAP for any other address. The PE device maintains a record of the association of IP addresses with MAC addresses for ARP requests that it receives over the Ethernet SAP.

An Ipipe SAP can be bound to a physical or logical port with PPP, cHDLC, ATM, or FR encapsulation. In 8.0 R5, when IPv6 is enabled, cHDLC, ATM or FR encapsulation are not supported. ATM users connect through a UNI using AAL-5 MUX IP or AAL-5 SNAP routed PDU encapsulation. Frame relay users connect using routed PDU IPv4 encapsulation. PPP interfaces use PPP/IPCP encapsulation of an IPv4 packet. Users of cHDLC connect using routed IPv4 encapsulation.

The 5620 SAM supports the following Ethernet SAP encapsulations for an Ipipe service:

- Null
- Dot1 Q
- Q in Q

Note — IPCP SAPs on the 7705 SAR can be configured to assign primary and secondary DNS addresses to the remote peer.

The following identifiers are used for packet forwarding:

- VCI/VPI as the ATM SAP identifier
- DLCI as the frame relay SAP identifier

Cpipe (circuit emulation VLL)

A Cpipe, or circuit emulation VLL service, provides a point-to-point CEM service between users who connect to 7210 SAS-M, 7210 SAS-M24F2X, 7210 SAS-M24F2XFP [ETR], 7750 SR, 7710 SR, or 7705 SAR devices in an IP/MPLS network directly. The endpoints of a Cpipe uses CEM encapsulation.

The Cpipe L2 access interface can be bound to a unstructured DS1 or E1 channel, a channelized DS0 channel group, or a DS0 group with CAS signalling. Consider the following when creating a Cpipe:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints.
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

9500 MPR Cpipe

A 9500 MPR Cpipe service provides a CEM-to-CEM or CEM-to-Ethernet service between 9500 MPR NEs over a VLAN path. A VLAN path consists of several hops; each hop is a 9500 MPR node.

A 9500 MPR service is created by configuring sites and access interfaces, and then associating the service with a VLAN path. The 5620 SAM creates cross-connects on all 9500 MPRs along the VLAN path. The cross-connects are associated with a specific VLAN path instance for a service. The VLAN path instance and all of the cross-connects on the service can be viewed along with other service properties.

All 9500 MPR services use the default customer and are identified by a VLAN ID assigned at each inflow interface and a service ID. The service ID and VLAN ID have different values.The VLAN ID can be automatically assigned by the 5620 SAM or assigned by the user. When the 5620 SAM assigns the VLAN ID the ID is based on the VLAN group that the endpoint 9500 MPR belongs to.

VLL spoke switching

VLL spoke switching allows you to create a VLL service by cross-connecting two spoke SDPs. Spoke switching allows you to scale L2 services, such as VLLs and H-VPLS, over a multi-area network without the requirement for a full mesh T-LDP. The 5620 SAM supports spoke switching on all VLL types, however, all service instances must be the same type.

The 5620 SAM supports VLL services with spoke switching on the 7750 SR and 7450 ESS.

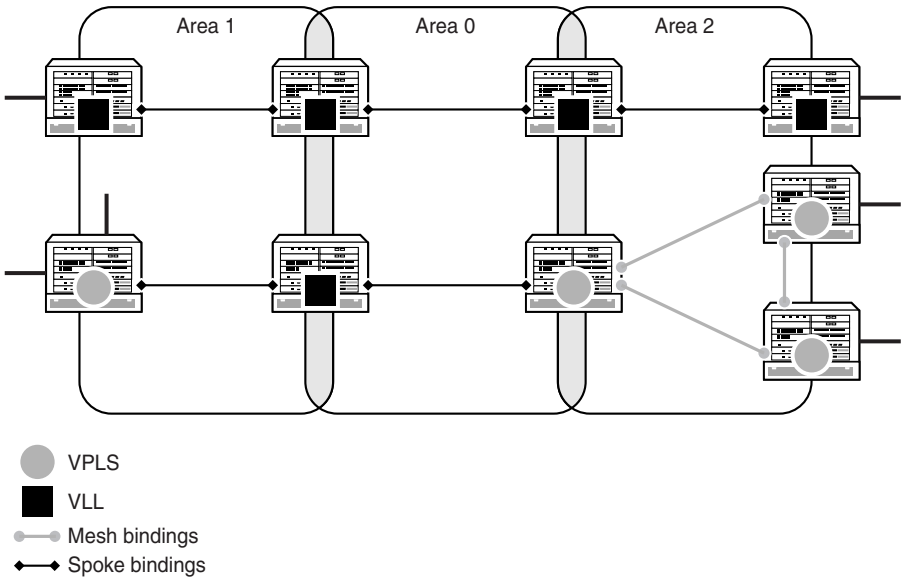
Table 67-2 describes the VLL site types that you can use in a spoke switching configuration.

Table 67-2 VLL site types

VLL site type	Description
Terminating	VLL instance has one or two VLL SAPs.
Switching	VLL instance cross-connects two spoke bindings.

Figure 67-1 shows a switching VLL that connects two VPLS. The configuration uses two T-PEs, three S-PEs, and two pairs of spoke bindings to connect the two VPLS.

Figure 67-1 VLL spoke switching



Configuration requirements

You must consider the following configuration rules when provisioning VLL services with spoke switching:

- Service type must be a VLL at the switching node.
- VC IDs can be different for the segments in the service.
- Segments in the service can run on different types of tunnels; for example, LDP, GRE, and RSVP SDPs.
- VLL instances in a service must use the same service ID to avoid the discovery of multiple and composite services.
- VLL with one or more switching sites must have two or more terminating sites.
- Autobinding creation service is not supported for switching VLLs.

VLL redundancy

VLL redundancy requires that you associate the SAP or SDP bindings to an endpoint. You can configure the endpoint association as active or standby so that you can create a redundant configuration. The associated nodes use signaling to determine the active SAP or SDP binding. The 5620 SAM supports VLL redundancy on the 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR.

A VLL service site can have up to two local endpoints. A local endpoint combines a SAP with a binding (access) or a group of bindings (network). A SAP or an SDP binding can also exist without an endpoint association.

The 7450 ESS, 7710 SR, and 7750 SR support HSDPA offload fallback for VLL Apipe and Epipe services by allowing fallback from an active PW on a primary spoke SDP to a secondary SAP.

Table 67-3 describes the components in redundant VLL configurations.

Table 67-3 VLL components for redundant configurations

VLL component	Description
Primary or Redundant binding	Primary or redundant binding is the same as a regular spoke binding. Up to four spoke bindings can form a VLL instance network endpoint. Only one binding can be configured as the primary; up to 3 others can only be configured as redundant spokes. Each redundant spoke has a precedence value to decide which spoke is the immediate backup. Only the terminating VLL instance can have multiple bindings on the network side endpoint. A switching VLL instance has up to 2 bindings, one on each side.
Inter-Chassis Backup	You can use an ICB in conjunction with a redundant SAP to provide protection for the SAP. The SAP must also be associated with a MC-LAG or MC-APS port. The ICB transports network traffic to the SAP on the second PE when the local SAP is unavailable. You must define a switching state for the redundant SAP. You must also configure the return ICB on the opposite endpoint of the protected site.

Configuration options

Table 67-4 describes the redundancy configuration options for each VLL site.

Table 67-4 VLL redundancy configuration options

Option	Configuration	Description
1	SAP SDP binding	You can create an endpoint without any SAP or SDP.
2	SAP SAP	You can create an endpoint without any SAP or SDP.
3	SDP binding SDP binding	You can configure this option for switching sites only.
4	SAP Endpoint with SDP bindings (maximum of 4 spokes and 1 ICB)	Figure 67-2 shows the configuration of this option on the PE nodes.
5	Endpoint with SAP/ICB SDP binding	Figure 67-3 shows the configuration of this option on Node B.
6	Endpoint with SAP/ICB endpoint with SAP/ICB	Figure 67-4 shows the configuration of this option.
7	Endpoint with SAP/ICB Endpoint with up to 4 SDP bindings	Figure 67-5 shows the configuration of this option.

Figure 67-2 VLL redundancy configuration - option 4

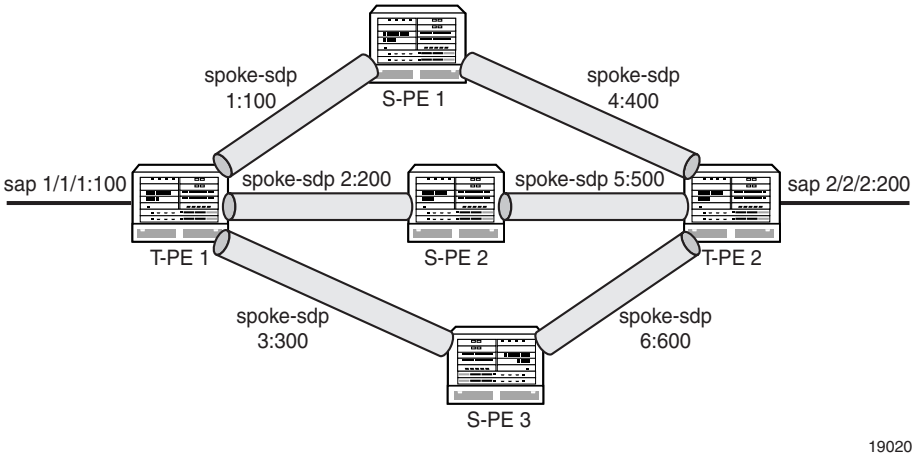
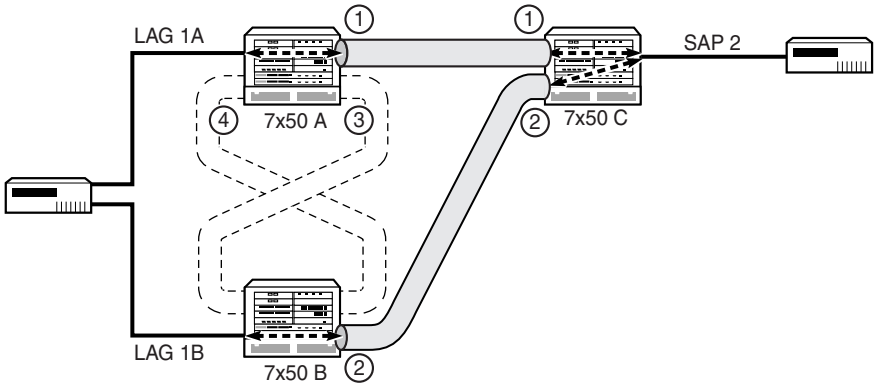


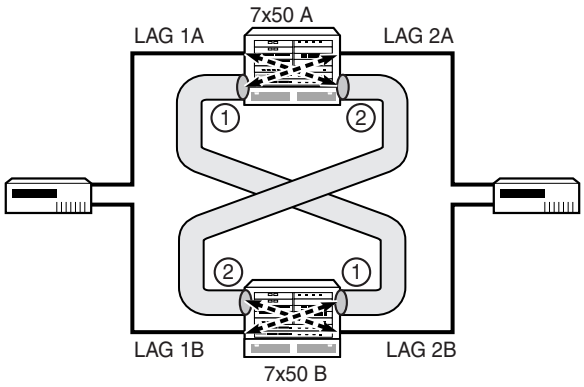
Figure 67-3 VLL redundancy configuration - option 5



1 SPOKE-SDP 1:100
2 SPOKE-SDP 3:300
3 SPOKE-SDP 2:200 (ICB)
4 SPOKE-SDP 4:400 (ICB)

19022

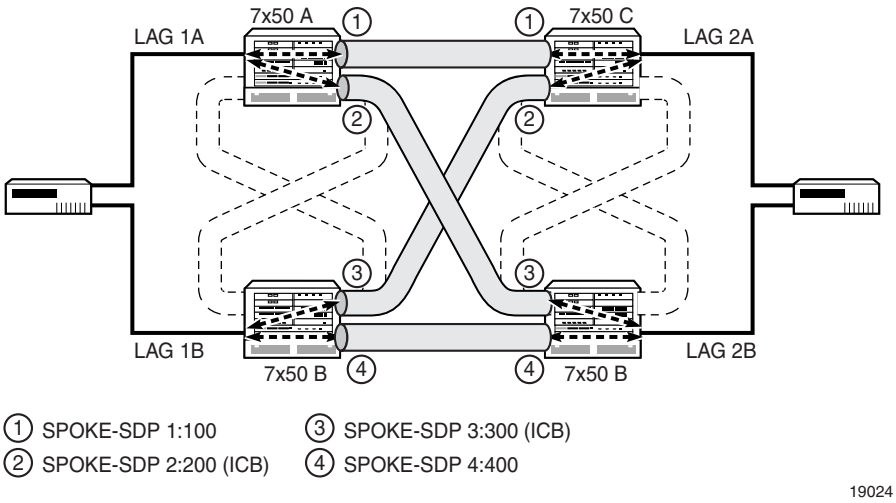
Figure 67-4 VLL redundancy configuration - option 6



1 SPOKE-SDP 1:100 (ICB)
2 SPOKE-SDP 1:200 (ICB)

19023

Figure 67-5 VLL redundancy configuration - option 7



Configuration requirements

You must consider the following configuration rules when provisioning VLL services with spoke switching and redundancy:

- A VLL service can have one or more VLL instances. An instance can reside on a 7210 SAS-M, 7705 SAR, 7750 SR, 7450 ESS, or 7710 SR.
- Local endpoint rules:
  - A VLL instance has a maximum of two endpoints. A terminating VLL instance has at least one access endpoint and a switching VLL instance has two network endpoints.
  - A network endpoint has a maximum of four spoke-bindings, which can include any combination of the following: a single primary spoke, one or more secondary spokes with precedence, and one ICB spoke.
  - A SAP or a binding has a maximum of one endpoint association.
  - An endpoint has a maximum of one SAP.
  - A SAP or a binding with association to an endpoint can be moved to another endpoint or removed from that endpoint.
- SAP rules:
  - A MC-LAG SAP or MC-APS SAP cannot be deleted when there is an ICB on the same endpoint.
  - SAPs cannot exist on switching sites.
  - A maximum of two SAPs can exist for each site.
  - A SAP with a non-ICB spoke cannot exist on the same endpoint.
  - Apipe and Epipe services support MC-APS.

- Spoke binding rules:
  - The SDP types (GRE, MPLS) used by the redundant spoke bindings do not have to be the same when you manually create the spoke bindings.
  - Redundant configurations are not supported for S-PE because there are a maximum of two spoke bindings for a switching VLL instance.
  - An ICB SDP binding should not be created on an endpoint without a MC-LAG SAP or MC-APS SAP.
  - Only one ICB can exist for each endpoint.
  - ICB SDP binding can only have a precedence of 4, the lowest priority.
  - Only one primary spoke can exist for each endpoint.
  - Spoke SDP binding cannot associate with an endpoint on a switching site.
- HSDPA offload fallback rules:
  - Apipe and Epipe services support HSDPA offload fallback on ATM interfaces.
  - The spoke SDP must be configured with primary precedence.
  - The SAP must be configured with MC-APS or ATM channel.
  - When the SAP is configured with MC-APS, the spoke SDP can be configured with ICB.

HSDPA Offload Resiliency

Mobile service providers deliver both voice and data services to their customers using mobile handsets. The data services provided require significantly more bandwidth than voice services. In order to minimize the operational costs (specifically, bandwidth), service providers typically separate the voice and data traffic at the mobile base station. The voice traffic may be backhauled over an ATM infrastructure, while a Metro Ethernet infrastructure (their own or third-party) is used to backhaul the data traffic. The separation of data traffic onto a separate network for backhaul is referred to as High Speed Data-Link Packet Access offload.

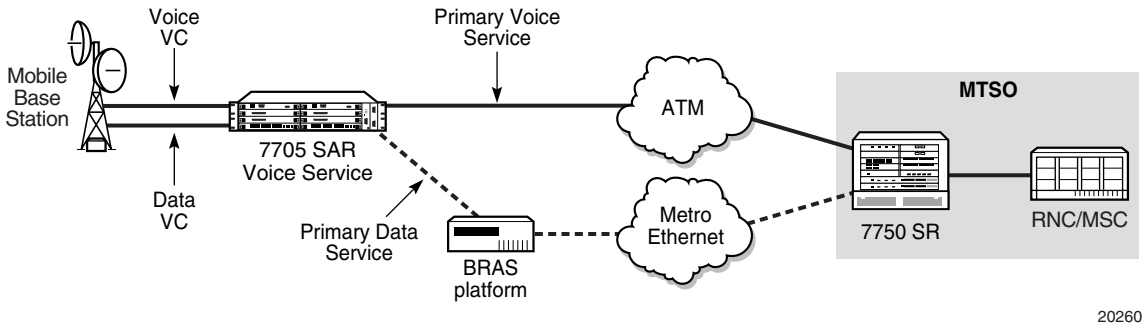
The HSDPA Apipe services traverse a path over the Metro Ethernet network which contains single potential points of failure that are unprotected. The ATM network can be used to provide a transient path for the data service in the event of a failure in the Metro Ethernet infrastructure, as long as the voice traffic is not impacted (data traffic is given lower QoS priority by the 7705 SAR and 7750 SR NEs). Clearly there is potential for the data service to suffer degradation (depending on the bandwidth required), until the fault in the Metro Ethernet network is resolved. However the SLA requirements for the data service are typically best effort.

The ability to switch to this alternate transient pathway for the data service is referred to as HSPDA resiliency.

HSPDA resiliency is implemented through the use of VLL Apipes on the 7705 SAR, Release 1.1 or later. The network architecture used in the ATM backhaul scenario is shown in Figure 67-6.

Note — For HSPDA offload resiliency, the primary and secondary services must be on the same NE.

Figure 67-6 ATM-based HSDPA offload architecture - nominal operation



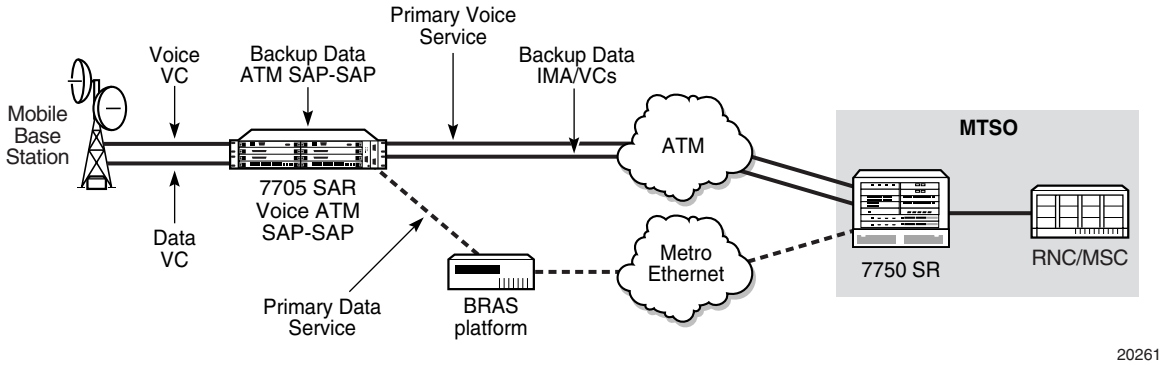
The mobile base station node separates the voice and data traffic and delivers the two different traffic types to the 7705 SAR on different VCs. Both the voice and data services use Apipe pseudo-wires to carry the traffic over the backhaul network to the 7705 SAR. The HSDPA Apipe service is paired with an OAM service (not shown in Figure 67-6) which is used by the wireless infrastructure to monitor the end-to-end path between the wireless endpoints.

For the ATM voice traffic, an internal Apipe is used on the 7705 SAR to switch ATM cells between the access VC/IMA group and the network side VC/IMA group. The service does not span the radio access network between the 7705 SAR and the 7750 SR located at the Mobile Telephone Switching Office (MTSO).

Data Apipe services (HSDPA/OAM) use service tunnels based on either MPLS or GRE. GRE is generally used in the context of a third-party Metro Ethernet network, since there is a Broadband Remote Access Server (BRAS) in the path between the DSLAM and the 7750 SR located at the MTSO (BRAS platforms do not support MPLS). MPLS is typically used when the mobile provider owns the Metro Ethernet network.

When the resiliency solution described below detects a failure in the Metro Ethernet network, its protection mechanism switches the traffic associated with the data service from the path over the Metro Ethernet network to a path which traverses the ATM (shown in Figure 67-7). The detection, switchover, and switchback mechanisms are implemented by the 5620 SAM.

Figure 67-7 HSDPA Offload Protection - ATM data backhaul



A backup (secondary) data service for an active (primary) data service is pre-configured on the 7705 SAR. For a typical 7705 SAR deployment at a cell site, two backup services are required, one for the HSDPA service and one for the OAM service. These backup services are created by the operator during the deployment of the 7705 SAR. A peer resiliency relationship between the active and backup services must also be configured.

The backup services used are internal Apipes. The switchover from primary to secondary is triggered by an event from the 7705 SAR sent to 5620 SAM, which indicates that the service tunnel (SDP) has failed. When the failure event is processed by 5620 SAM, the SAPs on the active data services are moved (along with the associated VCs) from the active service to its peer backup service and are enabled. After the re-configuration of the SAPs on the backup services completes, the traffic is moved to the backup services, which then carry the traffic over the ATM portion of the network. When the switchover is complete, an alarm is raised against the primary service indicating that it has been switched to the secondary service.

Other considerations include the following:

- If a service configured as primary is deleted from 5620 SAM or the CLI, then the corresponding resiliency is also deleted.
- If a service configured as secondary is deleted from 5620 SAM, this is blocked and a pop-up message indicates that the corresponding resiliency must first be deleted.
- If a service configured as secondary is deleted from the CLI, an alarm is raised indicating that the resiliency is misconfigured. If a secondary service is then subsequently added to the resiliency, this alarm is cleared.
- If the SAP initially configured on the primary service is deleted, the 5620 SAM raises an alarm. If the SAP is restored in the same service, the alarm clears.
- When the 5620 SAM detects that a failed SDP is up, which indicates that the primary service has recovered, the resiliency is set to the Secondary (Debounced) state and a damping timer is started. If the SDP goes down while the resiliency is in the Secondary (Debounced) state, the resiliency changes to the Secondary state and the damping timer stops. If the SDP changes state during the damping time, the value of the damping timer doubles until it rises to the maximum damping time. This prevents the service from flapping between primary and secondary. If the SDP does not change operational state during the damping time, the resiliency is set to Primary, the SAP is moved from the secondary to the primary service, and the alarm related to the service switch clears.
- After the primary service is restored, the damping timer value is set back to its initial value. The damping timer value is not displayed. The initial damping time is 30 000 ms; the time doubles, if required, to a maximum of 480 000 ms.
- The availability of this HSDPA resiliency feature is controlled by the 5620 SAM license key. If this feature is enabled using the 5620 SAM license key, then the Manage→Redundancy→HSDPA Resiliency feature is available on the main 5620 SAM menu, otherwise it does not appear. This feature also requires the SAM(P) module. A new package is added to the 5620 SAM License form called the Mobile Services Package. The HSDPA Resiliency feature is available when this package is enabled.

SDP bindings bandwidth allocation

You can administratively account for the bandwidth used by VLL services inside an RSVP SDP that consists of RSVP LSPs. The SR service manager keeps track of the available bandwidth for each SDP.

When you create a service tunnel, you configure an SDP Bandwidth Booking Factor percentage, which is applied to the SDP available bandwidth. You then assign an SDP Admin Bandwidth value (in kbps) to the spoke SDP. When you bind a VLL service to this SDP, this amount of bandwidth is subtracted from the adjusted available SDP bandwidth. If you subsequently delete the VLL service binding from this SDP, this bandwidth amount is added back into the adjusted SDP available bandwidth. If you overbook the total adjusted SDP available bandwidth when adding a VLL service, a warning is issued and the binding is rejected.

This feature does not guarantee bandwidth to a VLL service, as there is no change to the data path to enforce the bandwidth of an SDP by means such as shaping or policing of the constituent RSVP LSPs. Also, this feature does not provide a CAC capability for a local VLL service which consists of a cross-connect between two SAPs.

In addition, if multipoint services such as VPLS and VPRN are using the same SDP for forwarding packets, the amount of bandwidth consumed by these services is also not accounted for. Therefore, it is advisable to dedicate an SDP for VLL services for which bandwidth reservation is required. Furthermore, VPLS and VPRN services which use separate SDPs but which forward packets over the same network port as the VLL SDP also do not have their bandwidth accounted for. This may impact the bandwidth available to the VLL services.

Auto SDP binding (for all spoke bindings or just the return binding) cannot be used when there is a bandwidth request for the binding. The converse also applies. An error message appears when saving the configuration if this conflict occurs. 5620 SAM checking is done for OSSI.

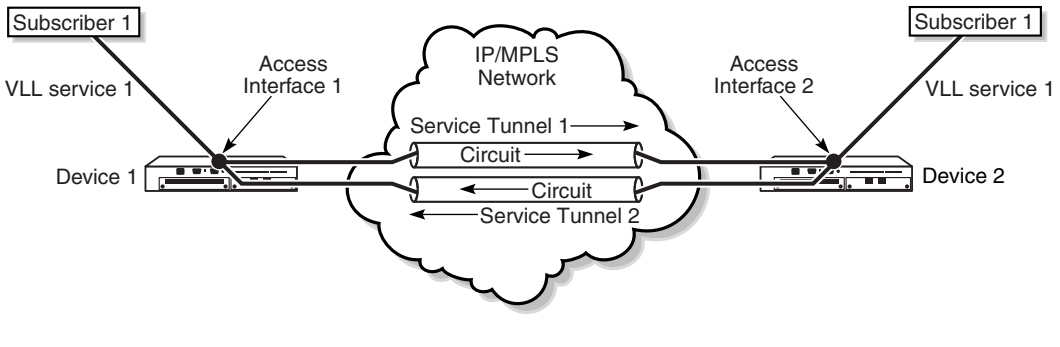
Copying and moving SAPs between ports

You can copy and move SAPs between ports. See section "Moving and copying SAPs between ports" in chapter 15 for more information.

67.2 Sample VLL service

Figure 67-8 shows a sample VLL service.

Figure 67-8 Sample VLL service



Assuming the core IP/MPLS network and service tunnels have already been configured, Table 67-5 shows the high-level tasks required to configure this sample VLL service.

Table 67-5 Sample VLL service configuration

Task	Description
1. Configure policies as required	Policies should be configured prior to creating a service. Participation in policies is defined when you configure or modify resources such as access interfaces during VLL service creation or modification. The following key policies can be applied to resources that are part of a VLL service. • Access ingress and egress interface policies, or ATM policies. Choose Policies→QoS→SROS QoS→Access Ingress, Access Egress, or ATM QoS to open these forms. • Scheduler policy. Choose Policies→QoS→SROS QoS→Scheduler to open the scheduler policy form. • ACL IP and ACL MAC filter policies. Choose Policies→Filter→ACL IP Filter or ACL MAC Filter to open the filter policy form. • Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form. • ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form.
2. Configure ports as access ports for use in the service	If applicable, choose a port from the navigation tree, right-click on the port, and choose Properties from the contextual menu. Specify the port as an access port and specify an encapsulation type, if required.
3. Configure service tunnels as required	Service tunnels are automatically created if there are no tunnels between the source and destination devices. You must choose GRE as the transport type for the 5620 SAM to automatically create service tunnels. To manually create service tunnels, choose Manage→Service Tunnels. Unidirectional service tunnels carry service traffic between edge managed devices using aggregated SDP bindings. SDP bindings can be associated with service tunnels during service configuration. During service creation, you can also configure the 5620 SAM to automatically create and associate service tunnels with SDP bindings. In this case, you do not have to create service tunnels before you create the service. After you have created a VLL, status indicators display selected operational failures on the service tunnel and peer SAP.
4. Create and configure Subscriber 1	Choose Manage→Service→Customers to open the customer manager form and create a customer.

(1 of 2)

Task	Description

5. Create and configure Service 1	Choose Create→Service→VLL→*Type of VLL service*. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure Service 1.
	• Associate Subscriber 1 with the service.
	• Specify Device 1 and Device 2 as the sites for the VLL service.
	• Configure and specify Access Interface 1 and Access Interface 2 as the access interfaces for the VLL service. You do the following when you configure access interfaces.
	  • Specify the ports for the access interfaces. Ethernet ports must be configured as access ports.
	  • Specify participation of the access interfaces in access ingress, access egress, and ATM QoS policies as required.
	  • Specify participation of the access interfaces in aggregation rate limiting across a card or port. If aggregation is not required, specify participation of the access interfaces in ingress and egress scheduler policies. If aggregation is required, specify participation of the access interfaces in an aggregation scheduler policy.
	  • Specify participation of the access interfaces in scheduler policies as required.
	  • Set the ATM OAM Terminate parameter to Up when the VLL L2 access interface port belongs to a MC-APS channel and the VC Type parameter is set to ATM-SDU.
	Create and configure circuits in both directions. Associate the circuit from Device 1 to Device 2 with Service Tunnel 1. Associate the circuit from Device 2 to Device 1 with Service Tunnel 2. You can also configure the 5620 SAM to automatically create and associate service tunnels with circuits.

(2 of 2)

67.3 Workflow to create a VLL service

1. Set up group and user access privileges.
2. Configure the network:
   - i. Build the IP or IP/MPLS core network.
   - ii. Configure ports for the service as access ports.
   - iii. Configure service tunnels, if required.
3. Configure pre-defined QoS, scheduling, filter, accounting, and time of day suite policies.

4 Provision the service:

i Set up customers or associate existing customers with the new service.

ii Create the VLL service:

- Define the service type as Epipe, Apipe, Fpipe, Ipipe, or Cpipe.
- Ensure that the LSP network is configured when the transport mechanism is MPLS.
- Specify the devices (sites) used in the service based on the following topologies:
  - Traditional VLL: terminating site only
  - Switching VLL: switching site with two or more terminating sites
  - Redundant VLL: ICB spoke to MC-LAG (Epipe) or MC-APS (for Apipe and Epipe)
- Specify the following information for redundant VLL services:
  - endpoints
  - access interfaces for VLL terminating sites
- Specify the following information to create a VLL Apipe or Epipe HSDPA offload fallback solution:
  - endpoints
  - SAP on endpoint one with MC-APS or ATM channel
  - spoke SDP with ICB on endpoint one
  - spoke SDP with primary precedence on endpoint two
  - SAP on endpoint two with MC-APS
  - spoke SDP with ICB on endpoint two
- Specify aggregation on a service basis, or across a card or port.
- Specify QoS, scheduling, accounting, ANCP, MEP association and filter policies.
- Specify the time of day suite.

5 Create SDP bindings to use the service tunnels.

6 Turn up the service.

67.4 Workflow to create a 9500 MPR Cpipe service

1 Set up group and user access privileges.

2 Configure the network:

i Create VLAN groups and assign 9500 MPR NEs to the groups.

ii Create 9500 MPR VLAN paths.

3 Provision the service:

i The 5620 SAM uses the default customer for all 9500 MPR Cpipe VLL services.

ii Create the Cpipe VLL service:

- Define the service type as 9500 VLL Cpipe.
- Specify the VLAN path used by the service.
- Specify the devices (sites) used in the service.
- Specify the access interfaces for the service sites.

67.5 VLL service management procedures

Use the following procedures to perform VLL service creation and management task

Procedure 67-1 To create a VLL Epipe service using configuration forms

1 Choose Create→Service→VLL→Epipe from the 5620 SAM main menu. The VLL Epipe (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - VLL Epipe form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - VLL Epipe form closes and the VLL Epipe (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Inherit Service ID Value
- Default VC ID
- Service Name
- Description
- Service Tier
- Administrative State
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
- Transport Type
- OLC State

The Service ID parameter is enabled when the Auto-Assign ID parameter is disabled.

The Default VC ID parameter is enabled when the Inherit Service ID Value parameter is disabled.

The Profile Name and Transport Type parameters are only displayed when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled. The Transport Type parameter is only configurable if the Profile Name parameter is left blank.

The OLC State parameter is configurable after you click on the Apply button.

The CAC Status, CAC Probable Cause, and Last CAC Time fields are visible if service CAC has been configured. See step 41 for more information. The Last CAC Time field displays the last time that a CAC verify or CAC audit was run.

5 Perform one of the following:

a Create a site for the VLL. Go to step 6.

b Complete VLL creation if sites and interfaces are to be created later. Go to step 45.

6 Click on the Components tab button.

7 Right-click on VLL Epipe and choose Create Site. The Select Network Elements - VLL Epipe form opens with a list of available sites.

8 Choose a site and click on the OK button. The Site (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- MTU
- Enable MTU Check
- Administrative State
- Monitor Access Interface Operational State
- Per Service Hashing for LAG Enabled
- VLL Site Type

The VLL Site Type parameter is configurable only on the 7450 ESS, 7710 SR, and 7750 SR.

10 Click on the Apply button.

11 Click on the Components tab button.

12 Perform one of the following:

a Link the site to a Backbone VPLS. Go to step 13.

b Create endpoints for a redundant VLL. Go to step 15.

Note — Redundant VLL Epipe services are configurable on the 7705 SAR, 7450 ESS, 7750 SR, and 7710 SR.

c Create an L2 access interface for the VLL terminating site. Perform Procedure 67-11.

d Create a spoke SDP binding for the site. Go to step 22.

e Complete site creation. Go to step 42.

13 Choose the Backbone VPLS site to link the Epipe service to. For additional information on Provider Backbone Bridging, see chapter 68.

i Click on the Backbone tab button.

ii Click on the Select button. The Select Backbone VPLS Site - Site form is displayed.

iii Click the Search button. A list of all the B-Sites that can be used by the Epipe is displayed. You can narrow the search by using the using the filtered properties shown in the form.

Note — The B-Sites listed are only those that are on the same node as the Epipe site.

iv Choose a B-VPLS and click on OK. The Select Backbone VPLS Site - Site form closes and the Service ID of the chosen B-VPLS appears on the Site (Create) form.

Note — The selection of a B-Site in this step must be repeated for both Epipe sites you create. You must select a B-Site that is on the same node as the Epipe site you are creating.

v In the PBB block, configure the following parameters:

- ISID
- Destination MAC Address or MAC Name

Note 1 — The ISID parameter should be set to the same value for both Epipe sites you create for this service.

Note 2 — To select a previously created Mac Name, click on the Select button and select a MAC Name from the list in the Select MAC Destination MAC Address Alias window. See Procedure 17-48 for more information on how to create a MAC Name.

Note 3 — The Destination MAC Address or MAC Name parameter you set for this Epipe site should be the same as the Source MAC Address of the B-Site on the other node of the Epipe service you are creating.

vi Configure the Force Q Tag Forwarding parameter. This parameter is only displayed if the NE for this site is in chassis mode D.

vii Click on Apply. The Operational Destination MAC Address is updated with the configured Destination MAC Address or MAC Address associated with the selected MAC Name.

14 If you are creating an Epipe service linked to a Backbone VPLS go to step 19.

15 Right-click on Endpoints and choose Create Endpoints. The Endpoint (Create) form opens.

16 Configure the parameters:

- Name
- Description
- Revert Time (second)
- Active Hold Delay (100s of milliseconds)
- Enable T-LDP Standby Signaling

17 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears.

Repeat steps 15 through 17 for each endpoint in the VLL service.

18 Click on the Apply button.

19 Perform one of the following:

a Create an L2 access interface for the VLL terminating sites. Perform Procedure 67-11.

Note — If you are configuring access dual-homing with local switching over PBB tunnels, you must configure two L2 access interfaces. The L2 access interfaces must be on LAGs that participate in the MC LAG.

b Create a spoke SDP binding for the site. Go to step 22.

c Complete site creation. Go to step 42.

20 Click on the Components tab button.

21 If you are creating an Epipe service linked to a Backbone VPLS go to step 42.

22 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

23 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

24 Configure the parameters:

- Auto-Assign ID
- VC ID
- VC Type
- VLAN VC Tag
- Ingress Label
- Egress Label

25 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Transport Tunnel parameter is enabled, 5620 SAM obeys the following conditions:

- Tunnels that do not meet the bandwidth requirements are never selected.
- When more than one tunnel meets the bandwidth requirements, the tunnel with the most available bandwidth is selected.
- When two tunnels meets the bandwidth requirements and have the same available bandwidth, the tunnel with the fewest SDP bindings on it is selected.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

Note — 5620 SAM will block the manual selection of a tunnel with insufficient bandwidth if the following condition is set in the nms-server.xml file:

<vll-CAC enforceTunnelBandwidth="true"/>

The condition is false by default. If it is left as false, 5620 SAM will not block the manual selection of a tunnel with insufficient bandwidth, but the State Cause flag "Insufficient Bandwidth To Allocate To SDP Binding" will be raised.

Refer to Chapter 5 for related notes on modifying the nms-server.xml file. It is recommended that you contact your Alcatel-Lucent technical support representative before modifying this file, since this action can have serious consequences.

26 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

27 When you set the Precedence parameter to 0, you can configure a secondary SAP on an ATM interface, MC-APS, or APS for HSPDA offload fallback.

28 Configure the parameters:

- Enable Hash Label
- Force VLAN VC Forwarding
- SDP Admin Bandwidth (kbps)

29 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth (kbps) parameter in step 28.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

30 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

31 Choose an Application Profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of Application Profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding - VLL service form displays only local profiles on the NE.

32 Click on the States tab button.

33 Configure the Administrative State parameter.

34 Click on the Pseudowire OAM tab button.

35 Configure the Control Word parameter.

36 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the egress ACL filter information displayed.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - Spoke SDP Binding form opens.

vii Choose an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - Spoke SDP Binding form opens.

ix Choose an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the IPv6 egress ACL filter information displayed.

37 Assign an accounting policy to the SDP binding, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Choose an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the accounting policy information displayed.

38 Associate a MEP to the spoke SDP binding, if required.

i Click on the MEPs tab button.

ii Click on the Add button. The MEP (Create) form opens on the General tab.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step x.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The MEP (Create) form closes.

39 Click on the OK button. The Spoke SDP Binding form closes and a dialog box appears.

40 Click on the OK button. The Site (Create) form reappears with the new spoke SDP binding information displayed in the service components tree.

A VLL with spoke switching requires that there is a switching site and two or more terminating sites. Repeat steps 22 through 40 to define the sites required for your VLL configuration.

41 To configure bandwidth for the service if required, click on the Bandwidth tab and proceed as follows:

Note — The Bandwidth tab is only available if service CAC is configured; see chapter 5 for information about enabling and disabling service CAC.

i For each CoS, enter the value for the Reserved Bandwidth, as required.

ii Click on the General tab to determine the CAC status.

If the Verify CAC button is enabled, the CAC has not been verified. The Probable Cause and CAC Status fields provide details.

The CAC Status field describes the current CAC status of the service. CAC statuses are as follows.

- CAC Verified indicates that all tunnels have sufficient bandwidth to admit service and that requested bandwidth for the service is booked on the appropriate physical links.
- CAC Failed indicates that the attempt made to admit service into the network was unsuccessful. The most likely cause for this is insufficient bandwidth. See the Probable Cause field for more specific information.
- BW Defined, No CAC Request indicates that the required bandwidth is defined on the service; however, a CAC request has not occurred.
- CAC To be Verified indicates that a tunnel has been configured on the service either manually or through the CLI; however, the required bandwidth has not been verified in the network.

The Probable Cause field describes possible reasons for the current CAC state. Probable causes are as follows.

- No Candidate Tunnels Found indicates that the autobind tunnel function was found, but no suitable tunnels were found.
- Different PBB Tunnels Applied to Service indicates that two or more different PBB tunnels are configured on this service.
- Not Enough Bandwidth on any Candidate Tunnels indicates that one or more candidate tunnels were found, but the available bandwidth was insufficient to admit the service.
- Automatic PBB Tunnel Selection Failed indicates that a suitable PBB tunnel was found, but there were errors when attempting to assign the tunnel to the service. A dialog box will provide more details.
- Site Missing Tunnel indicates that at least one selected site is not configured with a PBB tunnel.
- All PBB Tunnels have not been Verified indicates that all sites within the service have a tunnel configured, but the available bandwidth has not been booked or verified in the network.

iii To manually verify the CAC, click on the Verify CAC button if it is enabled. The 5620 SAM will attempt to find the most appropriate PBB tunnel for the service-based on available bandwidth, and to automatically bind the tunnel to the service if one has not already been assigned.

42 Click on the OK button. The Site (Create) form closes and a dialog box appears.

43 Click on the OK button. The VLL Epipe (Create) form reappears with the new information displayed in the service components tree.

44 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 6 to 43.

b Complete service creation. Go to step 45.

45 Click on the OK button. The VLL Epipe (Create) form closes.

You can use the topology maps to view the service. See chapter 4 for more information about service topology maps.

Procedure 67-2 To create a VLL Epipe service on an 7210 SAS-E or 7210 SAS-M

1 Choose Create→Service→VLL→Epipe from the 5620 SAM main menu. The VLL Epipe (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - VLL Epipe form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - VLL Epipe form closes and the VLL Epipe (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Administrative State
- OLC State

You can configure the Service ID parameter when the Auto-Assign ID parameter is disabled.

You can configure the Default VC ID parameter when the Inherit Service ID Value parameter is disabled.

You can configure the OLC State parameter after you click on the Apply button.

5 Click on the Components tab button.

6 Right-click on VLL Epipe and choose Create Site. The Select Network Elements - VLL Epipe form opens with a list of available sites.

7 Choose a 7210 SAS site and click on the OK button. The Site (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Name
- Description
- Administrative State
- SAP Type
- Monitor Access Interface Operational State
- Customer VID

9 Click On the OK button. A dialog box appears.

10 Click on the OK button.

11 To create a non-7210 SAS terminating site, right-click on VLL Epipe and choose Create Site. The Select Network Elements - VLL Epipe form opens with a list of available sites. The terminating site must be physically connected to the 7210 SAS by a port or LAG.

Note — The non-7210 SAS terminating sites typically are a 7450 ESS, 7750 SR, or 7710 SR.

12 Choose a terminating site and click on the OK button. The Site (Create) form opens with the General tab displayed.

13 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type

You can only configure the VLL Site Type parameter when the terminating site is a 7450 ESS, 7710 SR, or 7750 SR.

Note — The site must be exclusively terminating, when physically connected to the 7210 SAS.

14 Create an Uplink SAP on the port or lag of the 7210 SAS, which is physically connected to the port or lag of the terminating site.

a Right-click on Access Interfaces below the site and choose Create L2 Access Interface. The L2 Access Interface (Create) form opens with the General tab displayed.

b Configure the parameters:

- Description
- Administrative State

Note — If the 7210 SAS-E sites are connected in a ring network, you must configure an Uplink SAP between each 7210 SAS-E site.

15 Click on the Port tab button.

16 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

17 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

18 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value

19 Create an L2 access interface, on the 7210 SAS and the terminating site.

20 Click on the OK button. A dialog box appears.

21 Click on the Yes button.

22 Close the form.

Procedure 67-3 To create a VLL Epipe service on the 9500 MPR (ANSI only)

1 Choose Create→Service→9500 VLL→Epipe from the 5620 SAM main menu. The Epipe Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the Epipe service. The Select Customer - Epipe Service form opens.

3 Choose the Default Customer as the customer for the Epipe service and click on the OK button. The Select Customer - Epipe Service form closes and the Epipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Specify VLAN Path

The Service ID parameter is enabled when the Auto-Assign ID parameter is disabled.

The OLC State parameter is configurable after you click on the Apply button.

5 Click on the Select button to choose a VLAN path to associate with the Epipe service. The Select VLAN Path - Epipe Service form opens.

6 Choose a VLAN path to use for the service and click on the OK button. The Select VLAN Path - Epipe Service form closes and the Epipe Service (Create) form reappears with the VLAN path information displayed on the General tab.

7 Configure the parameters:

- Auto-Assign ID
- VLAN ID

The VLAN ID parameter is enabled when the Auto-Assign ID parameter is disabled.

Note — The CEM to Eth Service Class is set automatically and is read-only.

8 Configure the parameter:

- Clock Source

9 Click on the Components tab button.

10 Right-click on an Epipe Site and choose Properties. The Epipe Site (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Name
- Description

12 Click on the Components tab button.

13 Right-click on the Access Interfaces and choose Create L2 Access Interface. The L2 Access Interface (Create) form opens with the General tab displayed.

14 Configure the parameters:

- Name
- Auto-Assign ID
- Mac Address
- Monitor Access Interface Operational State

15 Click on the Port tab button.

16 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists Ethernet ports in access mode.

17 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

18 Click on the OK button. A dialog box appears.

19 Click on the OK button. The L2 Access Interface (Create) form closes, and the Epipe Site (Create) form reappears with the new interface information displayed in the service components tree.

20 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 10 to 21.

b Complete service creation. Go to step 22 .

21 Click on the OK button. The VLL Epipe (Create) form closes.

Use the service topology maps to view the service. See chapter 4 for more information about service topology maps.

22 Click on the OK button. The VLL Epipe (Create) form closes.

Use the service topology maps to view the service. See chapter 4 for more information about service topology maps.

Note — In case of a service creation failure and/or generated NE inconsistencies, see Procedure 34-10.

Procedure 67-4 To create a VLL Apipe service using configuration forms

VLL Apipe services are configurable only on the 7450 ESS in mixed mode, 7750 SR and 7710 SR.

1 Choose Create→Service→VLL→Apipe from the 5620 SAM main menu. The VLL Apipe (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - VLL Apipe form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - VLL Apipe form closes and the VLL Apipe (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Inherit Service ID Value
- Default VC ID
- Service Name
- Description
- Service Tier
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
- Transport Type
- OLC State

The Service ID parameter is enabled when the Auto-Assign ID parameter is disabled.

The Default VC ID parameter is enabled when the Inherit Service ID Value parameter is disabled.

The Profile Name and Transport Type parameters are only displayed when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled. The Transport Type parameter is only configurable if the Profile Name parameter is left blank.

5 Perform one of the following:

a Create a site for the VLL. Go to step 6.

b Complete VLL creation if sites and interfaces are to be created later. Go to step 35.

6 Click on the Components tab button.

7 Right-click on VLL Apipe and choose Create Site. The Select Network Elements - VLL Apipe form opens with a list of available sites.

8 Choose a site and click on the OK button. The Site (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type
- Interworking Type

The VLL Site Type parameter is configurable only on the 7450 ESS and 7750 SR.

10 Click on the Components tab button.

11 Perform one of the following:

a Create endpoints for a redundant VLL. Go to step 12.

Note — Redundant VLL Apipe services are configurable on the 7450 ESS, 7705 SAR, 7710 SR, and 7750 SR.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 67-11.

c Create a spoke SDP binding for the site. Go to step 17.

d Complete site creation. Go to step 36.

12 Right-click on Endpoints and choose Create Endpoint. The Endpoint (Create) form opens.

13 Configure the parameters:

- Name
- Description
- Revert Time (second)
- Active Hold Delay (100s of milliseconds)

14 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears.

Repeat steps 12 through 14 for each endpoint in the VLL service.

15 Click on the Apply button.

16 Perform one of the following:

a Create an L2 access interface for the VLL terminating sites. Perform Procedure 67-11.

b Create a spoke SDP binding for the site. Go to step 17.

c Complete site creation. Go to step 36.

17 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding form opens with the General tab displayed.

18 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

19 Configure the parameters:

- Auto-Assign ID
- VC ID
- Ingress Label
- Egress Label
- SDP Admin Bandwidth (kbps)

20 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Transport Tunnel parameter is enabled, 5620 SAM obeys the following conditions:

- Tunnels that do not meet the bandwidth requirements are never selected.
- When more than one tunnel meets the bandwidth requirements, the tunnel with the most available bandwidth is selected.
- When two tunnels meets the bandwidth requirements and have the same available bandwidth, the tunnel with the fewest SDP bindings on it is selected.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

Note — 5620 SAM will block the manual selection of a tunnel with insufficient bandwidth if the following condition is set in the nms-server.xml file:

<vll-CAC enforceTunnelBandwidth="true"/>

The condition is false by default. If it is left as false, 5620 SAM will not block the manual selection of a tunnel with insufficient bandwidth, but the State Cause flag "Insufficient Bandwidth To Allocate To SDP Binding" will be raised.

Refer to Chapter 5 for related notes on modifying the nms-server.xml file. It is recommended that you contact your Alcatel-Lucent technical support representative before modifying this file, since this action can have serious consequences.

21 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

22 When you set the Precedence parameter to 0, you can configure a secondary SAP on an ATM interface, MC-APS, or APS for HSPDA offload fallback.

23 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth (kbps) parameter in step 19.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

24 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

25 Choose an Application Profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of Application Profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding - VLL service form displays only local profiles on the NE.

26 Click on the States tab button.

27 Configure the Administrative State parameter.

28 Click on the Pseudowire OAM tab button.

29 Configure the Control Word parameter.

If you set the VC Type parameter to ATM-SDU in step 4, you must set the Control Word parameter to Preferred.

30 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

31 Click on the OK button. The Site (Create) form reappears with the new spoke SDP binding information displayed in the service components tree.

32 Click on the OK button. The Site (Create) form closes and a dialog box appears.

33 Click on the OK button. The VLL Apipe (Create) form reappears with the new information displayed in the service components tree.

34 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 6 to 33.

b Complete service creation. Go to step 35.

35 Click on the OK button. The VLL Apipe (Create) form closes.

You use the service topology maps to view the service. See chapter 4 for more information about service topology maps.

36 If required, modify the SDP binding parameters for ATM cell concatenation.

i Open and modify the Apipe configuration form, as described in Procedure 67-14.

ii Click on the Spoke SDP Binding tab.

iii Choose a SDP binding from the list and click on the Properties button.

iv Click on the ATM tab.

v Configure the parameters:

- Aal-5 Frame Aware
- Admin Concat Limit
- Max Concat Delay
- Clp Change

vi Save the changes and close the Apipe configuration form.

Procedure 67-5 To create a 9500 MPR Apipe service (ETSI only)

1 Choose Create→Service→9500 VLL→Apipe from the 5620 SAM main menu. The Apipe Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the Apipe service. The Select Customer - Apipe Service form opens.

3 Choose the Default Customer as the customer for the Apipe service and click on the OK button. The Select Customer - Apipe Service form closes and the Apipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Specify VLAN Path

The Service ID parameter is enabled when the Auto-Assign ID parameter is disabled.

5 Click on the Select button to choose a VLAN path to associate with the Apipe service. The Select VLAN Path - Apipe Service form opens.

6 Choose a VLAN path to use for the service and click on the OK button. The Select VLAN Path - Apipe Service form closes and the Apipe Service (Create) form reappears with the VLAN path information displayed on the General tab.

Note — If no VLAN path exists, see Procedure 66-3 in Chapter 66 for more information about how to create VLAN paths.

7 Configure the parameters:

- VLAN ID
- Auto-Assign ID
- Service Class
- PW Label
- Auto-Assign ID
- VC Type

The VLAN ID and PW Label parameters are enabled when the Auto-Assign ID parameters are disabled.

8 If you specified the ATM to Eth option in step 7, configure the MAC Address parameter.

9 Click on the Components tab button.

10 Right-click on an Apipe Site and choose Properties. The Apipe Site (Create) form opens with the General tab displayed.

11 Configure the parameters:

- Name
- Description

12 Click on the Components tab button.

13 Right-click on the Access Interfaces and choose Create L2 Access Interface. The L2 Access Interface (Create) form opens with the General tab displayed.

14 Configure the parameters:

- Name
- Description

15 Click on the Port tab button.

16 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

17 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

Note 1 — If ports on a card slot of the 2+2 x Ethernet (EAS) card are used to create the Apipe service, first configure the Type parameter on the card slot. See Procedure 17-64 for more information on configuring this parameter.

Note 2 — If MPT-MC or MPT-HC ports are being used as network ports on the 2+2 x Ethernet (EAS) card, then the peer MAC Address must be specified for the L2 Access Interface.

18 Do one of the following.

a If you selected a value of VCC for the VC Type parameter, go to step 19.

b If you selected a value of VPC for the VC Type parameter, go to step. 21.

19 Configure the parameters:

- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)

20 Go to step 22.

21 Configure the parameters:

- Outer Encapsulation Value (VPI)
- Outer Encapsulation Value (VPI)

22 Click on the ATM tab button.

23 Click on the Select button to choose an Ingress ATM Policy. The Select Ingress ATM Policy - ATM Configuration form opens.

24 Use the configurable filter and Search button to choose a policy, and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes, and the L2 Access Interface (Create) form displays the policy information.

25 Click on the Select button to choose an Egress ATM Policy. The Select Egress ATM Policy - ATM Configuration form opens.

26 Use the configurable filter and Search button to choose a policy, and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes, and the L2 Access Interface (Create) form displays the policy information.

27 Click on the OK button. A dialog box appears.

28 Click on the OK button. The L2 Access Interface (Create) form closes, and the Apipe Site (Create) form reappears with the new interface information displayed in the service components tree.

29 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 10 to 22.

b Complete service creation. Go to step 30.

30 Click on the OK button. The VLL Apipe (Create) form closes.

Use the service topology maps to view the service. See chapter 4 for more information about service topology maps.

Note — In case of a service creation failure and/or generated NE inconsistencies, see Procedure 34-10.

Procedure 67-6 To create a VLL Fpipe service using configuration forms

VLL Fpipe services are configurable only on the 7450 ESS in mixed mode, 7750 SR and 7710 SR.

1 Choose Create→Service→VLL→Fpipe from the 5620 SAM main menu. The VLL Fpipe (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - VLL Fpipe form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - VLL Fpipe form closes and the VLL Fpipe (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Inherit Service ID Value
- Default VC ID
- Service Name
- Description
- Service Tier
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
- Transport Type
- OLC State

The Service ID parameter is enabled when the Auto-Assign ID parameter is disabled.

The Default VC ID parameter is enabled when the Inherit Service ID Value parameter is disabled.

The Profile Name and Transport Type parameters are only displayed when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled. The Transport Type parameter is only configurable if the Profile Name parameter is left blank.

The OLC State parameter is configurable after you click on the Apply button.

5 Perform one of the following:

a Create a site for the VLL. Go to step 6.

b Complete VLL creation if sites and interfaces are to be created later. Go to step 33.

6 Click on the Components tab button.

7 Right-click on VLL Fpipe and choose Create Site. The Select Network Elements - VLL Fpipe form opens with a list of available sites.

8 Choose a site and click on the OK button. The Site (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type

The VLL Site Type parameter is configurable only on the 7450 ESS and 7750 SR.

10 Click on the Components tab button.

11 Perform one of the following:

a Create endpoints for a redundant VLL. Go to step 12.

Note — Redundant VLL Fpipe services are configurable on the 7450 ESS, 7750 SR, and 7710 SR.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 67-11.

c Create a spoke SDP binding for the site. Go to step 17.

d Complete site creation. Go to step 35.

12 Right-click on Endpoints and choose Create Endpoint. The Endpoint (Create) form opens.

13 Configure the parameters:

- Name
- Description
- Revert Time (second)
- Active Hold Delay (100s of milliseconds)

14 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears.

Repeat steps 12 through 14 for each endpoint in the VLL service.

15 Click on the Apply button.

16 Perform one of the following:

a Create an L2 access interface for the VLL terminating sites. Perform Procedure 67-11.

b Create a spoke SDP binding for the site. Go to step 17.

c Complete site creation. Go to step 35.

17 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding form opens with the General tab displayed.

18 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

19 Configure the parameters:

- Auto-Assign ID
- VC ID
- Ingress Label
- Egress Label

20 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Transport Tunnel parameter is enabled, 5620 SAM obeys the following conditions:

- Tunnels that do not meet the bandwidth requirements are never selected.
- When more than one tunnel meets the bandwidth requirements, the tunnel with the most available bandwidth is selected.
- When two tunnels meets the bandwidth requirements and have the same available bandwidth, the tunnel with the fewest SDP bindings on it is selected.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Choose a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

Note — 5620 SAM will block the manual selection of a tunnel with insufficient bandwidth if the following condition is set in the nms-server.xml file:

<vll-CAC enforceTunnelBandwidth="true"/>

The condition is false by default. If it is left as false, 5620 SAM will not block the manual selection of a tunnel with insufficient bandwidth, but the State Cause flag "Insufficient Bandwidth To Allocate To SDP Binding" will be raised.

Refer to Chapter 5 for related notes on modifying the nms-server.xml file. It is recommended that you contact your Alcatel-Lucent technical support representative before modifying this file, since this action can have serious consequences.

21 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

22 Configure the parameters:

- Enable Hash Label
- SDP Admin Bandwidth (kbps)

23 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth (kbps) parameter in step 22.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

24 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

25 Click on the States tab button.

26 Configure the Administrative State parameter.

27 Click on the Pseudowire OAM tab button.

28 Configure the Control Word parameter.

If you set the VC Type parameter to FR-DLCI in step 4, you must set the Control Word parameter to Preferred.

29 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the egress ACL filter information displayed.

30 Click on the OK button. The Spoke SDP Binding form closes and a dialog box appears.

31 Click on the OK button. The Site (Create) form reappears with the new information displayed in the service components tree.

32 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 7 to 31.

b Complete service creation. Go to step 33.

33 Click on the OK button. A dialog box appears.

34 Click on the OK button. The VLL Fpipe (Create) form reappears.

35 Click on the OK button. The VLL Fpipe (Create) form closes.

You use the service topology maps to view the service. See chapter 4 for more information about service topology maps.

Procedure 67-7 To create a VLL Ipipe service using configuration forms

1 Choose Create→Service→VLL→Ipipe from the 5620 SAM main menu. The Ipipe Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - Ipipe Service form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - Ipipe Service form closes and the Ipipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Inherit Service ID Value
- Default VC ID
- Service Name
- Description
- Service Tier
- Administrative State
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
- Transport Type
- Use Bandwidth-Reserved Paths
- OLC State

The Service ID parameter is enabled when the Auto-Assign ID parameter is disabled.

The Default VC ID parameter is enabled when the Inherit Service ID Value parameter is disabled.

The Profile Name and Transport Type parameters are only displayed when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled. The Transport Type parameter is only configurable if the Profile Name parameter is left blank.

The OLC State parameter is configurable after you click on the Apply button.

5 Perform one of the following:

a Create a site for the VLL. Go to step 6.

b Complete VLL creation if sites and interfaces are to be created later. Go to step 39.

6 Click on the Components tab button.

7 Right-click on Ipipe Service and choose Create Ipipe Site. The Select Network Elements - Ipipe Service form opens with a list of available sites.

8 Choose a site and click on the OK button. The Ipipe Site (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type
- Enable CE IP Address Discovery
- Enable IPv6
- Stack Capability Signaling

The VLL Site Type parameter is configurable only on the 7450 ESS and 7750 SR.

The Enable CE IP Address Discovery parameter is configurable only for VLL terminating sites.

The Enable IPv6 parameter is configurable only when the Enable CE IP Address Discovery parameter is enabled.

Note — The IPv6 capability is only supported on the 7450 ESS in mixed mode (chassis mode D and above), 7710 SR (chassis mode C and above), and 7750 SR (chassis mode C and above).

The Stack Capability Signaling parameter is configurable only when the Enable IPv6 parameter and the Enable CE IP Address Discovery parameters are enabled.

10 Click on the Components tab button.

11 Perform one of the following:

a Create endpoints for a redundant VLL. Go to step 12.

Note — Redundant VLL Ipipe services are configurable only on the 7705 SAR, 7450 ESS, 7710 SR, and 7750 SR.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 67-11.

c Create a spoke SDP binding for the site. Go to step 18.

d Complete site creation. Go to step 35.

12 Right-click on Endpoints and choose Create Endpoint. The Endpoint (Create) form opens.

13 Configure the parameters:

- Name
- Description
- Revert Time (second)
- Active Hold Delay (100s of milliseconds)
- Enable T-LDP Standby Signaling

14 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears.

15 Repeat steps 12 to 14 for each endpoint in the VLL service.

16 Click on the Apply button.

17 Perform one of the following:

a Create an L2 access interface for the VLL terminating sites. Perform Procedure 67-11.

b Create a spoke SDP binding for the site. Go to step 18.

c Complete site creation. Go to step 35.

18 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

19 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

20 Configure the parameters:

- Auto-Assign ID
- VC ID
- VC Type
- Ingress Label
- Egress Label

21 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Transport Tunnel parameter is enabled, 5620 SAM obeys the following conditions:

- Tunnels that do not meet the bandwidth requirements are never selected.
- When more than one tunnel meets the bandwidth requirements, the tunnel with the most available bandwidth is selected.
- When two tunnels meets the bandwidth requirements and have the same available bandwidth, the tunnel with the fewest SDP bindings on it is selected.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Mesh SDP Binding form opens.

ii Choose a service tunnel for the mesh SDP binding and click on the OK button. The Select Tunnel - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the service tunnel identifier.

Note — 5620 SAM will block the manual selection of a tunnel with insufficient bandwidth if the following condition is set in the nms-server.xml file:

<vll-CAC enforceTunnelBandwidth="true"/>

The condition is false by default. If it is left as false, 5620 SAM will not block the manual selection of a tunnel with insufficient bandwidth, but the State Cause flag "Insufficient Bandwidth To Allocate To SDP Binding" will be raised.

Refer to Chapter 5 for related notes on modifying the nms-server.xml file. It is recommended that you contact your Alcatel-Lucent technical support representative before modifying this file, since this action can have serious consequences.

22 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

23 Configure the parameters:

- Enable Hash Label
- SDP Admin Bandwidth (kbps)

24 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required:

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameters.

Note — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth (kbps) parameter in step 23.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Choose a service tunnel for the mesh SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

25 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

26 Choose an Application Profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of Application Profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding service form displays only local profiles on the NE.

27 Click on the States tab button.

28 Configure the Administrative State parameter.

29 Click on the Pseudowire OAM tab button.

30 Configure the Control Word parameter.

31 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the egress ACL filter information displayed.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - Spoke SDP Binding form opens.

vii Choose an IPv6 ingress filter and click on the OK button. The Select IPv6 Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - Spoke SDP Binding form opens.

ix Choose an IPv6 egress filter and click on the OK button. The Select IPv6 Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding form reappears with the IPv6 egress ACL filter information displayed.

32 Click on the Ipipe tab button.

33 Configure the Peer CE IP Address parameter.

34 Click on the OK button. The Spoke SDP Binding form closes and a dialog box appears.

35 Click on the OK button. The Site (Create) form reappears with the new spoke SDP binding information displayed in the service components tree.

36 Click on the OK button. The Site (Create) form closes and a dialog box appears.

37 Click on the OK button. The VLL Ipipe (Create) form reappears with the new information displayed in the service components tree.

38 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 6 to 37.

b Complete service creation. Go to step 39.

39 Click on the OK button. The VLL Ipipe (Create) form closes.

You use the service topology maps to view the service. See chapter 4 for more information about service topology maps.

Procedure 67-8 To create a VLL Cpipe service using configuration forms

VLL Cpipe services are configurable only on the 7710 SR, 7750 SR, 7705 SAR, and 7210 SAS-M. Consider the following when creating a VLL Cpipe:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

1 Choose Create→Service→VLL→Cpipe from the 5620 SAM main menu. The VLL Cpipe (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VLL service. The Select Customer - VLL Cpipe form opens.

3 Choose a customer for the VLL service and click on the OK button. The Select Customer - VLL Cpipe form closes and the VLL Cpipe (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Inherit Service ID Value
- Default VC ID
- Service Name
- Description
- Service Tier
- Administrative State
- VC Type
- Automatic SDP Binding/PBB Tunnel Creation
- Profile Name
- Transport Type

The Service ID parameter is enabled when the Auto-Assign ID parameter is disabled.

The Default VC ID parameter is enabled when the Inherit Service ID Value parameter is disabled.

The Profile Name and Transport Type parameters are only displayed when the Automatic SDP Binding/PBB Tunnel Creation parameter is enabled. The Transport Type parameter is only configurable if the Profile Name parameter is left blank.

The OLC State parameter is configurable after you click on the Apply button.

5 Perform one of the following:

a Create a site for the VLL. Go to step 6.

b Complete VLL creation if sites and interfaces are to be created later. Go to step 33.

6 Click on the Components tab button.

7 Right-click on VLL Cpipe and choose Create Site. The Select Network Elements - VLL Cpipe form opens with a list of available sites.

8 Choose a site and click on the OK button. The Select Network Elements - VLL Cpipe form closes and the Site (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- VLL Site Type

10 Click on the Components tab button.

11 Perform one of the following:

a Create endpoints for a redundant VLL. Go to step 12.

b Create an L2 access interface for the VLL terminating site. Perform Procedure 67-11.

c Create a spoke SDP binding for the site. Go to step 17.

d Complete site creation. Go to step 30.

12 Right-click on Endpoints and choose Create Endpoints. The Endpoint (Create) form opens.

13 Configure the parameters:

- Name
- Description
- Revert Time (second)
- Active Hold Delay (100s of milliseconds)

14 Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears.

Repeat steps 12 to 14 for each endpoint in the VLL service.

15 Click on the Apply button.

16 Perform one of the following:

a Create an L2 access interface for the VLL terminating sites. Perform steps 4 to 27 and steps 32 to 34 of Procedure 67-11.

b Create a spoke SDP binding for the site. Go to step 17.

c Complete site creation. Go to step 31.

17 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding form opens with the General tab displayed.

18 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

19 Configure the parameters:

- Auto-Assign ID
- VC ID
- Ingress Label
- Egress Label
- SDP Admin Bandwidth (kbps)

20 Perform one of the following to specify a transport tunnel for the spoke SDP binding:

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Enable the Auto Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Transport Tunnel parameter is enabled, 5620 SAM obeys the following conditions:

- Tunnels that do not meet the bandwidth requirements are never selected.
- When more than one tunnel meets the bandwidth requirements, the tunnel with the most available bandwidth is selected.
- When two tunnels meets the bandwidth requirements and have the same available bandwidth, the tunnel with the fewest SDP bindings on it is selected.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Mesh SDP Binding form opens.

ii Choose a service tunnel for the mesh SDP binding and click on the OK button. The Select Tunnel - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the service tunnel identifier.

Note — 5620 SAM will block the manual selection of a tunnel with insufficient bandwidth if the following condition is set in the nms-server.xml file:

<vll-CAC enforceTunnelBandwidth="true"/>

The condition is false by default. If it is left as false, 5620 SAM will not block the manual selection of a tunnel with insufficient bandwidth, but the State Cause flag "Insufficient Bandwidth To Allocate To SDP Binding" will be raised.

Refer to Chapter 5 for related notes on modifying the nms-server.xml file. It is recommended that you contact your Alcatel-Lucent technical support representative before modifying this file, since this action can have serious consequences.

21 If you are creating redundant SDP bindings, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to select an endpoint for the transport tunnel. The drop-down menu displays the available endpoints.

ii Configure the parameters:

- Inter-Chassis Backup
- Precedence
- Active State

22 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Allow the 5620 SAM to configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

Note — When the Auto Select Return Transport Tunnel parameter is enabled, 5620 SAM will consider and use a portion of the bandwidth you specified when setting the SDP Admin Bandwidth (kbps) parameter in step 19.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Choose a service tunnel for the mesh SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

23 Click on Select in the Return SDP Binding Endpoint panel to choose a Return Endpoint on the terminating site. Select the required endpoint from the drop-down list that appears.

24 Click on the States tab button.

25 Configure the Administrative State parameter.

26 Click on the Pseudowire OAM tab button.

27 Configure the Control Word parameter.

28 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

29 Click on the OK button. The Site (Create) form reappears with the new spoke SDP binding information displayed in the service components tree.

30 Click on the OK button. The Site (Create) form closes and a dialog box appears.

31 Click on the OK button. The VLL Cpipe (Create) form reappears with the new information displayed in the service components tree.

32 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 6 to 31.

b Complete service creation. Go to step 33.

33 Click on the OK button. The VLL Cpipe (Create) form closes.

Use the service topology maps to view the service. See chapter 4 for more information about service topology maps.

Procedure 67-9 To create a 9500 MPR Cpipe service

1 Choose Create→Service→9500 VLL→Cpipe from the 5620 SAM main menu. The Cpipe Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the Cpipe service. The Select Customer - Cpipe Service form opens.

3 Choose the Default Customer as the customer for the Cpipe service and click on the OK button. The Select Customer - Cpipe Service form closes and the Cpipe Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Administrative State
- Specify VLAN Path

The Service ID parameter is enabled when the Auto-Assign ID parameter is disabled.

The OLC State parameter is configurable after you click on the Apply button.

5 Click on the Select button to choose a VLAN path to associate with the Cpipe service. The Select VLAN Path - Cpipe Service form opens.

6 Choose a VLAN path to use for the service and click on the OK button. The Select VLAN Path - Cpipe Service form closes and the Cpipe Service (Create) form reappears with the VLAN path information displayed on the General tab.

7 Configure the parameters:

- Auto-Assign ID
- VLAN ID

The VLAN ID parameter is enabled when the Auto-Assign ID parameter is disabled.

8 Configure the Service Class parameter.

9 If you specified the CEM to Eth option in step 8, configure the parameters:

- EC ID Tx
- Auto-Assign ID
- EC ID Rx
- Auto-Assign ID
- Clock Source
- Mac Address

The EC ID Tx and EC ID Rx parameters are enabled when the associated Auto-Assign ID parameter is disabled.

10 Click on the Components tab button.

11 Right-click on Cpipe Service and choose Create Cpipe Site. The Select Network Elements - Cpipe Service form opens with a list of available 9500 MPR sites.

12 Choose a site and click on the OK button. The Select Network Elements - Cpipe Service form closes and the Cpipe Site (Create) form opens with the General tab displayed.

13 Configure the parameters:

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

14 Click on the Components tab button.

15 Right-click on the Access Interfaces and choose Create L2 Access Interface. The L2 Access Interface (Create) form opens with the General tab displayed.

16 Configure the Name parameter.

17 Click on the Port tab button.

18 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

19 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

20 Click on the OK button. A dialog box appears.

21 Click on the OK button. The L2 Access Interface (Create) form closes, and the Cpipe Site (Create) form reappears with the new interface information displayed in the service components tree.

22 Repeat steps 15 to 21 if you need to create another L2 access interface for the site in the Cpipe service.

23 Perform one of the following:

a Create an additional site for the VLL service, if required. Repeat steps 10 to 22.

b Complete service creation. Go to step 24.

24 Click on the OK button. The VLL Cpipe (Create) form closes.

Use the service topology maps to view the service. See chapter 4 for more information about service topology maps.

Note — In case of a service creation failure and/or generated NE inconsistencies, see Procedure 34-10.

Procedure 67-10 To fix a failed cross-connection in a 9500 MPR Cpipe

The 5620 SAM may fail to establish one or more cross-connects when you deploy a 9500 MPR Cpipe service, or a cross-connect may fail after the service is created. If you determine that a service is down because of a failed cross-connect, you can try to re-establish the cross-connect.

Note — You must clear deployment errors that are associated with a failed cross-connect before you attempt to re-establish the cross-connect.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria for the service type that you need to find and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a 9500 MPR Cpipe service and click on the Properties button. The Cpipe Service (Edit) form opens with the General tab displayed.

4 Click on the Complete Service button. A dialog box appears.

5 Click on the Yes button.

6 Verify that the cross-connects are operational.

7 Close the Manage Services form.

Procedure 67-11 To create a VLL L2 access interface on a terminating site

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Choose a VLL and click on the Properties button. The VLL *VLL_type* (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Navigate to the Access Interfaces icon for the required site. The path is VLL *VLL_type*→Site→Access Interfaces.

6 Right-click on Access Interfaces below the site and choose Create L2 Access Interface. The L2 Access Interface (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Description
- Administrative State
- ATM Connection Type
- MC Ring Node

The ATM Connection Type parameter is configurable only in a VLL Apipe service that has the VC Type parameter set to ATM-cell.

The MC Ring Node parameter is configurable only in a VLL Epipe service.

8 If you are creating a redundant L2 access interface, configure the endpoint in the Redundancy panel:

i Click on the Select button in the Redundancy panel to choose an endpoint for the L2 access interface. The drop-down menu displays the available endpoints.

ii Choose an endpoint from the drop-down menu.

9 Click on the Select button beside the Application Profile parameter. The Application Profile String: - L2 Access Interface form opens.

Note — The Application Profile parameter is configurable only for an Epipe and Ipipe L2 access interface.

10 Choose a profile from the list and click on the OK button. The Application Profile String: - L2 Access Interface form closes and the L2 Access Interface (Create) form is refreshed with the application profile information.

Note — The Application Profile String: - L2 Access Interface form only displays local profiles that are on the node.

11 Click on the Port tab button.

12 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

13 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

Note — If you choose an ethernet tunnel endpoint, the Port form is refreshed and an Ethernet Tunnel tab is added.

14 Perform one of the following:

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 64-14 for more information about deleting MSAPs.

a If you are creating an Epipe or Ipipe L2 access interface, configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- LLF Enabled

  The LLF Enabled parameter is configurable only for Epipe L2 access interfaces on ports with Null encapsulation.

When the selected port uses Dot1 Q encapsulation, you can enable the Auto-Assign ID check box to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for Dot1 Q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form.

The Inner Encapsulation Value parameter is configurable only when the port encapsulation type is Q in Q.

The Outer Encapsulation Value (VPI) parameter is configurable only when the port encapsulation type is ATM.

If the port you have chosen is an Ethernet Tunnel Endpoint, you will be able to set the Outer Encapsulation Value to 8191. This automatically enables the Ethernet Tunnel Endpoint Control SAP parameter.

The Inner Encapsulation Value (VCI) parameter is configurable only when the port encapsulation type is ATM.

If you are creating an Epipe and use Dot1 Q or Q in Q encapsulation, then you can enable ingress VLAN translation, if required. Configure the parameters:

- Translation
- Translation ID

b If you are creating an Apipe L2 access interface, configure the parameters:

- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- Encapsulation Value (Start VPI)
- Encapsulation Value (End VPI)
- Encapsulation Value (VPI)
- LLF Enabled

The Encapsulation Value (Start VPI) parameter and the Encapsulation Value (End VPI) parameter are configurable only when the VC Type parameter is set to ATM-cell in step 4 of Procedure 67-4 and the ATM Connection Type parameter is set to PVT in step 7 of this procedure.

The Encapsulation Value (VPI) parameter is configurable only when the VC Type parameter is set to ATM-VPC in step 4 of Procedure 67-4.

The LLF Enabled parameter is configurable only for SAPs with “Port” ATM Connection Type and on a clear channel under 4 port OC3-STM1 ASAP MDA.

c If you are creating an Fpipe L2 access interface, configure the Outer Encapsulation Value parameter.

d If you are creating a CPipe L2 access interface, go to step 17.

15 Configure the Ethernet Tunnel Endpoint Control SAP parameter, if required.

Note — Enabling the Ethernet Tunnel Endpoint Control SAP parameter creates the control L2 Access Interface (also known as a Control SAP). It also automatically sets the value of the Outer Encapsulation Value parameter to 8191.

If you are currently creating a same-fate SAP, the Ethernet Tunnel Endpoint Control SAP parameter must not be enabled.

16 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

Note — If a bundle was selected in step 13, only the Scheduling Class parameter is configurable.

The Fragment Interleave parameter is configurable only in a VLL Epipe or Ipipe service.

17 Assign ingress and egress QoS policies to the interface, if required.

a To configure a 7750 SR, 7450 ESS, 7710 SR or 7705 SAR:

Note — Items such as policies, schedulers and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service components tree, choosing Properties, and configuring the parameters on the appropriate tab.

i Click on the QoS tab button.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use Shared Queue
- HSMDA Packet Byte Offset (bytes)

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only on Epipe L2 access interfaces.

The Ingress Match QinQ Dot1P parameter is not configurable if the port encapsulation type is ATM or FR.

The HSMDA Packet Byte Offset (bytes) parameter is configurable only on Epipe and Ipipe L2 access interfaces.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - L2 Access Interface form opens.

iv Choose an ingress QoS policy and click on the OK button. The Select Ingress Policy - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the ingress QoS policy information displayed.

Note — For Epipe and Ipipe VLL L2 access interfaces, if you select an access ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you are configuring for the Epipe or Ipipe L2 access interface has the access ingress queue group with the same name created on it.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - L2 Access Interface form opens.

vi Choose an egress QoS policy and click on the OK button. The Select Egress Policy - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the egress QoS policy information displayed.

Note — For Epipe and Ipipe VLL L2 access interfaces, if you select an access egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you are configuring for the Epipe or Ipipe L2 egress interface has the access egress queue group with the same name created on it.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

vii Click on the Select button in the HSMDA Egress Secondary Shaper panel to choose an HSMDA egress secondary shaper policy. The Select HSMDA Egress Secondary Shaper form opens.

Note — Egress secondary shapers are supported on Epipe and Ipipe L2 access interfaces.

viii Choose a secondary shaper and click on the OK button. The Select HSMDA Egress Secondary Shaper form closes and the L2 Access Interface (Create) form reappears with the egress secondary shaper information displayed.

ix (Epipe service only) Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

x Choose a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

xi (Epipe service only) Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

xii Choose a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

b To configure a 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], or 7210 SAS-X24F2XFP:

i Click on the Select button in the 7210 Specific panel to choose a SAS ingress policy. The Select SAS Ingress Policy - L2 Access Interface form opens.

ii Choose a SAS ingress policy and click on the OK button. The Select SAS Ingress Policy - L2 Access Interface form closes and the information is displayed.

Note — To support H-metering, you must choose a SAS ingress policy with all meter rate modes set to trtcm2.

iii Configure the following parameters in the Aggregate Rate Limit panel:

- Ingress Meter
- Ingress Meter Rate (kbps)
- Ingress Meter Burst

Note 1 — The Ingress Meter parameter is configurable only for the 7210 SAS-X24F2XFP during creation of a SAP. The parameter must be set to true to support H-metering.

Note 2 — For the 7210 SAS-X24F2XFP, the Ingress Meter Rate (kbps) and Ingress Meter Burst parameters can be modified only after a SAP is created.

18 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 22.

Note — The Schedulers tab is configurable only if a port is assigned to the interface earlier in the procedure.

19 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame Base Accounting

Note 1 — The Egress Aggregate Rate Limit (kbps) and Frame Base Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — You cannot specify an egress scheduler when the Egress Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - L2 Access Interface form opens.

iv Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - L2 Access Interface form opens.

vi Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

vii Go to step 22.

b Specify that an aggregation scheduler policy is applied to the interface.

i Set the Aggregation parameter to On.

ii Configure the Frame Base Accounting parameter.

iii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - L2 Access Interface form opens.

iv Choose an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

v Go to step 22.

20 Click on the Aggregation Rate tab button to configure the aggregation rate; otherwise, go to step 22.

Note — The Aggregation Rate tab is configurable only if a port is assigned to the HSMDA SAP.

21 Configure the Aggregate Rate Limit (kbps) parameter in the Ingress Aggregate Rate Limit and Egress Aggregate Rate Limit panels.

22 Assign ingress and egress ACL filters to the interface, if required.

Note 1 — IPv6 ACL filters are not supported on the 7705 SAR.

Note 2 — ACL filters are not supported for CPipe L2 access interfaces.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - L2 Access Interface form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - L2 Access Interface form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the egress ACL filter information displayed.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - L2 Access Interface form opens.

vii Choose an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - L2 Access Interface form opens.

ix Choose an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - L2 Access Interface form closes and the L2 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

23 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab button.

ii Click on the Select button to choose an accounting policy. The Select Accounting Policy - L2 Access Interface form opens.

iii Choose an accounting policy and click on the OK button. The Select Accounting Policy - L2 Access Interface form closes, and the L2 Access Interface (Create) form refreshes with the accounting policy name.

iv Configure the Collect Accounting Statistics parameter.

v If you are configuring statistics collection for a 7210 SAS-E or 7210 SAS-M, go to step vi. Otherwise, go to step 24.

vi Configure the parameters:

- Enable Egress Packets Forwarding
- Ingress Counter Mode

24 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab button.

ii Click on the Select button in the Time Of Day Suite panel. The Select Time Of Day Suite - L2 Access Interface list form opens.

iii Choose a time of day suite and click on the OK button. The Select Time Of Day Suite - L2 Access Interface list form closes, and the L2 Access Interface (Create) form reappears with the time of day suite name.

Note 1 — You cannot assign a ToD suite to a L2 access interface if accounting statistics collection is enabled on the L2 access interface. You must disable the Collect Accounting Statistics parameter in step 23.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics will only be collected if a Time Of Day Suite is applied on the SAP.

25 Configure an ethernet tunnel.

Note — You can only configure an ethernet tunnel if you are creating a same-fate SAP or a control/data SAP.

i Click on the Ethernet Tunnel tab.

ii If you are configuring a fate-sharing Ethernet Tunnel Endpoint SAP (also referred to as same-fate SAP) then go to step iii. Otherwise, go to step 26.

iii Click on the Add button. The Ethernet Tunnel (Create) form opens.

iv Configure the parameters:

- Path ID
- Tag (Outer Encapsulation Value)
- Tag (Inner Encapsulation Value)

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The L2 Access Interface (Create) form refreshes with the Ethernet Tunnel entry.

26 If you need to create an Epipe or Ipipe L2 access interface, specify the queue overrides by clicking on the Override tab button. See chapter 44 for information about queue overrides.

Note — The Override tab contains four sub-tabs: Access Ingress Queue, Access Egress Queue, Access Ingress HSMDA Queue, and Access Egress HSMDA Queue. However, only two of the four are active, depending on the port type that you have chosen for this interface.

If you configured an HSMDA port, then the Access Ingress HSMDA Queue and Access Egress HSMDA Queue sub-tabs are active. If you configured a non-HSMDA port, then the Access Ingress Queue and Access Egress Queue sub-tabs are active.

27 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button. The ANCP Static Map (Create) form opens.

ii Configure the ANCP String parameter.

iii Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

iv Choose an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

v Click on the OK button. The ANCP Static Map form closes.

28 Associate a MEP to an Epipe or Apipe L2 access interface, if required.

i Click on the MEPs tab button.

ii Click on the Add button. The MEP (Create) form opens.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Choose an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step x.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The MEP (Create) form closes.

29 If you are creating an Epipe, Apipe, or Ipipe L2 access interface, specify OAM functionality and assign ingress and egress ATM policies to the interface. Otherwise, go to step 33.

i Click on the ATM tab button.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- ATM OAM Terminate

The ATM OAM Terminate parameter is configurable only on Apipe L2 access interfaces. When the VLL access interface port belongs to a MC-APS channel and the VC Type parameter is set to ATM-SDU, set the ATM OAM Terminate parameter to Up.

The AAL5 Encapsulation parameter is configurable only on Epipe and Ipipe L2 access interfaces.

The ATM OAM Alarm Cell Handling parameter is configurable on Apipe L2 access interfaces only when the VC Type parameter is set to ATM-VCC or ATM-VPC in step 4 of Procedure 67-4. The parameter is configurable on Epipe and Ipipe L2 access interfaces.

The ATM OAM Terminate is configurable on Apipe L2 access interfaces only when the VC Type parameter is set to ATM-SDU or ATM-VCC in step 4 of Procedure 67-4.

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Choose an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes and the L2 Access Interface (Create) form reappears with the ingress ATM policy information displayed.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Choose an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes and the L2 Access Interface (Create) form reappears with the egress ATM policy information displayed.

30 If you are creating an Ipipe L2 access interface, specify Ipipe functionality for the interface. Otherwise, go to step 33.

i Click on the IPIPE tab button.

ii Configure the parameters:

- CE IP Address
- MAC Refresh Interval
- MAC Address
- Use Broadcast MAC Address

The MAC Address parameter, MAC Refresh Interval parameter, and Use Broadcast MAC Address parameters are configurable only when the port encapsulation type is Dot1 Q, Q in Q, or Null.

31 If you are creating an Epipe L2 access interface with CEM encapsulation, specify the CEM functionality for the service. Otherwise, go to step 33.

Note — Consider the following when creating a VLL Epipe L2 access interface with CEM encapsulation:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

i Click on the OK button to close the L2 access interface configuration form. The Site (Create) form reappears.

ii Click on the OK button. The Site (Create) form closes and the VLL Cpipe (Create) form reappears.

iii Click on the Apply button.

iv Expand the Site object on the Components tab. Right-click on the SAP object for the L2 access interface that you are creating and choose Properties from the contextual menu. The L2 Access Interface (Edit) form opens with the General tab displayed.

v Click on the CEM EPipe tab button.

vi Configure the parameters:

- Jitter Buffer (ms)
- Payload Size (octets)
- RTP Header
- Report Alarm
- Local ECID
- Remote ECID
- Remote MAC Address

32 If you are creating a Cpipe L2 access interface, specify the CEM functionality for the service. Otherwise, go to step 33.

Note — Consider the following when creating a VLL Cpipe L2 access interface:

- The Time Slots parameter of the DS0 channel must be configured with at least one time slot.
- Time slots are automatically configured for unstructured E1 and T1 endpoints
- The Clock Source parameter of the DS1 channel must be set to Node-Timed.

i Click on the OK button to close the L2 access interface configuration form. The Site (Create) form reappears.

ii Click on the OK button. The Site (Create) form closes and the VLL Cpipe (Create) form reappears.

iii Click on the Apply button.

iv Expand the Site object on the Components tab. Right-click on the SAP object for the L2 access interface that you are creating and choose Properties from the contextual menu. The L2 Access Interface (Edit) form opens with the General tab displayed.

v Click on the CEM CPipe tab button.

vi Configure the parameters:

- Jitter Buffer (ms)
- Payload Size (octets)
- RTP Header
- Report Alarm

33 Click on the OK button. A dialog box appears.

34 Click on the OK button. The L2 Access Interface (Create) form closes, and the Site (Create) form reappears with the new interface information displayed in the service components tree.

Repeat steps 6 to 34 to create another L2 access interface for the site in the VLL service.

Note 1 — If you are configuring access dual-homing with local switching over PBB tunnels, you must configure two L2 access interfaces. The L2 access interfaces must be on LAGs that participate in the MC LAG. See chapter 40 for information about MC LAGs.

Note 2 — If you are creating the L2 access interface during service creation, return to the appropriate VLL service creation procedure:

- For Epipes, go to step 19 of Procedure 67-1.
- For Apipes, go to step 16 of Procedure 67-4.
- For Fpipes, go to step 16 of Procedure 67-6.
- For Ipipes, go to step 17 of Procedure 67-7.
- For Cpipes, go to step 16 of Procedure 67-8.

Procedure 67-12 To create an HSDPA resiliency configuration

See "HSDPA Offload Resiliency" in section 67.1 for information about HSDPA resiliency.

1 Choose Manage→Redundancy→HSDPA Resiliency from the 5620 SAM main menu. The HSDPA Resiliency Manager form opens.

2 Click on the Create button. The HSDPA Resiliency (Create) form opens.

3 Configure the parameters:

- Description
- Administrative State

4 Click the Select button beside the Name parameter in the Site panel. The Select Site - HSDPA Resiliency form opens. Only sites utilizing a 7705 SAR chassis are displayed.

5 Choose a site and click on the OK button. The Select Site - HSDPA Resiliency form closes and the HSDPA Resiliency (Create) form is displayed with your site choice shown in the Name parameter field.

6 Click the Select button beside the Name parameter in the Primary Service panel. The Select Primary Service - HSDPA Resiliency form opens with a list of services.

Note — The Select Primary Service - HSDPA Resiliency form does not give you the option to create the required Apipe service. See Procedure 67-4 to create the required service before configuring HSDPA Resiliency.

7 Choose a service and click on the OK button. The HSPDA Resiliency (Create) form refreshes with the primary service information.

8 Click the Select button beside the Name parameter in the Secondary Service panel. The Select Secondary Service - HSDPA Resiliency form opens with a list of services.

Note — The Select Secondary Service - HSDPA Resiliency form does not give you the option to create the required Apipe service. See Procedure 67-4 to create the required service before configuring HSDPA Resiliency.

9 Choose a service and click on the OK button. The HSPDA Resiliency (Create) form refreshes with the secondary service information.

10 Click on the OK button. The HSDPA Resiliency (Create) form closes.

11 Perform one of the following:

a Perform Procedure 67-13 to turn up or manually operate an HSDPA resiliency configuration.

b Close the HSDPA Resiliency Manager form.

Procedure 67-13 To activate and manually operate an HSDPA resiliency configuration

See section "HSDPA Offload Resiliency" for a detailed description of this feature.

1 Choose Manage→Redundancy→HSDPA Resiliency from the 5620 SAM main menu. The HSDPA Resiliency Manager form opens.

2 Choose the required HSDPA resiliency configuration from the displayed list and click the Properties button. The HSDPA Resiliency (Edit) form opens with the properties of the configuration displayed on the General tab.

The Active Service field displays whether the Primary or Secondary Service is active. When you initially want to turn up a resiliency configuration, typically Primary is displayed.

3 Set the Administrative State parameter to Disabled. Activity for the resiliency configuration can only be manually switched from this form when this parameter is set to Disabled.

4 Perform one of the following:

a Set the Administrative State parameter to Enabled. Activity automatically switches between the primary and secondary services as required when this parameter is enabled.

b Click on the Turn Up button to manually activate the HSDPA resiliency configuration. Do this if the Administrative State parameter is not enabled.

c If the Primary Service is currently active, you can click on the Force Secondary Service Active button. This manually forces the configuration to the Secondary Service (if up), regardless of state of damping timer. The Active Service field displays Secondary if the switchover is successful.

d If the Secondary Service is currently active, you can click on the Force Primary Service Active button. This manually forces the configuration to the Primary Service (if up), regardless of state of damping timer. The Active Service field displays Primary if the switchover is successful.

e Click on the Shut Down button to de-activate the HSDPA resiliency configuration.

f Click on the Faults tab to view and address alarms related to the configuration.

5 Click on the OK button. The HSDPA Resiliency (Edit) form closes.

6 Close the HSDPA Resiliency Manager form.

Procedure 67-14 To modify a VLL service

Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a VLL service and click on the Properties button. The VLL *Type_of_VLL* (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs list the service elements that can be individually or collectively selected and configured:

Note 1 — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

Note 2 — Some service element do not apply to all VLL services.

- Components tab — displays the various service components in a tree format
- Sites tab — lists the sites that are included in the service
- Endpoints tab — lists the service endpoints
- L2 Access Interfaces tab — lists the L2 access interfaces that are included in the service
- Spoke SDP Bindings tab — displays the spoke SDP bindings that are associated with the service
- VLAN Path Instance - list VLAN path instances associated with a 9500 MPR service
- Template tab — displays the template used to create the service, if applicable.
- Tests tab
- Faults tab — displays the faults associated with the service

Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Modify the parameters for the service as required.

To configure items in the Components tab, select and right-click on the items and choose Properties from the contextual menu.

To configure items on the tabs that contain lists of service elements, select the items and click on the Properties button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The VLL *Type_of_VLL* (Edit) form closes and the Manage Services form reappears.

7 Click on the Close button to close the Manage Services form.

Procedure 67-15 To view the service operational status

The Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a service and click on the Properties button. The VLL *Type_of_VLL* (Edit) form opens.

4 View the Operational State and State Cause indicators. When the Operational State is Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab button to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab button to view the aggregated alarms for the object. The Aggregated Alarms tab is displayed.

8 Close the VLL *Type_of_VLL* (Edit) form.

9 Click on the Close button to close the Manage Services form.

Procedure 67-16 To run an OAM validation test

An OAM validator test suite must be created for the tested entity. See chapter 75 for more information about how to create a validator test suite.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a service and click on the Properties button. The VLL *Type_of_VLL* (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

   i Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form appears.

   ii Configure the filter criteria. A list of OAM validator test suites appears.

   iii Choose an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab button. The Test Suite tab is displayed.

7 Click on the Validation Result tab button.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab button to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise, go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result form.

14 Close the VLL *Type_of_VLL* (Edit) form.

15 Close the Manage Services form.

Procedure 67-17 To view peer status information

You can view peer status faults in the peer PE SAP and service tunnel in the Peer State Cause panel of the Spoke SDP Binding form.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the service and click on the Properties button. The VLL *Type_of_VLL* (Edit) form opens.

4 Click on the Spoke SDP Binding tab button.

5 Choose an entry and click on the Properties button. The Spoke SDP Binding (Edit) form opens.

6 Click on the States tab button.

7 View the peer status information in the Peer State Cause panel. When the service tunnel or peer SAP is down or partially down, a check mark beside the appropriate Peer State Cause indicator identifies the type of associated service fault.

8 Click on the Cancel button to close the Spoke SDP Binding (Edit) form.

Procedure 67-18 To view the service topology

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VLL service and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - *Service Name* map opens.

See chapter 4 for more information about service topology views.

Procedure 67-19 To modify a VLL service using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the component tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a VLL and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains a number of sub-procedures describing the various components that can be created and modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating site components. Go to step 9.
- Creating spoke SDP bindings. Go to step 17.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the option allowing you to create a new site. This may be an Epipe, Cpipe, Ipipe, Apipe, or Fpipe site, depending on what type of VLL service you are modifying.

The Select Network Elements form appears.

5 Choose one or more sites to add to the service and click OK. The Site (Create) form for the new site is displayed. If you selected more than one site, the Site (Multiple Instances) (Create) form for the new sites is displayed.

6 Click on OK. The Site (Create) (or Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

7 If you want to perform detailed configuration of site properties for the new site, right-click the site icon and select Properties from the contextual menu. The Site (Edit) form opens. Refer to Procedures 67-1 through 67-9 for detailed site configuration information for the various types of VLL services.

8 Return to step 3 for a list of other functions you can perform from the topology view or go to step 25 to finish.

Creating site components

9 Right-click on any site icon in the service topology map. A contextual menu is displayed. You can choose to create one of the following:

- Endpoint. Go to step 10.
- L2 Access Interface. Go to step 13.

10 If you choose to create an Endpoint, then the Endpoint (Create) form is displayed.

11 Configure the Name parameter for the endpoint.

Refer to Procedures 67-1 through 67-8 and 67-11 for detailed information on further configuring the endpoint, if required.

12 Click OK. The Endpoint (Create) form closes and the new endpoint is displayed in the topology view.

13 If you choose to create an L2 Access Interface, then the L2 Access Interface (Create) form is displayed.

14 Click on the Port tab and assign a port to the interface.

Refer to Procedures 67-1 through 67-9 and 67-11 for detailed information on further configuring the interface, as required.

15 Click OK. L2 Access Interface (Create) form closes.

16 Return to step 3 for a list of other functions you can perform from the topology view or go to step 25 to finish.

Creating spoke SDP bindings

17 Choose the sites you want to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.

Note — When you create a spoke binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

18 Choose Connect from the contextual menu and choose the Create Spoke SDP Binding option.

The Spoke SDP Binding (Create) form is displayed.

Note 1 — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

Note 2 — You can also create a spoke SDP binding between a site icon and an endpoint icon, or between two endpoint icons in the topology view. Appropriate endpoints must first exist or be created to enable this.

19 Enable the Auto Select Transport Tunnel parameter.

20 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedures 67-1 through 67-8 for more detailed information on creating and configuring spoke SDP bindings for the various types of VLL services, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 30 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

21 Assuming that the spoke SDP binding was successfully created in step 20, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a spoke binding for the return tunnel.

22 Right-click on the second site you selected and choose the Create Spoke SDP Binding ... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

23 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 30 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

24 Return to step 3 for a list of other functions you can perform from the topology view or go to step 25 to finish.

25 Close the Service Topology form.

26 Close the Manage Services form.

Procedure 67-20 To delete a VLL service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Choose a VLL service from the list.

4 Click on the Delete button. A dialog box appears and prompts you to confirm that you understand the implications of deleting the service.

5 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

6 Click on the Close button to close the Manage Services form.

68 — VPLS management

68.1 VPLS management overview

VPLS is a class of virtual private network multipoint L2 service that allows multiple customer sites to be connected in a single bridged domain contained within the service provider-managed IP/MPLS network. Customer sites in the VPLS appear to be on the same LAN, even if the sites are geographically dispersed.

VPLS offers the following advantages:

- Ethernet interfaces on the host access side simplify provisioning.
- All routers in the VPLS are part of the same LAN, which simplifies IP addressing and allows customers to control and simplify their routing strategies.
- VPLS is protocol independent, which means there is no L2 protocol conversion between LAN and WAN technologies.

A VPLS can span a single site or multiple sites. A VPLS that spans a single site is called a local VPLS. In a local VPLS, customer data enters the service through multiple access interfaces on a single PE device. No circuit provisioning is required for the local VPLS.

A VPLS that spans multiple sites is called a distributed VPLS. In a distributed VPLS, customer data enters the service using two or more interfaces on different PE devices. The VPLS is transported by service circuits over an IP/MPLS provider core network carried by service tunnels. Service tunnels are created using GRE or MPLS LSPs.

You can use HVPLS to eliminate the need for a full mesh of virtual circuits between devices in the VPLS. See "HVPLS" in this section for more information.

The 5620 SAM supports end-to-end VPLS configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Pre-configured template. A user that is assigned the template management role can create a service template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

The General tab of the 5620 SAM service management form displays useful information about the operational state of the service and its sites through the Aggregated Operational State and State Cause indicators.

You can run the OAM Validation test suite for the service by clicking on the Validate button. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. In addition, the Validation Result tab on the Tests tab displays detailed information about the OAM test result. OAM validation tests are not supported for HVPLS. See chapter 75 for more information about how to configure OAM validation test suites.

The Aggregated Operational State indicator has four possible values: Up, Down, Partially Down, and Unknown. The value is derived from the operational states of the sites that are part of the service, as follows:

- Up—all sites are operationally up
- Partially Down—at least one site is operationally down
- Down—all sites are operationally down
- Unknown—the service has no provisioned sites

When the Aggregated Service Site Operational State is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator. Alarms can be viewed on the Faults page.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology map views. See chapter 72 for more information about the hierarchical organization of composite services.

Common to all services, such as VPLS, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces and circuits, when the service is configured or modified. The following policies are common to all services:

- QoS policies to define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy Manager and the Access Egress Policy Manager.
- Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies to define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy Manager.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy and HSMDA Scheduler Policy forms.
- Filter policies to control network traffic into or out of an interface or circuit based on IP or MAC matching criteria. Filter policies are configured using the ACL IP Filter Manager and the ACL MAC Filter Manager.
- Accounting policies to count the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy Manager.
- ANCP policies provide status and control information based on port-up and port-down messages and current line rate changes between the edge device and the access node. ANCP policies are configured using the Manage Subscriber Policies form.
- Time of day suites specify time and day restriction policies that are assigned to QoS policies and schedulers, ACL filters, and aggregation schedulers. Time of day suites and time range policies are configured using the Time of Day Suite form and Time Range form, respectively.

See chapter 43 for more information about policies.

Packets that arrive at an edge device are associated with a VPLS based on the access interface on which they arrive. An access interface is uniquely identified using the following parameters:

- physical Ethernet port or POS port and channel
- encapsulation type
- encapsulation identifier (if required)

If there are service issues, the service provider can use OAM tools to troubleshoot service and network transport issues, and ensure problems are handled properly through the physical and logical network. See chapter 35 for more information.

To provide a VPLS over an MPLS infrastructure, the device is configured to provide bridging and replication for each VPLS. The routers that are part of the VPLS are connected by MPLS LSPs. Multiple VPLS can use the same set of service tunnels. Multiple service tunnels can rely on multiple LSPs. The signaling is specified in sets of ingress and egress VC labels for each VPLS.

The following additional features are configured for the VPLS:

- MAC learning for the access ports and tunnels, including filtering based on MAC addresses on a per SAP basis
- MAC learning protection on SAPs to prevent DoS attacks from sourcing
- rate limiting of broadcast, destination unknown, and multicast traffic on a per access port basis
- FIB for each VPLS, including FIB size limits, static MAC addresses, alarms, and discarding unknown locations
- optional support for spanning tree for loop detection
- GSMP for each VPLS
- L2 management interfaces for each VPLS

HVPLS

A hierarchical VPLS is created by enhancing the VPLS core mesh with a spoke SDP binding that is connected to another site in the same VPLS, a site in another VPLS, or a VLL site.

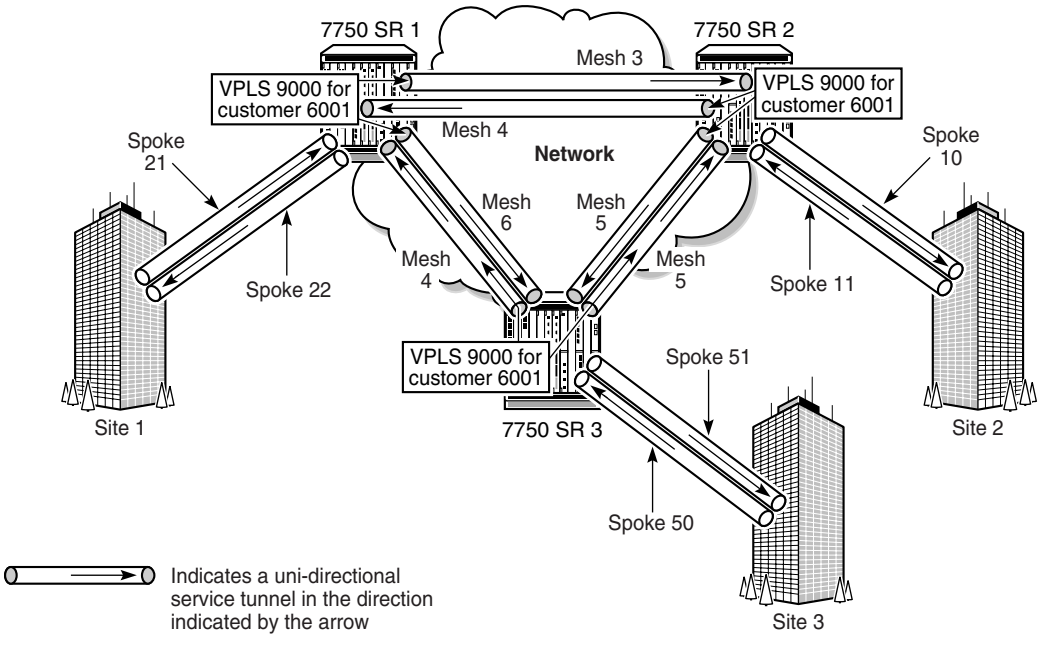
HVPLS offers the following advantages:

- reduces the complexity of mesh configuration
- decreases the amount of signaling of routes between devices

When traffic arrives at an access-spoke circuit, it acts like a bridge port where flooded traffic received on the access spoke is replicated to all other spokes, meshes, or SAPs but it is not transmitted on the port where it is received.

Figure 68-1 shows a sample HVPLS with a mesh and spoke configuration. Spokes 50 and 51 are unidirectional access-spoke circuits bound to service tunnels. The access-spoke circuits exist within the context of a VLL service or VPLS that is interconnected to the original, fully meshed VPLS. Alternatively, the access-spoke circuit can provide interconnectivity to a service site.

Figure 68-1 HVPLS configuration



The 5620 SAM supports the following HVPLS interconnectivity using spoke SDPs:

- VPLS to VPLS
- intra-VPLS
- VPLS to VLL

MVPLS

VPLS topology loops can occur if either of the following is true:

- Two VPLS are connected by redundant spoke SDPs.
- A CE NE is connected to a VPLS with redundant L2 access interfaces.

To remove topology loops, RSTP must be enabled on the redundant spoke SDPs or L2 access interfaces to block some of them from passing traffic. This requires the creation of an MVPLS.

MSTP is an extension of RSTP which allows VLANs to be grouped into spanning tree instances. Each instance has an independent spanning tree topology. MSTP can be run in an MVPLS to provide multiple forwarding paths for data traffic, which allows load balancing and reduces the number of spanning tree instances required to support a large number of VLANs. An MST region comprises a set of interconnected switches that have the same MST configuration. Each region can be configured with up to 16 MST instances. The instance with ID 0 is an internal spanning tree that runs an MST region and sends and receives BPDUs. All other spanning tree instance information is encapsulated within MSTP BPDUs.

An MVPLS is created to run RSTP or MSTP and manage traffic on the associated VPLS. An MVPLS contains sites, spoke SDP bindings, mesh SDP bindings, and L2 access interfaces. The MVPLS spoke SDP bindings and L2 access interfaces are configured to manage the associated VPLS spoke SDP bindings and L2 access interfaces.

In the case of spoke redundancy, the MVPLS runs RSTP on the redundant spoke SDPs and associates the resultant traffic-blocking actions with all VPLS that use the same spoke SDPs.

MVPLS traffic blocking can also be used on the access side to manage redundant L2 access interface connections. A VLAN ID range is specified for each MVPLS L2 access interface which identifies the VC IDs of the managed VPLS L2 access interfaces.

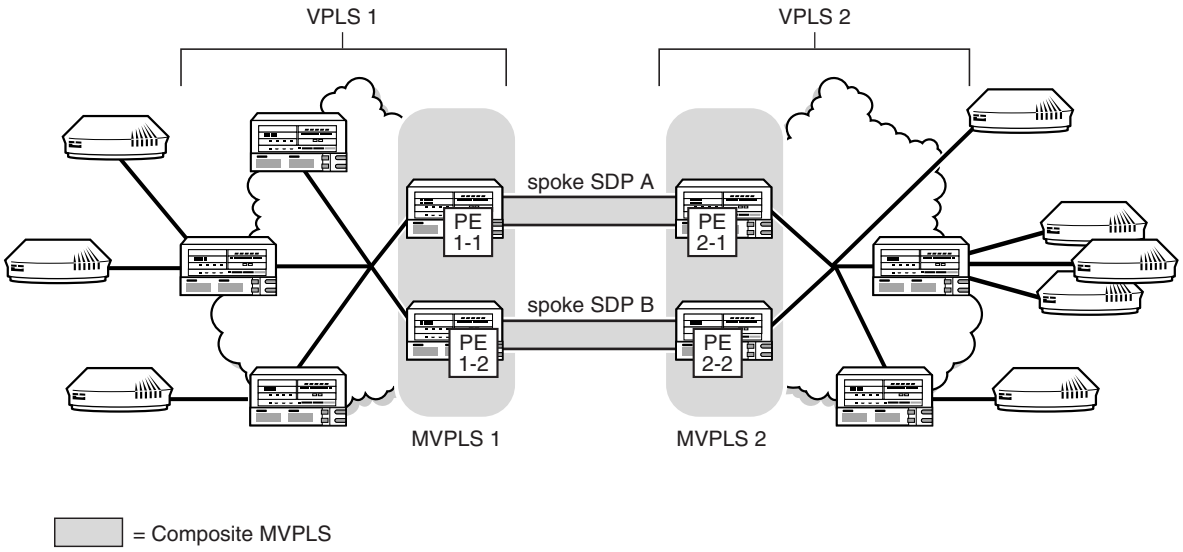
RSTP is enabled by default on an MVPLS. When the Admin state of an MVPLS is down, all managed L2 access interfaces and spoke SDPs in the associated VPLS are disabled. However, if the Admin state of individual L2 access interfaces or spoke SDPs of an MVPLS are down, then the managed VPLS L2 access interfaces or spoke SDPs are not affected by traffic blocking.

A common MVPLS situation occurs when two VPLS are connected by redundant spoke SDPs. If traffic is not blocked on one of the redundant spoke SDPs, then a loop results. To remove the loop, RSTP must be run on the spoke SDPs that form the loop to block one of the redundant spoke SDPs. Blocking is accomplished by creating an MVPLS on each side of the redundant spoke SDPs and creating a composite MVPLS to connect the MVPLS.

Another common MVPLS situation occurs when an access switch with many VLANs is redundantly connected to two other bridges, on which each uplink carries half the VLANs. MSTP allows you to build multiple spanning trees over VLAN trunks and to group and associate the VLANs to spanning tree instances, each with a different port instance cost and port instance priority.

Figure 68-2 shows an example of a composite MVPLS that is composed of MVPLS 1, MVPLS 2, and spoke SDPs.

Figure 68-2 Composite MVPLS



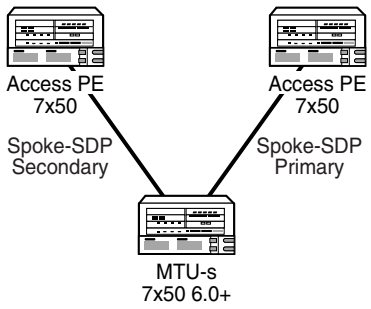
Another scenario occurs when multiple L2 access interfaces from a VPLS are connected to the same customer edge equipment. In this case, a single MVPLS must be created with L2 access interfaces defined to manage the traffic on the associated VPLS redundant L2 access interfaces.

Dual homing for VPLS

A VPLS can be configured for dual homing through the use of redundant spoke SDPs. 5620 SAM handles the redundant spoke SDPs by grouping them together to form an endpoint object. The redundant spoke SDPs provide active and standby pseudowires for the service. This spoke SDP access arrangement allows data flow control and management support without requiring STP, which cannot be enabled on a spoke SDP binding that is under an endpoint. For VPLS, you can associate only spoke SDP bindings with an endpoint, and each endpoint can be associated with a maximum of two spoke SDP bindings.

Figure 68-3 shows a simple dual homing configuration.

Figure 68-3 MTU redundant access to VPLS



VPLS dual homing provides the ability to have an NE deployed as an MTU-s with links to multiple PE NEs without requiring an MVPLS.

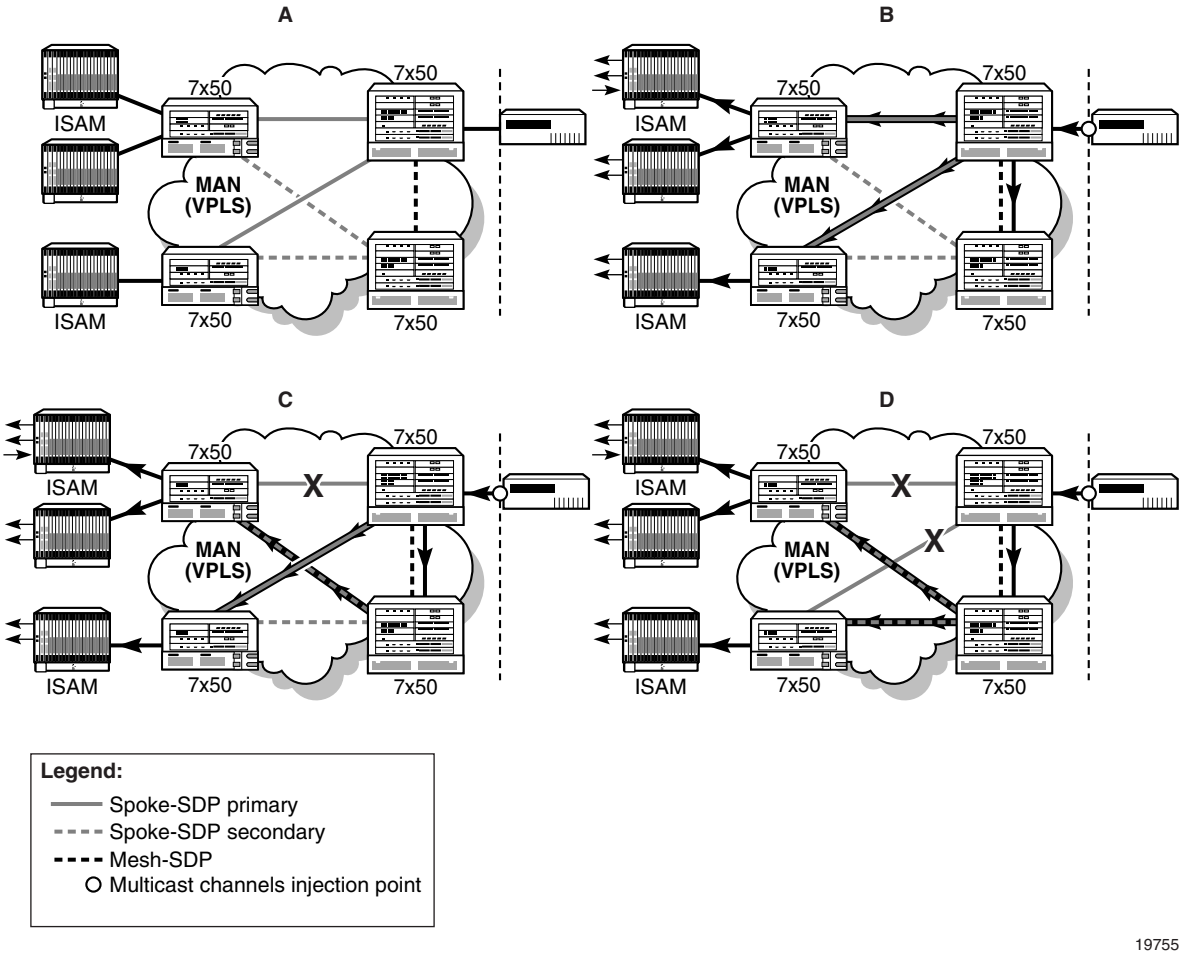
Note 1 — You cannot create a VPLS endpoint on a site that has an active or inactive MC ring SAP. See chapter 42 for more information.

Note 2 — You cannot create an endpoint in an MVPLS.

In this example, the MTU-s has spoke SDPs to two PE devices. One is designated as the primary spoke and the other as the secondary, or standby spoke, based on a precedence value specified for each spoke. The standby spoke is in a blocking state when the primary spoke is available. If the primary spoke becomes unavailable, the MTU-s immediately switches the traffic to the standby spoke. You can configure the service to revert back to the original configuration, after a specified delay, when the primary spoke is again available. Forced manual switchover is also supported.

You can configure a MAC flush to speed the convergence during a switchover. The PE devices that receive the MAC flush remove each MAC address that is associated with the affected VPLS instance and forward the MAC flush to the other PE devices in the VPLS. Figure 68-4 shows a dual-homed VPLS for BTV distribution.

Figure 68-4 BTV distribution in redundant VPLS architecture

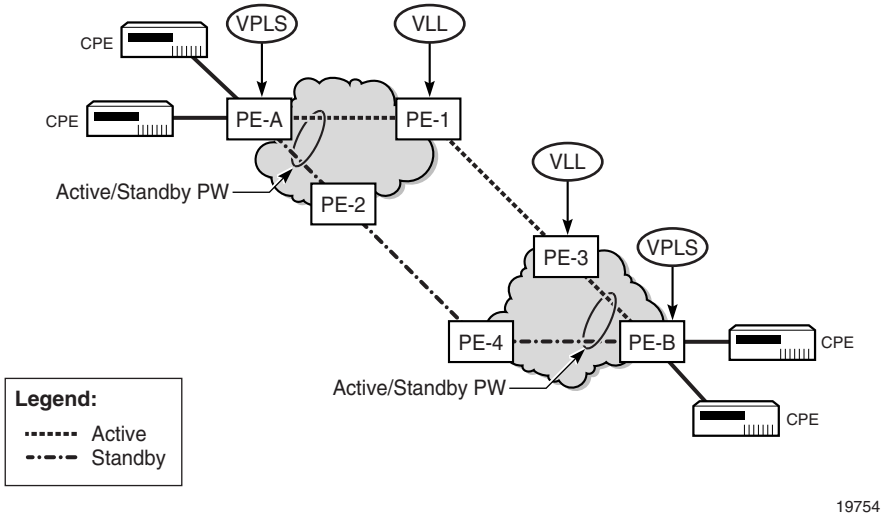


In the nominal operating mode shown in panel A, the edge router (grey icon) has been configured to statically join all multicast channels and inject them into the aggregation network. The access layer 7x50 unit (directly connected to ISAM) is dual-homed into two aggregation layer 7x50s edge routers (larger icons) using primary and secondary spoke SDPs. A mesh SDP interconnects both aggregation nodes. Injected BTV traffic from the edge router is broadcast on the primary spoke SDPs to the connected MTU devices (panel B).

A copy of the channels is also sent on the mesh SDP to the peer aggregation node, which also replicates the traffic to the connected spoke SDPs (aggregation layer nodes are not aware of primary/secondary spoke selection done by the MTU layer devices). The MTUs only receive traffic from the primary spoke SDP. Traffic received on the secondary spoke SDP is blocked. In the event of a link failure (panel C) or MDA failure (panel D), the MTU switches over to the secondary spoke SDP and immediately start receiving traffic from it instead of the primary spoke SDP.

Composite services also support VPLS with redundant spoke SDP bindings to VLL services. Figure 68-5 shows a VPLS and VLL combination example that provides an E2E redundant path.

Figure 68-5 VPLS and VLL combination to provide E2E redundant path



Provider Backbone Bridging in VPLS

Provider Backbone Bridging (PBB) is a technology configuration employed in next-generation networks that utilize carrier-grade Ethernet as the transport architecture. It addresses the potentially enormous increase in MAC addresses stored in the router lookup databases by encapsulating the customer frame in a Provider Ethernet header. The Customer MAC address (C-MAC) is then only dealt with by lower tier (or satellite) H-VPLS PEs. The core H-VPLS PEs only need to handle the backbone provider's MAC addresses (B-MAC), which are substantially less in number. For this reason, the technique is also referred to as MAC-in-MAC encapsulation.

IEEE 802.1ah defines an architecture and bridge protocols for interconnection of multiple Provider Bridge Networks (PBNs). PBB is defined in IEEE as a connectionless technology based on multipoint VLAN tunnels. MSTP is used as the core control plane for loop avoidance and load balancing. As a result, the coverage of the solution is limited by STP scale in the core of large service provider networks.

A Provider Backbone Bridged Network is a Virtual Bridged Local Area Network that comprises Backbone Edge Bridges (BEBs) and Backbone Core Bridges (BCBs) under the administrative control of a single backbone provider. Each BEB provides interfaces that encapsulate or verify the encapsulation of customer frames, and then relay those frames across the backbone. The term that the customer used may also mean a provider who is purchasing a service from another provider and using either a PBN or PBBN internally.

Backbone VLANs are used to create multipoint trunks in the backbone. The B-VLAN determines the route the frames take and limits broadcasting within the backbone. The B-TAG is added to the frame at the Customer Backbone Port (CBP). The selection of B-VLAN used to form the B-TAG is determined by the configuration of the CBP service instance table. This table maps ISIDs to B-VIDs and is created as part of service provisioning.

Backbone VLAN Connectivity

The backbone provider can use and configure MSTP to provide a number of independent spanning tree active topologies and can assign each B-VLAN to one of these active topologies to best use the resources in the network. MVRP, running in the context of each spanning tree active topology, configures the extent of each B-VLAN to the subset of that active topology necessary to support connectivity between the customer points of attachment to the instance of MAC service provided, and can reconfigure that connectivity as required if the spanning tree active topology changes. The operation of MSTP within a backbone provider's network is independent of the operation of any spanning tree protocol within attached provider or customer networks. This is achieved by removing all MSTP BPDUs received or to be transmitted at the service access interfaces. The operation of MVRP within a PBBN is independent of the operation of any configuration protocol within attached customer networks.

SR PBB implementation

The IEEE PBB model is organized around a B-component handling the provider backbone layer and an I-component concerned with the mapping of Customer/Provider Bridge (Q in Q) domain (that is, MACs, and VLANs) to the provider backbone (that is, B-MACs, and B-VLANs). The I-component contains the boundary between the customer and backbone MAC domains. PBB encapsulates the customer payload in a provider backbone Ethernet header, which allows the C-MACs to be hidden from the core PEs. A special Group MAC is used for the Backbone Destination MAC when the customer frame type is either unicast, multicast, broadcast, or unknown.

The SR PBB solution can be summarized as follows:

- Two VPLS variants are employed, namely B-VPLS and I-VPLS, functioning as the B-type BEB, and the I-type BEB respectively. A B-VPLS instance (a service instance within a service router) and its corresponding I-VPLS instances must be co-located in a service router. From a network-wide perspective, a B-VPLS comprises multiple Backbone Virtual Switch Instances (B-VSIs).

Note — For the description in this section and in the procedures in this chapter, B-VSI is used for a single B-type BEB instance, and is referred to as a B-Site. Similarly, I-VSI is used for a single I-type BEB instance, and is referred to as an I-Site.

- mB-VPLS and mI-VPLS are also available to provide loop avoidance for B- and I-VPLS in the same way as m-VPLS and regular VPLSs operate.
- A 5620 SAM VPLS can include regular sites and either B-Sites or I-Sites. The service should not contain both B-Sites and I-Sites. When a VPLS has at least one B-Site it becomes a B-VPLS. When a VPLS has at least one I-Site, it becomes an I-VPLS.

Note — Regular sites, B-Sites, and I-Sites cannot change their type after they are created.

- An I-Site can be bound to one B-Site, but a B-Site can be used by multiple I-VPLSs.
- The PBB function is only applicable to 7750 SR, 7450 ESS, and 7710 SR, Release 6.0 or later, OS 9700E and OS 9800E, Release 6.4.2 or later.

B-VPLS and I-VPLS instances

PBB processing may be seen as a chain of two linked VPLS contexts, namely B-VPLS and I-VPLS. Their characteristics are summarized in the sections that follow.

I-VPLS

I-VPLS is the abbreviated form for Service Instance ID (ISID) VPLS. An I-VPLS instance on a service site is referred to as an I-Site.

The following are I-VPLS and I-Site characteristics:

- An I-Site operates using customer addressing and maps the C-MACs to B-MACs.
- You can select one B-Site to associate with an I-Site; the B-Site must be on the same PE NE as the I-Site.
- I-Sites support only spoke SDP bindings and not mesh SDP bindings.
- An I-Site L2 access interface, or I-SAP, can co-exist on a port with regular L2 access interfaces or subscriber management M-L2 access interfaces. The existing port encapsulation is supported. An encapsulation tag that is used for service selection on an I-SAP is removed before the PBB encapsulation is added. The appropriate encapsulation tags are added at the remote PBB PE when sending the packet out on the egress access interface.

- An I-Site can be connected to one or more regular VPLS sites. A regular (network level) VPLS can have a mix of regular sites and I-Sites. The I-Sites of such services are responsible for the mapping of C-MACs to B-MACs. The regular sites of the service function as normal (bridge).
- ISID is a 24-bit field that carries the service instance identifier associated with this frame. It is used at the destination PE as a demultiplexer field, a function similar to a VC label. Default to service ID only works if the service ID is within the ISID range. For a service with service ID larger than 16 777 215, the ISID value must be specified.
- The ISID must be unique on one router.
- The Provider MSTP support in an M-VPLS is in the I-VPLS space.
- The I-Site MTU must be at least 18 bytes smaller than the B-Site MTU to which it is bound.
- If a VPLS has an I-Site attached to it, the VPLS has the Include I-Site(s) checkbox filled in. This checkbox appears on the service's General tab, after the I-Site has been created.
- IGMP snooping can be configured for I-Sites and I-L2 Access Interfaces.

Backbone-VPLS (B-VPLS)

Multiple L2 services can use a single B-VPLS. Ordinarily, a pair of SDP bindings (in opposite directions) provide either point-to-point connection between two sites of a service (as SDP bindings) or between different services (as a service connector). However, a B-VPLS provides a multipoint connection between sites of a service or for multiple services.

The following are properties and characteristics of a B-VPLS and B-Sites:

- The B-VPLS operates using the provider or backbone addressing (B-MACs).
- The B-VPLS provides backbone tunneling for one or multiple I-VPLSs.
- The B-VPLS accepts mesh or spoke SDP bindings, thereby providing both routing and MAC hiding using PBB/PW encapsulation.
- The B-VPLS accepts access interfaces using PBB encapsulation for tunneling through an Ethernet-only network.
- A regular (network level) VPLS can have a mix of regular sites and B-Sites to function as a B-VPLS (that is, operating using B-MACs).
- The backbone's Source MAC address can be configured on a B-Site. All the I-Sites provisioned under this B-Site shares the provisioned values. By default, this is a loopback chassis MAC address. It must be a unicast MAC address.
- A B-Site site can not be deleted until all its I-Site associations are removed.
- A B-Site can have both spoke and mesh SDP bindings and only an MPLS type of tunnel can be used (including LDP SDP). This also applies for a regular pseudowire, where the outgoing PBB frame on a B-SDP (that is, a B-PW) contains a B-VID qtag only if the PW type is Ethernet VLAN. Alternatively, if the pseudowire type is Ethernet, the B-VID qtag is stripped before the frame goes out.

- Only Null, Dot1Q, and Q in Q encapsulation types can be used by a B-Site L2 access interface. These access interfaces must use PBB encapsulation and have the following properties:
  - Ethernet Dot1Q is applicable to the bulk of PBB use cases, such as one B-VID.
  - Ethernet Null is supported for direct connection between neighboring I-VPLS, for example, when no B-VID is required and all traffic is sent to or from local I-VPLS.
  - There is no requirement for a PBB SAP type for PBB on the B-VPLS SAPs. Only the B-VID is used for tunnel delimitation on the port.
  - The default access interface type is blocked for the B-L2 access interface.
  - The following rules apply to the SAP processing of PBB frames:

    > For transit frames (frames not destined to a local MAC), there is no need to process the I-tag component of the PBB frames. Regular Ethernet SAP processing is applied to the backbone header (B-MACs and B-VID).

    > If a local I-VPLS instance is associated with the B-VPLS, then local frames (frames originated or terminated on local I-VPLSs) are PBB encapsulated and de-encapsulated using the pbb-etype provisioned under:

    related port->I-VPLS->root pbb component

    (listed in decreasing order of precedence, where the related port is highest in the order).
- If a VPLS has a B-Site attached to it, the VPLS has the Include B-Site(s) checkbox filled in. This checkbox appears on the service's General tab, after the B-Site has been created.

Service topology map views

Service and composite service topology maps support PBB.

The service map shows different types of sites with various icons for I-Sites, B-Sites, and Epipe PBB sites. With an I-VPLS bound to B-VPLS, the map shows the PBB backbone network as a cloud. The bindings between I-VPLS and B-VPLS are shown as a binding link.

MRP and MMRP support

The Multiple Registration Protocol allows participants in an MRP application to register Group MAC addresses with other participants in a Bridged LAN. An MRP participant may transmit and receive MRP PDUs. For the PBB implementation, the MRP parameters can be configured at the service site level, on the access interface, or the SDP binding.

If MRP is enabled on the node, 5620 SAM's MMRP application automatically advertises the presence of the Group B-MAC address on the active B-VPLS virtual links (that is, on the B-Site spoke bindings or the B-L2 access interfaces). You can view the MMRP entries advertised and/or received on the Forwarding Control>MMRP Entries tabs of the B-Site spoke bindings or the B-L2 access interfaces. All the MMRP entries may also be viewed together at the I-Site level.

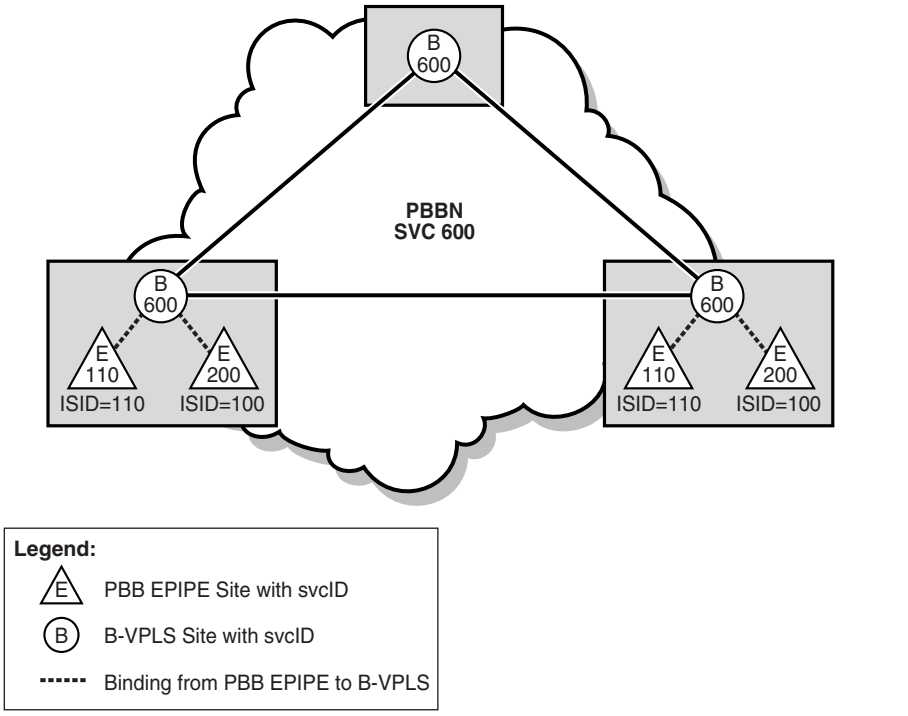
Epipe service with PBB

A PBB tunnel may be linked to an Epipe and to a B-VPLS. MAC switching and learning is not required for the point-to-point service, since all packets ingressing the Epipe access interface are PBB encapsulated and then forwarded to the PBB tunnel for the backbone destination MAC address. Similarly, all the packets ingressing the B-VPLS and destined for the ISID are PBB de-encapsulated and then forwarded to

the Epipe access interface. A fully-specified backbone destination address must be provisioned for each PBB Epipe instance to be used for each incoming frame on the related Epipe L2 access interface. If the backbone destination address is not found in the B-VPLS forwarding database, then packets may be flooded through the B-VPLSs.

To enable an Epipe service with PBB, the Epipe site is configured as a PBB site and functions similarly to a VPLS I-Site. This can only be specified during the site's creation. On the Epipe PBB site, you select a B-Site that acts as the tunnel for the Epipe. You also specify the destination B-MAC address of the remote PE where the other site is located. Figure 68-6 shows a simplified view of this configuration.

Figure 68-6 Epipe service link to a B-VPLS



See the *7750 SR OS Services Guide* for more information about PBB.

BGP Auto Discovery

BGP Auto Discovery enables a VPLS PE router to discover other PE routers that are part of the same VPLS domain. This allows each PE's configuration to consist only of the identity of the VPLS instance established on a specific PE, and not the identity of every other PE in that VPLS instance. If you need to change the VPLS topology, only the affected PE's configuration needs to change. Other PEs automatically discover the change using MP-BGP and adapt themselves accordingly. In contrast, if the BGP AD functionality is not used, you must then explicitly configure each PE router with the identities of all the other PEs in a specific VPLS.

You must assign a single, globally unique VPLS-ID to each VPLS (that is, the same value for all sites to the same VPLS across the entire network). The VPLS-ID eliminates the possibility of a collision between VPLSs belonging to different service providers.

There is also a globally unique Route Distinguisher (RD) ID associated with a VPLS. Each site also needs a unique ID that is a BGP NLRI. The PE address does not have to be globally routable, but it must be unique within the VPLS. The PE ID can be the PE router ID, for operational convenience.

Each site must also be associated with one or more RT Extended Communities, and the RTs control the distribution of NLRIs.

Each PE distributes the NLRI for each of its sites, with itself as the BGP next hop, and with the appropriate RT for each NLRI. A PE with a specific RT imports all NLRIs that have that same RT (and learns the other PEs addresses through their next hops). H-VPLS can be configured by using multiple RTs.

In summary, the BGP advertisement for a specific site in a PE includes:

- An NLRI. This is the VSI-ID.
- A BGP next hop equal to the loopback address of the PE.
- An extended community attribute containing the VPLS-ID.
- An extended community attribute containing one or more RTs.

Targeted-LDP [(T-)LDP] signaling is set up for the point-to-point PWs between sites using the selected (T-)LDP sessions corresponding to the remote PE(s) that have been recently added to their list.

To auto-create a Spoke-SDP, a PW Template must be created and pushed down to the NE. The SAM policy distribution mechanism is used to send out the template and maintain consistency in the network. The template selection is at the PE level, not at the service level, since not all PEs are capable of supporting BGP AD and some site types do not support BGP discovery (for example, I-Sites, at 5620 SAM, Release 6.1 R1).

Consider the following with regard to tunnel creation:

- If you plan to use BGP AD for all or part of the VPLS, you must not enable automatic mesh SDP binding creation.
- A provisioned PW to a specific remote PE takes precedence over one that is auto-discovered using BGP AD. In other words, if there is an existing SDP binding available, the router selects this existing binding and does not automatically create a new one.
- When the 5620 SAM auto-tunnel creation function is being used for non-BGP AD VPLSs, the automatically-created components are excluded from discovery. Also, you cannot select an automatically-created SDP or SDP binding when you create a service tunnel that is to be used as part of a BGP AD VPLS.

A 5620 SAM-managed VPLS or H-VPLS may consist of various site types located on different PEs, and which in turn, may be of differing versions. Due to these possibilities, some restrictions apply in terms of using Auto Discovery. For example, an M-VPLS site cannot be in the same service with a regular site. However, BGP AD-enabled sites and regular sites can be components of the same VPLS.

BGP VPLS

BGP VPLS is an extension of the VPLS concept. When configured as a BGP VPLS, such a service can interconnect with another BGP VPLS across different VPLS domains.

The control plane of the BGP VPLS provides auto-discovery and signaling capability. In this context, auto-discovery is a means for a PE router to discover other remote PE routers that are members of a given VPLS. The signaling function enables a PE router to know which pseudowire label a given remote PE router will use when sending the data to the local PE router. The BGP VPLS control plane carries sufficient information to provide the auto-discovery and signaling functions concurrently.

Some of the major features of the Alcatel-Lucent BGP VPLS solution include:

- The data plane is identical with the BGP AD (LDP VPLS) solution. For example, VPLS instances are interconnected via a pseudowire mesh. Split horizon groups may be used for loop avoidance between the pseudowires.
- Addressing is based on a two-byte VE ID assigned to the VPLS instance.
- The target VPLS instance is identified by the Route Target (RT) contained in the MP-BGP advertisement (extended community attribute).
- Auto-discovery is MP-BGP based.
- Pseudowire label signaling is MP-BGP based. As a result, the BGP NLRI content also includes label related information such as block offset, block size, label base, and so forth,

The Alcatel-Lucent BGP VPLS solution is compliant with RFC 4761.

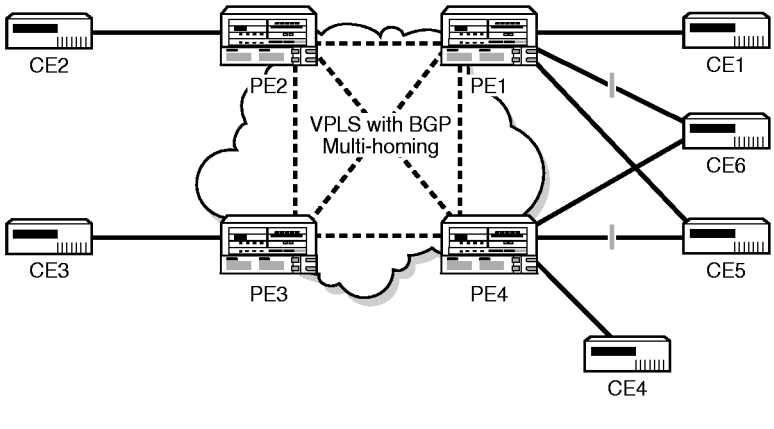
See the *7750 SR OS Services Guide* for more information regarding BGP VPLS.

BGP VPLS Multi-homing

The 5620 SAM allows BGP VPLS multi-homing to be established for CEs and access PEs by first configuring the multi-homing VPLS sites and then assigning the same multi-homing site ID to each.

Figure 68-7 shows an example of this approach, where a VPLS contains certain CEs that are multi-homed to pairs of VPLS PEs.

Figure 68-7 CE Multi-homing in VPLS



The BGP/LDP-signaled PW infrastructure (shown as the cloud at the center) is used to interconnect the VSIs between PEs. In this example, CE5 and CE6 are dual-homed to PE1 and PE4. To avoid loops, only one SAP must be active at any point in time between any multi-homed CE (such as CE5 or CE6) and its pair of connected PEs (such as PE1 and PE4). The others are blocked. Service providers use their MP-BGP on PE1 and PE4 to control the activation of the SAPs connected to the same customer site.

Other CE topologies (for instance, square connectivity) where, for example, CE1 and CE4 are part of the same customer site (and are themselves interconnected) are also supported.

When multi-homing a VPLS site using BGP (potentially into different autonomous systems), the PE routers (for example, PE1 and PE4) that are connected to the same customer site (for example, CE5) are configured with the same multi-homing ID. In this way, a loop-free topology is constructed using a routing mechanism such as BGP path selection. When a BGP speaker receives two equivalent NLRIs, it applies standard path selection criteria such as local preference and AS path length to determine which NLRI to choose.

Two VPLS NLRIs are considered equivalent from a path selection perspective if the following are identical:

- Route distinguisher
- Multi-homing ID

MVR on VPLS

MVR on VPLS is a bandwidth optimization method for applications on a broadband services network. At the port level, MVR allows a VPLS end user to subscribe or unsubscribe to a multicast stream on one or more network-wide multicast VPLS instances without requiring that the stream be part of the customer VPLS.

MVR on VPLS is a mechanism through which the supporting devices are able to participate in a multicast distribution system. Separate, dedicated VLANs must be constructed specifically for multicast traffic distribution.

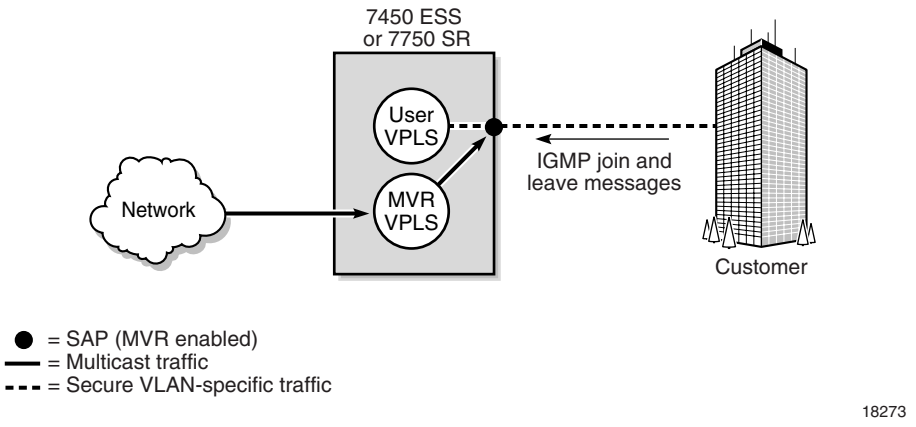
MVR assumes that hosts join and leave multicast streams by sending IGMP join and leave messages. The IGMP join and leave messages are sent inside the VPLS to which the host port is assigned. The multicast VPLS is shared in the network while the hosts remain in separate VLANs. For example, two user VPLS that are bound to the same MVR VPLS cannot exchange any information, but the same multicast service can still be provided to them.

An MVR VPLS is a VPLS that is responsible for sending multicast traffic through the network. An MVR VPLS is associated with a multicast package policy and has MVR-enabled sites. The MVR VPLS is configured to distribute certain multicast streams. An MVR VPLS can also be configured as a user VPLS to receive multicast traffic.

A user VPLS is a VPLS that contains SAPs that can receive multicast traffic from an MVR VPLS. Each SAP must be configured individually to use a specific MVR VPLS. Any VPLS, including an MVR VPLS, can be used as a multicast receiver for an MVR VPLS. IGMP and/or MLD snooping must be enabled on each site.

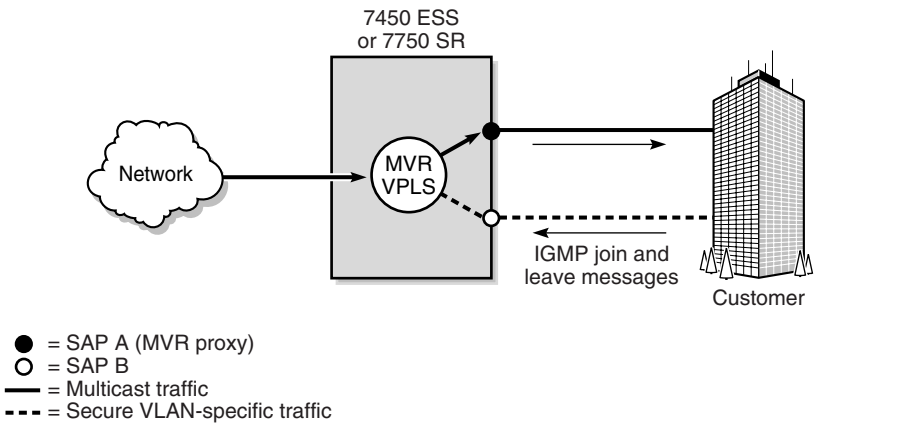
Figure 68-8 shows an example of MVR on VPLS. MVR reacts only to join and leave IGMP messages from the multicast groups configured for the MVR VPLS with which the user VPLS is associated. Join and leave messages from all other multicast groups are managed by IGMP and/or MLD snooping. Therefore, several MVR VPLS instances can be configured, each with its own set of multicast channels.

Figure 68-8 MVR on VPLS



In some situations, such as when a host is connected to a 7301 ASAM, the multicast traffic cannot be sent from the MVR VPLS to the VLAN on which the IGMP message was received (standard MVR behavior) but to another VLAN. This configuration is known as MVR by proxy. The 7450 ESS, 7750 SR, 7710 SR allow multicast traffic to be sent to a SAP other than the SAP from which the IGMP message originated. When configuring MVR by proxy, you must indicate the MVR VPLS on which the multicast channel is available and the SAP to which the multicast traffic must be copied. Figure 68-9 shows an example of MVR by proxy.

Figure 68-9 MVR by proxy



Configuring MVR on VPLS using the 5620 SAM involves the following steps.

1 Configure PIM before configuring MVR. See chapter 28 for more information.

2 Create a multicast package policy for all supporting NEs in an MVR VPLS. See chapter 46 for more information.

Alternatively, you can configure NEs individually in an MVR VPLS using a routing policy. See Procedure 27-8 for more information.

3 Create the MVR VPLS. See Procedure 68-1 for more information.

- Associate the multicast package policy with the service, which indicates that a VPLS is an MVR VPLS.
- Specify the VPLS sites that are the sources of the multicast groups. MVR must be enabled on each site.
- Configure SAPs only if you are configuring the MVR VPLS to be a user VPLS as well. See Procedure 68-1 for more information about configuring a user VPLS.

4 Create the user VPLS. See Procedure 68-1 for more information.

- The SAPs are standard host access points.
- Configure IGMP and/or MLD snooping and MVR on each site.
- Associate the MVR VPLS with each SAP for which access to multicast traffic is needed. This association means that IGMP requests received at that SAP for a multicast group are fulfilled as long as the multicast group being requested is included in the multicast package policy of the MVR VPLS. After the SAPs in a user VPLS have been associated with a specific MVR VPLS, the SAP becomes known to the MVR VPLS.

5 If using MVR by proxy, configure a VPLS SAP that is to act as the MVR proxy. See Procedure 68-1 for more information.

In a situation in which an MVR VPLS has VPLS sites that do not support MVR, the following conditions apply.

- The ability to configure MVR is not available for the VPLS sites and SAPs of a device that does not support MVR.
- Multicast package policies are not distributed to the devices that do not support MVR.

GSMP group on VPLS

The edge devices determine the circuit that opens an ANCP session. ANCP provides status and control information such as current line rate and port-up and port-down messages to the edge devices. The edge devices perform the following functions:

- adjust the H-QoS subscriber scheduler with the correct rate
- raise an alarm when the rate goes below a set threshold
- send DSL line OAM commands to complete OAM tests

A GSMP group is created under the GSMP tab of the VPLS site form. Multiple groups can be defined and different ANCP capabilities can be associated with different groups. A neighbor can be defined in a GSMP group. Multiple neighbors can be configured for each group.

Note — A GSMP group must be configured on VPLS, MVPLS or VPRN for an ANCP session to open.

L2 management interfaces on VPLS

L2 management interfaces act as a host. L2 management interfaces are created the same way out-of-band interfaces are created on VPLS. L2 management interfaces are used for CPM protocols such as telnet, SSH, SNMP, ping, and ANCP.

CPM filtering is used to limit access to L2 management interfaces.

Routed VPLS

A routed VPLS connector joins an L3 access interface within an IES or VPRN service context to a VPLS service on the same site. When an IES or VPRN IP interface is bound to a VPLS site name, the site name cannot be bound to another IP interface. While an IES or VPRN IP interface can only be bound to a single VPLS site, the service context containing the IP interface can have other IP interfaces bound to other VPLS sites. Both the IES or VPRN IP interface and VPLS site must be located on the same NE.

If a VPLS site name does not exist within the system, the binding between the IP interface and the VPLS site remains operationally down until a VPLS site name is assigned to the VPLS site. When an IP interface is bound to a VPLS site, the operational state of the routed VPLS binding is dependent upon the operational state of the VPLS site, and whether the IP interface binding is enabled on the VPLS site.

This functionality is limited to supporting devices.

Note 1 — You can create and manage a routed VPLS connector from the Components tab on the Composite Service (Edit) form or from an IES or VPRN access interface form, routed VPLS path.

Note 2 — The routed VPLS binding will not be operationally up until the Enable IP interface binding parameter is set to true and the VPLS site is operationally up. See Procedure 68-1 for more information.

FIBs

The FIB is the set of information that represents the best forwarding information for a destination. A FIB entry is analogous to a static MAC address, and every computer and network node has a MAC address that is hardware-encoded. In 5620 SAM, static MAC addresses can be also created on VPLS endpoint objects, access interfaces, and service circuits.

The edge devices perform the packet replication required for broadcast and multicast traffic across the bridged domain. Devices perform MAC-address learning to reduce the amount of unknown destination MAC address flooding. The edge devices learn the source MAC addresses of the traffic arriving on their access and network ports. You can also specify and manage static MAC addresses using the FIB entries table.

Each device maintains a FIB for each VPLS instance. Learned MAC addresses are populated in the FIB table of the service. All traffic is switched based on MAC addresses and forwarded between all participating sites using the service. Unknown destination packets (i.e., the destination MAC address has not been learned) are forwarded on all LSPs to the participating devices for that service until the router responds and the MAC address is learned by the device associated with that service.

Note — Each VPLS FIB entry consumes system resources. The devices allow you to set the maximum number of MAC entries allowed in a VPLS instance to prevent a VPLS instance from consuming a disproportionate amount of resources.

The size of the VPLS FIB can be configured with a low watermark and a high watermark expressed as a percentage of the total FIB size limit. If the actual FIB size grows above the configured high watermark percentage, an alarm is generated. If the FIB size falls below the configured low watermark percentage, the alarm is cleared.

MAC learning

Like an L2 device, learned MACs within a VPLS instance can be aged out if no packets are sourced from the MAC address for a specified period of time (the aging time). In each VPLS, there are independent aging timers for locally learned MAC and remotely learned MAC entries in the FIB. A local MAC address is a MAC address associated with an access interface, because it ingressed on a SAP. A remote MAC address is a MAC address received using a service tunnel from another device that is part of the VPLS.

Unknown MAC discard is a feature which discards all packets ingressing the service where the destination MAC address is not in the FIB. The normal behavior is to flood these packets to all end points in the service.

MAC learning can also occur for Split Horizon Groups (SHG) but with accompanying risks. For example, in an L2 environment of an SHG, hosts—among whom mutual communication is disallowed—can launch DoS attacks by sending a flood of packets that source an uplink MAC address to unprotected customer SAPs.

This situation can be managed by controlling MAC learning on the SAPs and SDPs in the following way: when a frame arrives at a protected SAP or SDP, the MAC is applied to its learning table; when a frame arrives at an unprotected customer SAP or SAP containing the address of a protected source MAC address, the frame is immediately dropped and not learned by the unprotected SAP. As a result, the

unprotected SAP does not know the MAC address of the uplink and, therefore, cannot use it to flood packets to other SAPs in the SHG. You can create a list of protected MAC addresses and configure the behavior of a SAP that receives a frame that contains a protected source MAC address or an unprotected destination MAC address.

MAC move

A sustained high MAC re-learn rate can be a sign of a loop somewhere in the VPLS topology. Typically, STP detects loops in the topology, but for those networks that do not run STP, the MAC move feature is an alternative way to protect the network against loops.

When enabled on a VPLS, MAC move monitors the re-learn rate of each MAC. If the rate exceeds the configured allowed limit, it disables the SAP on which the source MAC last arrived. The SAP can be disabled permanently or for a length of time that grows linearly with the number of times the SAP is disabled.

There is also the option of marking a SAP as non-blockable, which means that when the re-learn rate exceeds the limit, another SAP—one that is blockable—is disabled instead. When the MAC move parameter is set to blockable, ports can be blocked in a specific order depending on the number of times the re-learn rate exceeds the configured threshold period.

MAC move is configurable on VPLS SAPs and VPLS spoke SDPs. Blocking information for an object is displayed on the MAC move configuration form for the object. This information includes:

- the number of MAC learning retries that remain before blocking occurs
- the time that remains before the blocked object is unblocked
- the order of blocking, starting with tertiary, secondary and primary

Flooding

Traffic that is normally flooded throughout the VPLS can be rate limited on SAP ingress through the use of Service Ingress QoS Policies. In a Service Ingress QoS Policy, individual queues can be defined per forwarding class to provide shaping of broadcast traffic, MAC multicast traffic and unknown destination MAC traffic. You can also specify how to classify frames.

Multiple services and service types can be configured on a port. VPLS spanning tree protocols are configured on a per-service site basis, not a per-port basis, thus, multiple instances of STP per site are supported. Unknown destinations, broadcasts, and multicasts are flooded to all other SAPs in the service.

The flooding mechanism and the way that the Interior Gateway Protocol (IGP) operates ensure that no packets are duplicated on any interface. If SAPs are connected together, either through misconfiguration or for redundancy purposes, loops can form and duplicate packets can traverse the network. The STP is designed to prevent multiple SAPs from forwarding a packet into the VPLS

Spanning tree protocols

The 5620 SAM supports RSTP for VPLS instances and maintains support for legacy STP implementations. STP on the 7750 SR and 7710 SR incorporates an optimized and compatible implementation of IEEE 802.1D which attempts to eliminate STP blocking of links in the core of the VPLS. STP on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7450 ESS is used to guarantee that service tunnels are not blocked in any circumstance while not imposing artificial restrictions on the placement of the root bridge within the network. To provide this support, all mesh service tunnels are configured as root ports or designated ports.

RSTP, which is the default STP mode managed by the 5620 SAM, is compliant with IEEE standard 802.1D-2004. Other available STP types include an RSTP variant with 802.1w-2001 backward compatibility; an STP variant that is compliant with 802.1w-2001; and MSTP, an STP variant that is compliant with 802.1s-2002. The 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, 7750 SR, and 7710 SR support MSTP.

The 5620 SAM verifies STP parameters that are configured within each VPLS instance. However, it does not check the compatibility of STP configurations between interconnected VPLS instances.

IGMP snooping

IGMP snooping allows a device to snoop packets sent between IP multicast routers or switches and IP multicast hosts to learn the IP multicast group membership. The device checks the IGMP packets for the group registration information, and configures multicasting accordingly.

Without IGMP snooping, multicast traffic is forwarded to all ports, which is the same as broadcast traffic. IGMP snooping ensures that multicast traffic is only forwarded to ports that are members of the specific multicast group, which reduces the amount of multicast traffic passing through the device.

You can enable IGMP snooping for VPLS on the 7450 ESS, 7710 SR, 7750 SR, Release 1.0 R4 or later of the 7210 SAS-E, and Release 1.1 R6 or later of the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, and Release 6.4.2 R1 or later on the OS 9700E and OS 9800E. You can enable IGMP snooping for VPLS on the site, access interface, and spoke SDP components on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, and 7210 SAS-M24F2XFP [ETR]. A database of group members per VPLS instance is built by listening to IGMP queries and reports from each SAP and SDP of the instance. The reports are forwarded to the multicast routers.

IGMP snooping is not supported when MAC subnetting is enabled.

MLD snooping

Multicast Listener Discovery snooping is essentially the IPv6 version of IGMP snooping. The guidelines and procedures are very similar to IGMP snooping.

When MLD snooping is not enabled, L2 switches treat multicast traffic like an unknown MAC address or broadcast frame, that is, the frame is flooded out on every port of a VLAN. When MLD snooping is enabled, switches snoop the frame's L3 header for more efficient switching. In the context of IP multicast, only hosts that have expressed interest in receiving packets for the multicast groups have the frames forwarded to them.

The 7x50 and 7710 SR routers allow the enabling of MLD snooping for VPLS. A database of group members (per VPLS instance) is built by listening to MLD queries and reports from each SAP and SDP of the instance. These reports are forwarded to the multicast routers, if any are present.

MLD snooping is not supported when MAC subnetting is enabled.

Consider the following:

- Multicast groups can be learned (using the destination IP addresses of multicast packets) through MLD snooping or by static configuration at the port.
- The Fast leave feature modifies the membership leave mechanism by terminating the session immediately, rather than issuing a group-specific query to check if other members are still present on the network. Therefore, if a port (SAP or SDP) is configured for Fast leave, the session is terminated immediately without checking if the port also has other hosts subscribed to that same multicast group.
- A multicast router retains a list of multicast group memberships for each attached network. Therefore, a multicast router can assume the role of querier or listener. However, there can be only one querier per physical network.
- MLD snooping statistics are collected for each NE port, SAP, or SDP binding, and are viewable from the Statistics tab of a VPLS site properties form.
- The 5620 SAM supports MLDv1 and MLDv2.
- The 5620 SAM supports MVR.
- MLD snooping can co-exist with IGMP snooping and PIM snooping.
- MAC-based forwarding entries can be built using MLD snooping results.

PIM snooping

Protocol Independent Multicast snooping for VPLS allows a VPLS PE router to build multicast states by snooping PIM protocol packets that are sent over the VPLS. The VPLS PE then forwards multicast traffic based on the multicast states.

When all receivers in a VPLS are IP multicast routers running PIM, multicast forwarding in the VPLS can be efficient when PIM snooping for VPLS is enabled. After PIM snooping is turned up at the service level, all sites have PIM snooping configured and are set to the down state, by default. If any site does not support this feature, the 5620 SAM treats it as having PIM snooping turned off.

Since PIM snooping operates on PIM Hello packets as well as Join/Prune packets, PIM neighbors of the current router are learned by snooping on Hello packets. Therefore, in a meshed VPLS, every node learns from every other node's Hello packet and considers that node as a neighbor.

VPLS PE routers only snoop on PIM Hello and Join/Prune packets; they do not generate PIM messages on their own. Therefore, when PIM snooping is configured at the service level, all CE routers must have Join/Prune suppression disabled. If a VPLS PE router detects a condition where Join/Prune suppression is not disabled on one or more CE routers, the PE router puts PIM snooping into a non-operational state for the entire service. A trap on the PE is generated to report this condition and an alarm is raised to the 5620 SAM operator. To bring PIM snooping back to the operational state, PIM snooping must be disabled and then re-enabled.

Since PIM uses state refreshes, VPLS PE routers may not learn multicast states from all the CE routers, if PIM snooping was just enabled or the all snooping state was just cleared, until the next refresh.

To avoid traffic interruption, PIM snooping should hold up its operations for a period of time (60 seconds, if default timer is used). During this period of time, multicast traffic is flooded in the VPLS just like snooping was not enabled. SAM should have this hold-up timer configurable on VPLS properties panel having range 0-120 with 60 secs as default.

A variety of statistics are gathered for PIM snooping operation and are available for viewing and analysis in the PIM Snooping tab of a VPLS configuration form.

PIM snooping is not supported when MAC subnetting is enabled.

PIM snooping only supports IPv4.

Split horizon groups

SHGs control traffic that flows through SAPs or spoke SDPs for a VPLS site. SHGs prevent a packet received on a SAP within the group from being propagated to other members of the group.

SHGs are defined when you create or modify a VPLS site. You can create multiple SHGs for a VPLS site. SHGs can support a mix of spoke SDPs and SAPs. When you create SAPs or spoke SDPs they can be associated with an SHG.

Users can:

- configure, modify, or delete SHGs on a VPLS site
- associate SAPs or spoke SDPs with SHGs

Residential split horizon groups

RSHGs are SHGs with the Residential parameter enabled. SAPs that are associated with RSHGs are called lightweight SAPs. RSHGs use dual-pass queue optimization and do not support downstream broadcast or multicast traffic.

Users can:

- configure, modify, or delete RSHGs on a VPLS site
- associate SAPs or spoke SDPs with RSHGs

Note — If a SAP or spoke SDP is associated with an RSHG, then the following apply:

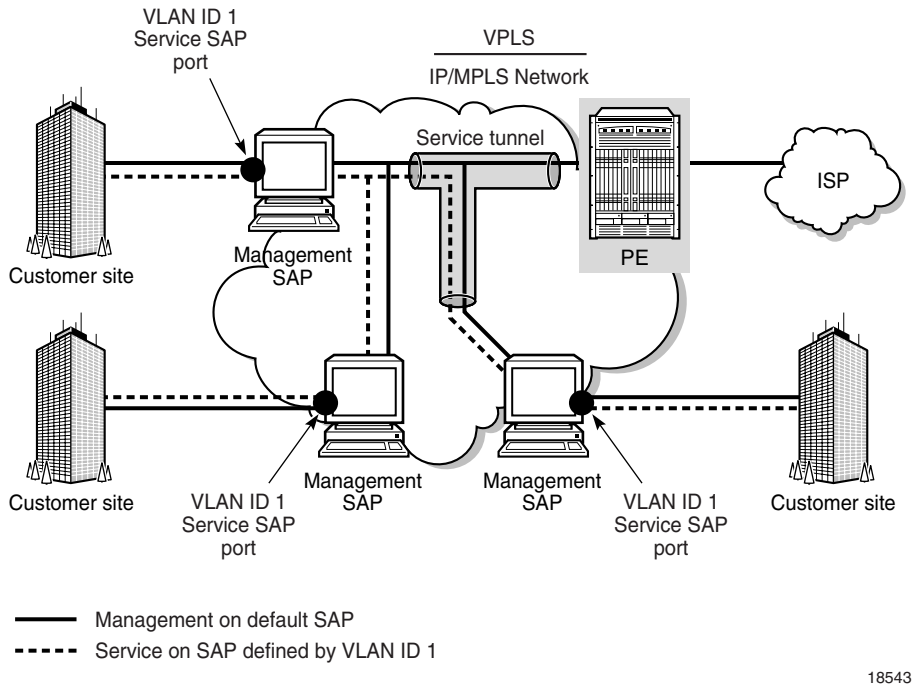
- MAC pinning is enabled by default and cannot be disabled for the interface
- IGMP snooping, MLD snooping, and MVR are not configurable for the interface

Default SAPs

The 5620 SAM allows you to create a default SAP that you can use in an L2-based service to perform management tasks or to deliver a specific class of end-user service. One default SAP can be defined on any dot1q encapsulated Ethernet port. You can create a default SAP by specifying an outer encapsulation value of 4095 or *. If OSSI is used, the outer encapsulation value is always 4095.

Figure 68-10 shows a default SAP used as a dedicated management port.

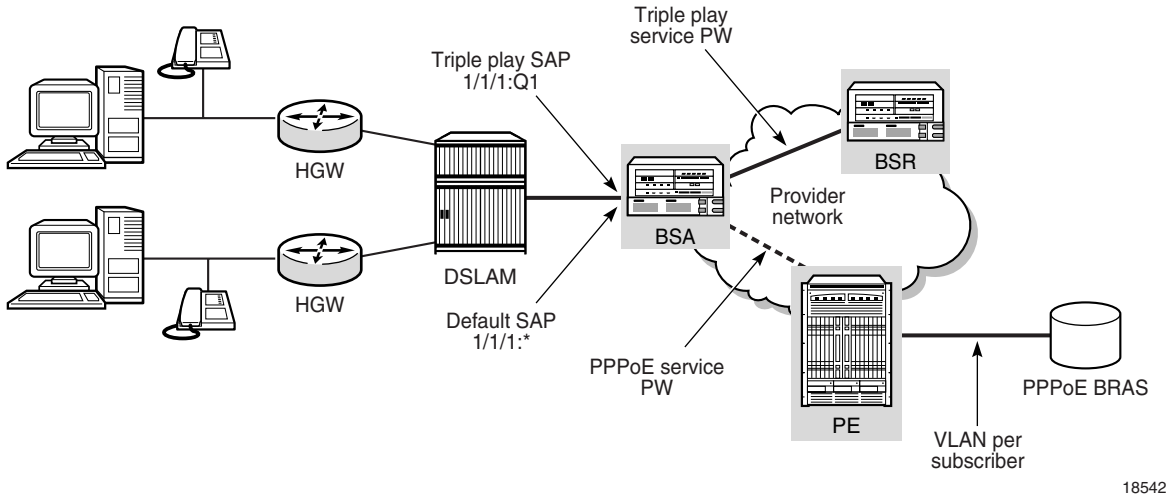
Figure 68-10 Default SAP as a dedicated management port



The dotted line shows that a business customer uses an entire port to access an L2 service using a VLAN tag ID 1, which is transparent to the network service provider. The service provider has assigned a default SAP for management of the customer network, as shown by the solid line. The customer uses one SAP for service delivery, and the service provider uses the default SAP to manage the customer network.

Default SAPs can also be used to differentiate one class of service from another on a single port. In Figure 68-11 the service provider can deliver aggregated high-speed Internet services on a single default SAP for multiple hosts while applying tags that assign one VLAN per host. At the same time, each of the remaining SAPs on the same port can be deployed for higher-level services, such as triple play delivery, in which multiple or individual hosts are assigned to a single SAP. Using such differentiated SAPs is efficient and significantly increases network scalability, because of the reduced number of SAPs allocated to various customers.

Figure 68-11 Default SAP to differentiate subscriber services



Layer 2 protocol tunneling termination

L2PT allows service providers to preserve the VLAN and Layer 2 protocol configurations of individual customers without impacting the traffic of other customers across the core network. L2PT termination allows Layer 2 PDUs to be transparently tunneled across the core network, avoiding interaction between the network provider and customer protocols.

Transparent L2PT is performed on the ingress side of every SAP or spoke SDP of the PE routers configured with L2PT termination. L2PT tunnels PDUs by overwriting the customer PDU of the destination MAC address in an Ethernet packet the multicast MAC address 01-00-0c-cd-cd-d0. The Ethernet packet is then transparently tunneled over the core network to a peer PE router. The peer PE router at the egress side of the tunnel restores the MAC address and the L2 protocol so that packets are forwarded to all ports in the same VLAN.

L2PT termination can only be enabled if STP is disabled on the VPLS.

BPDU translation

VPLS networks typically interconnect customer sites that use different access technologies, such as Ethernet and bridge-encapsulated ATM PVCs. Because of this, BPDU translation may be necessary to provide end-to-end interconnectivity.

If BPDU translation is enabled on a SAP or spoke SDP, the device intercepts all BPDUs and performs the required translation.

BPDU translation can be enabled only on a SAP or spoke SDP binding if STP is disabled on the VPLS.

DoS protection

To protect a VPLS from a high incoming packet rate that characterizes a DoS attack, you can use the 5620 SAM to create DoS protection policies for the VPLS L2 access interfaces. A DoS protection policy limits the number of control-plane packets that an interface receives each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

You can configure a DoS protection policy to control the following on a VPLS L2 access interface:

- the control-plane packet arrival rate per subscriber host on the interface
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

Each VPLS L2 access interface on an NE that supports DoS protection is automatically assigned a default DoS protection policy. The default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified. See Procedure 18-3 for information about creating a DoS protection policy.

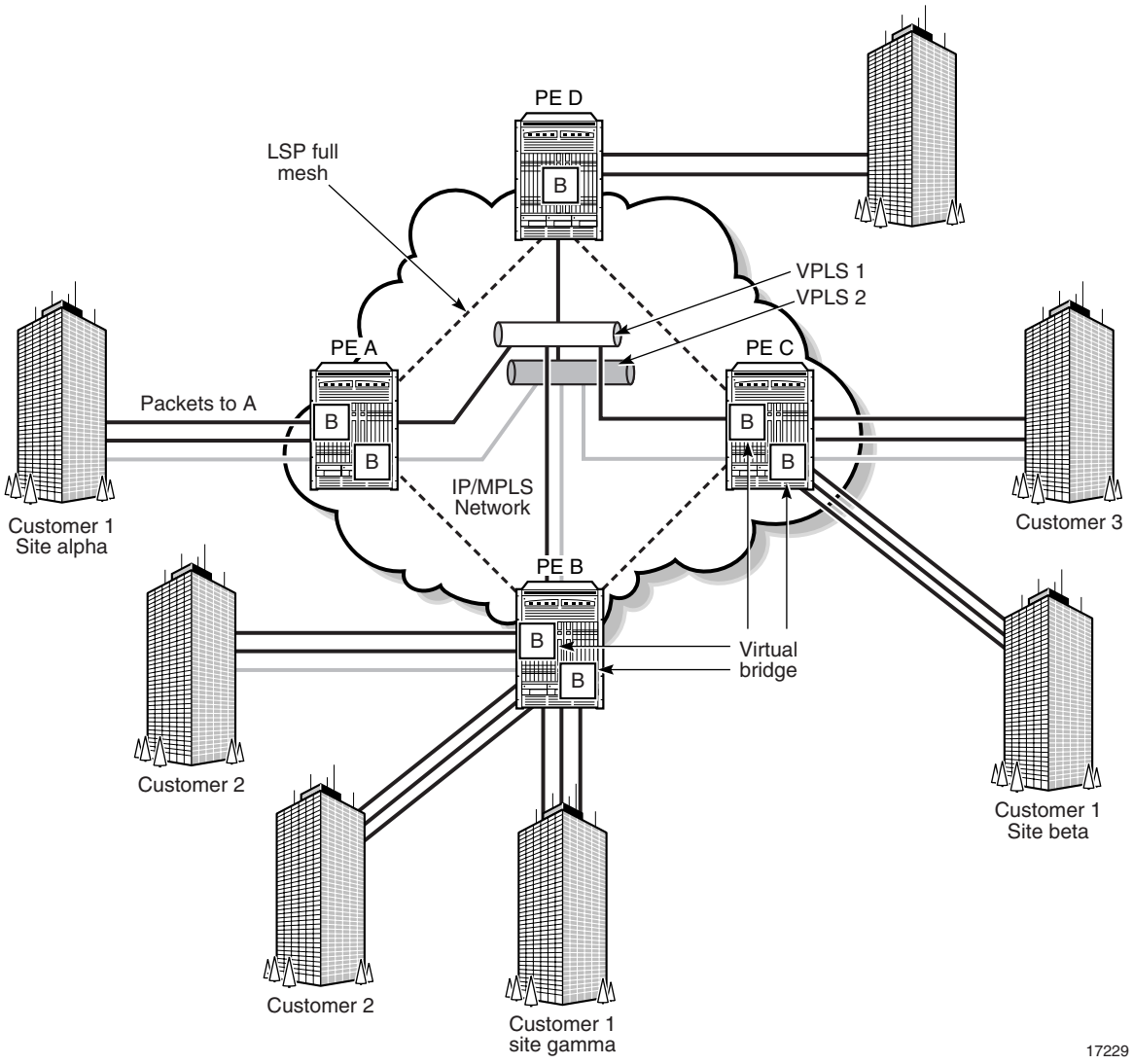
Copying and moving SAPs between ports

You can copy and move SAPs between ports. See "Moving and copying SAPs between ports" in chapter 15 for more information.

68.2 Sample VPLS configuration

Figure 68-12 shows a sample VPLS configuration.

Figure 68-12 Sample VPLS



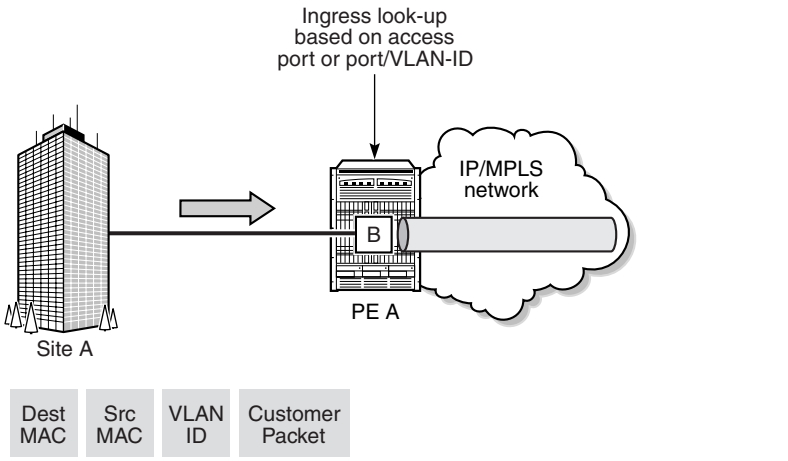
VPLS 1 is a distributed service, which consists of customer 1 connected to PE A, PE B, and PE C, at sites alpha, gamma, and beta, respectively. All three customer sites belong to VPLS 1.

In the following example, Customer 1 wants to send data from site alpha to site beta.

Customer 1 packets arriving at PE A are associated to the appropriate VPLS 1 for that customer, based on the combination of the access port and the dot1q (VLAN ID) in the packet. PE A learns the source MAC address in the packet and creates an entry in the FIB table that associates the MAC address to the access port on which it was received.

PE A is sending the packets to PE C. The destination MAC address in the packet is looked up in the FIB table of PE A for the VPLS instance, as shown in Figure 68-13.

Figure 68-13 Packet forwarding by ingress router PE A



The destination MAC address in the FIB table has one of two values:

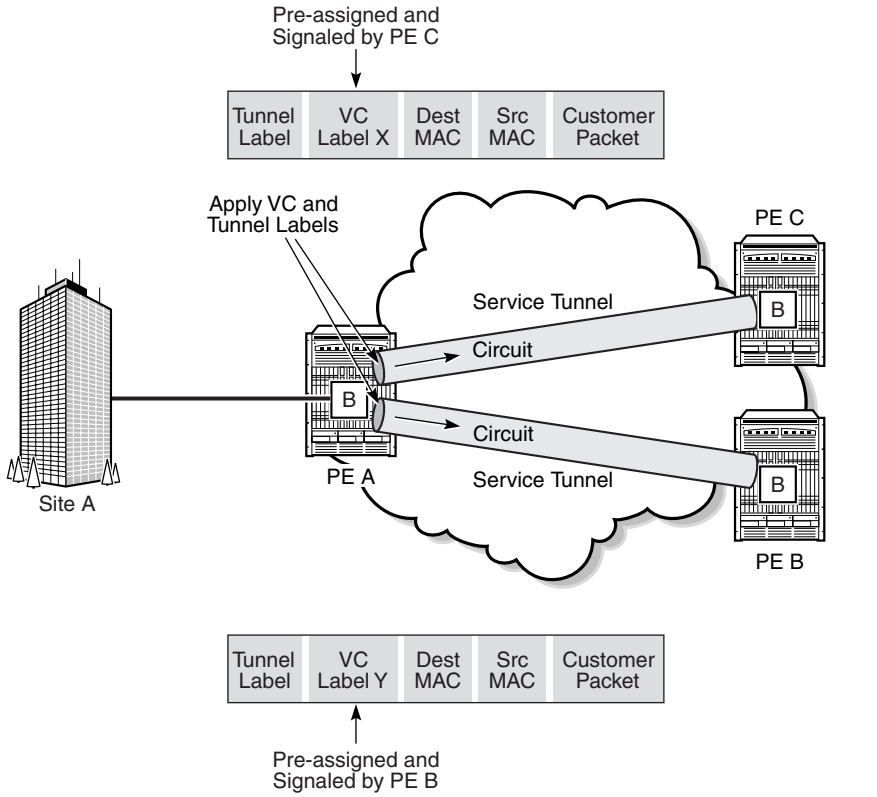
- known
- unknown

If the destination MAC address is known by PE A, an existing entry in the FIB table identifies the far-end PE C and the service VC label (VLAN ID) used to send the packets from PE A to PE C. PE A chooses a transport LSP to send the packets to PE C. The packets from the customer 1 site alpha to site beta are sent on the LSP after the VC label is removed and the transport label is added to the packet, as shown in Figure 68-13.

If the destination MAC address is not known by PE A, PE A floods packets to both PE B and PE C, which are both part of VPLS 1. PE A uses the VC labels (VLAN IDs) that PE B and PE C previously signaled for this VPLS 1.

As shown in Figure 68-14, the packets from PE A are transported across the core IP/MPLS network.

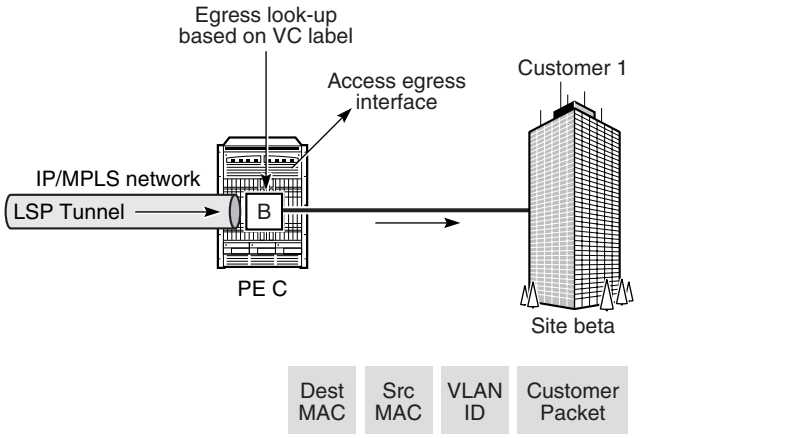
Figure 68-14 Packet forwarding from PE A across the core IP/MPLS network



The core routers are LSRs that switch the packets towards their destination based on the tunnel label, also called a transport label. The core routers are not aware that the packets belong to a VPLS.

When the packets from PE A arrive at PE C, PE C removes the tunnel label to reveal the VC label that associates the packets with VPLS 1, as shown in Figure 68-15.

Figure 68-15 Packet forwarding by egress router PE C



PE C learns the source MAC address of PE A and creates an entry in its FIB table that associates the MAC address and the VC label with PE A. The destination MAC address is looked up in the FIB table. It has one of two values:

- known
- unknown

If the destination MAC address is known by PE C, an existing entry in the FIB table identifies the local access (egress SAP) port used by VPLS 1 site beta and the service VC label (VLAN ID) that needs to be added to send the packets from PE C to customer 1.

If the destination MAC address is not known by PE C, PE C floods packets to all local access ports that belong to VPLS 1.

Assuming the core IP/MPLS network has already been configured, the following high-level tasks are required to configure this sample VPLS.

Table 68-1 Sample VPLS configuration

Task	Description
1. Configure policies as required	Policies must be configured before service creation. The following key policies can be applied to resources that are part of a VPLS: • Access ingress and access egress policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress to open the access ingress and egress interface policy forms. • Scheduler policy. Choose Policies→QoS→SROS QoS→Scheduler to open the scheduler policy form. • ACL MAC filter policies. These policies specify access control lists based on MAC addresses. You can specify MAC learning for access ports or tunnels. Choose Policies→Filter→ACL MAC Filter to open the ACL filter policy form. • Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form. • ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form. • DoS protection policy. Choose Administration→Security→NE DoS Protection to open the NE DoS protection form.
2. Configure ports as access ports for use in the service	Choose a port from the navigation tree, right click on the port, and choose Properties. Specify the port as an access port and specify an encapsulation type, if required.
3. Configure service tunnels, as required.	Service tunnels, or SDPs, are automatically created if there are no tunnels between the source and destination devices. You must choose GRE or LDP as the transport type for the 5620 SAM to automatically create service tunnels. To manually create service tunnels, choose Manage→Service Tunnels. Service tunnels carry service traffic between edge-managed routers. Services are associated with service tunnels by SDP bindings during service configuration. During service creation, you can also configure the 5620 SAM to automatically create SDP bindings to associate service tunnels with a service. In this case, you do not have to create service tunnels before you create the service.
4. Create and configure Customer 1.	Choose Manage→Service→Customers to open the customer manager form and create the customer.

(1 of 3)

Task	Description

5. Create and configure VPLS 1.	• Specify Customer 1 as the customer for the VPLS.
	• Configure MVR for the VPLS, if required.
	• Configure a GSMP Group and a GSMP group neighbor for the VPLS, if required.
	• Configure L2 management interfaces, if required.
	• Specify PE A, PE B, and PE C as the sites for the VPLS.
	• Specify VPLS STP parameters, if required.
	• Specify VPLS FIB parameters, if required.
	• Specify VPLS MAC move parameters, if required.
	• Specify VPLS MAC flush parameters, if required.
	• Enable VPLS PIM snooping, if required.
	• Specify VPLS IGMP snooping parameters, if required.
	• Specify VPLS MLD snooping parameters, if required.
	• Create an SHG for the VPLS, if required.
	• Configure and specify access interfaces on the PE A and PE C sites as the access interfaces for the VPLS to site alpha and site beta. You do the following when you configure interfaces:
	  • Specify the ports for the access interfaces and configure the access interfaces. Ports must be configured as access ports.
	  • Specify the EMG to which the L2 access interface belongs.
	  • Assign ingress and egress QoS policies as required.
	  • Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
	  • Assign ACL filter policies as required.
	  • Assign an accounting policy, if required.
	  • Specify a ToD suite, if required.
	  • Configure STP and FIB forwarding control.
	  • Configure subscriber management parameters, if required.
	  • Assign a DoS protection policy, if required.
	  • Configure VPLS PIM snooping, if required.
	  • Configure IGMP snooping for the interface, if required.
	  • Configure MLD snooping for the interface, if required.
	  • Configure DHCP for the interface, if required.
	  • Configure ARP host configuration, if required.
	  • Configure MVR for the interface, if required.
	  • Configure anti-spoofing for the interface, if required.
	  • Associate MEPs with SDP spoke bindings or SAPs, if required.
	  • Associate virtual MEPs with services, if required.
	  • Configure ANCP, if required.
	  • Configure ATM functionality, if required.
	• Create and configure service tunnels in both directions.
	• If the VPLS is a distributed VPLS, configure mesh SDP bindings to connect the VPLS sites. You can also configure the 5620 SAM to automatically create SDP bindings.

6. Create, update, or configure additional sites or L2 access interfaces for the VPLS.	• Repeat the above steps as required. • Create an MSAP policy, if required. See Procedure 64-7 for more information about creating an MSAP policy. • Configure the SAP Sub Type to be created. If your SAP is to support a shared SAP model, configure a Regular SAP; that is choose Regular as the SAP Sub Type. If you need to use an MSAP to support the one subscriber per SAP model, choose Capture as the SAP Sub Type and then configure the Capture L2 Interface parameters, which control the DHCP, PPPoE, or ARP triggered creation of MSAPs. See Managed SAP (MSAP) in section 64.1 for more information about creating a Capture SAP and MSAP.
7. For an HVPLS, use spoke SDP bindings to connect VPLS sites to other sites in the same VPLS, to sites in a different VPLS, or to VLL service sites.	An HVPLS consists of VPLS sites connected to other VPLS sites in the same or different VPLS, or to VLLs, using spoke SDP bindings. You perform the following when you configure an HVPLS. • Create one or more VPLS and VLL services, as required. See chapter 67 for information about creating a VLL service. See Procedure 68-1 in this chapter for information about creating a VPLS. • Create spoke SDP bindings between the service sites, one in each direction. Specify existing service tunnels and a VC ID for the spoke SDP bindings, as required.

(2 of 3)

Task	Description
8. Create a single MVPLS.	Create an MVPLS to run RSTP and to protect redundant spoke SDPs or SAPs in the associated VPLS.
9. Create a composite MVPLS to manage traffic blocking for multiple VPLS.	An MVPLS composite service manages traffic for multiple VPLS with redundant spoke SDPs or SAPs. You perform the following when you configure an MVPLS composite service. • Create a composite service and add the individual MVPLS. • Create spoke SDP connectors between the MVPLS.

(3 of 3)

68.3 Workflow to create a VPLS

1. Set up group and user access privileges.
2. Configure the network:
   - **i** Build the IP or IP/MPLS core network.
   - **ii** Configure ports for the service as access ports.
   - **iii** Configure service tunnels.
3. Configure predefined QoS, scheduling, filter, multicast package, accounting, and time of day suite policies. You do not have to create predefined policies if policies are created on a per-service basis.
4. Create and configure the VPLS.
   - **i** Define the service type as VPLS.
   - **ii** Ensure the LSP network is configured when the transport mechanism is MPLS.
   - **iii** Configure HVPLS spoke redundancy, if required.
   - **iv** Specify the sites for the service.
   - **v** Create endpoints for redundant configuration, if required.
   - **vi** Create a spoke SDP binding under any endpoints you created.
   - **vii** Configure the split horizon group parameters, if required.
   - **viii** Configure DHCP, if required.
   - **ix** Configure MVR, if required.
   - **x** Configure GSMP group and GSMP group neighbor parameters, if required.
   - **xi** Specify the STP parameters, if required.
   - **xii** Create MSTP instances and associate VLANs, if required.
   - **xiii** Specify protected MAC addresses, if required.

5 Create L2 access interfaces for the VPLS sites, as required.

i Specify aggregation on a service basis, or across a card or port.

ii Configure MSAP policies, if required. Create an MSAP Policy to control how the parameters are applied to an MSAP when it is automatically created. See Procedure 64-7 for more information.

iii Configure the SAP Sub Type as Regular or Capture, as required. Regular is the default value used for the creation of a SAP and Capture is the value used to enable the automatic creation of an MSAP. That is, you create a Capture SAP to enable the creation of an MSAP. See Procedure 64-8 for more information about creating a Capture SAP.

iv Assign QoS, scheduling, accounting, ANCP and filter policies.

v Specify MAC ACL filters, if required.

vi Assign a time of day suite, if required.

vii Configure the FIB and STP parameters.

viii Configure subscriber management, if required.

ix Assign a DoS protection policy, if required.

x Configure PIM snooping parameters, if required.

xi Configure IGMP snooping parameters, if required.

xii Configure MLD snooping parameters, if required.

xiii Configure DHCP relay parameters, if required.

xiv Configure ARP hosts, if required.

xv Configure MVR, if required.

xvi Configure anti-spoofing parameters, if required.

xvii Configure queue override parameters, if required.

xviii Configure MEP parameters, if required.

xix Configure ANCP, if required.

xx Configure L2 management interfaces, if required.

6 Create mesh SDP bindings for the VPLS, as required.

7 Turn up the service.

8 Add spoke SDP bindings for HVPLS, as required.

68.4 Workflow to create a VPLS service on OS 9700E and OS 9800E NEs

1. Set up group and user access privileges.
2. As a prerequisite for creating a VPLS service, configure the network:
   - i. Build the IP or IP/MPLS core network, including configuring the LSPs required to create service tunnels.
   - ii. Configure ports for the service as access ports.
   - iii. Configure service tunnels.
3. Configure predefined QoS, scheduling, filter, multicast package, accounting, and time of day suite policies. You do not have to create predefined policies if policies are created on a per-service basis.
4. Create and configure the VPLS.
   - i. Define the service type as VPLS.
   - ii. Specify the sites for the service.
   - iii. Create endpoints for redundant configuration, if required.
   - iv. Configure the split horizon group parameters, if required.
   - v. Configure DHCP, if required.
   - vi. Configure MVR, if required.
   - vii. Configure GSMP group and GSMP group neighbor parameters, if required.
   - viii. Specify the STP parameters, if required.
   - ix. Specify protected MAC addresses, if required.
5. Create L2 access interfaces for the VPLS sites, as required.
   - i. Specify aggregation on a service basis, or across a card or port.
   - ii. Configure the SAP Sub Type as Regular or Capture, as required. Regular is the default value used for the creation of a SAP and Capture is the value used to enable the automatic creation of an MSAP. That is, you create a Capture SAP to enable the creation of an MSAP. See Procedure 64-8 for more information about creating a Capture SAP.
   - iii. Assign QoS, scheduling, accounting, ANCP and filter policies.
   - iv. Specify MAC ACL filters, if required.
   - v. Assign a time of day suite, if required.
   - vi. Configure the FIB and STP parameters.
   - vii. Configure subscriber management, if required.

viii Assign a DoS protection policy, if required.

ix Configure PIM snooping parameters, if required.

x Configure IGMP snooping parameters, if required.

xi Configure MLD snooping parameters, if required.

xii Configure DHCP relay parameters, if required.

xiii Configure ARP hosts, if required.

xiv Configure MVR, if required.

xv Configure anti-spoofing parameters, if required.

xvi Configure queue override parameters, if required.

xvii Configure MEP parameters, if required.

xviii Configure ANCP, if required.

xix Configure L2 management interfaces, if required.

6 Create mesh SDP bindings for the VPLS, as required.

7 Turn up the service.

68.5 VPLS management procedures

Use the following procedures to perform VPLS creation and management tasks.

Procedure 68-1 To create a VPLS using configuration forms

Note — The following tab buttons are supported on the OS 9700E and OS 9800E NEs for VPLS configuration at the site level:

- General
- Components
- Scripts
- L2 Access Interface
- Forwarding Control
- Mesh SDP Bindings
- Templates
- Faults

1 Choose Create→Service→VPLS from the 5620 SAM main menu. The VPLS Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VPLS. The Select Customer - VPLS Service form opens.

3 Choose a customer for the VPLS and click on the OK button. The Select Customer - VPLS Service form closes, and the VPLS Service (Create) form displays the customer information.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Administrative State
- Inherit Service ID Value
- Default Mesh VC ID
- Automatic Mesh SDP Binding Creation
- Profile Name
- Transport Type
- OLC State

The OLC State parameter is configurable after you click on the Apply button.

The Profile Name and Transport Type parameters are only displayed when the Automatic Mesh SDP Binding Creation parameter is enabled. The Transport Type parameter is only configurable if the Profile Name parameter is left blank.

5 Depending on the type of device being configured, the MVR tab is configurable. Assign a multicast package policy to the VPLS, if required.

i Click on the MVR tab button.

ii Click on the Select button to choose a multicast package policy. The Select Multicast Package Policy - VPLS Service - Subscriber form opens.

iii Choose a multicast package policy and click on the OK button. The Select Multicast Package Policy - VPLS Service - Subscriber form closes, and the VPLS Service (Create) form refreshes with the multicast package policy name.

After the multicast package policy is applied to the VPLS, the policy is distributed as the routing policy to all MVR-capable VPLS sites. If you apply another package policy to the site, the new policy is distributed to the site. The previously distributed policy remains on the site.

6 If you are configuring the service for BGP Auto-Discovery, go to step 7. Otherwise, go to step 10.

7 Click on the BGP AD tab button.

8 Set the BGP AD Administrative Status parameter to Up. The BGP AD Service Identification group appears.

9 Configure the VPLS ID parameter. This parameter must be a unique network-wide ID.

10 Perform one of the following:

a Create a site for the VPLS. Go to step 11.

b Complete service creation if sites, L2 access interfaces, and SDP bindings for the VPLS are to be created later. Go to step 42.

11 Click on the Components tab button.

12 Right-click on the Sites icon and choose Create VPLS Site. The Select Network Elements - VPLS Service - Subscriber form opens with a list of available sites.

Note — The options to create either a B-Site or an I-Site are used when you are creating a VPLS that utilizes Provider Backbone Bridging. See "Provider Backbone Bridging in VPLS" in section 68.1 for more information.

13 Select a site and click on the OK button. The VPLS Site (Create) form opens with the General tab displayed.

14 Configure the parameters:

- Name
- Description
- MTU
- Enable MTU Check
- Default Mesh VC ID
- Administrative State
- Monitor Access Interface Operational State
- GSMP Administrative State
- PIM Snooping Enabled
- Per Service Hashing for LAG Enabled
- Enable IP Interface Binding
- SAP Type
- Customer VID
- PPPoE Circuit ID

Note 1 — The Enable IP Interface Binding parameter is configurable only on the 7450 ESS in mixed mode, and on the 7750 SR, Release 8.0 R5 or later.

Note 2 — The parameters that appear on the VPLS Site (Create) form depend on the device type and release that you are configuring.

If you are configuring a 7250 SAS-ES or 7250 SAS-ESA site, configure the following additional parameters:

- Default VC ID
- Inherit Service ID Value
- Enable Secure SAPs
- VPLS Tag
- VC Type

15 If you are configuring a 7250 SAS-ES or 7250 SAS-ESA site, go to step 30.

16 Configure MFIB, STP, FIB, and MAC learning protection parameters for the site, if required.

i Click on the Forwarding Control tab button. The MFIB tab is displayed.

ii Configure the parameters:

- Table size (entries)
- High Watermark (%)
- Low Watermark (%)

iii Click on the STP tab button to configure STP parameters for the site, if required. Otherwise, go to step iv.

- Bridge Forward Delay (seconds)
- Bridge Hello Time (seconds)
- Bridge Max Age (seconds)
- Priority
- STP Mode
- Maximum BPDUs (PDUs/Hello Interval)
- Administrative State

Note 1 — Alcatel-Lucent STP in a VPLS interoperates with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters balance the STP resiliency and speed of convergence. Modifying the bridge-level parameters must be done within the constraints of the following formulas:

- 2 × (Bridge Forward Delay – 1.0 s) >= Bridge Max Age
- Bridge Max Age >= 2 × (Bridge Hello Time + 1.0 s)

Note 2 — If you are configuring an MVPLS site, set the STP Mode parameter to RSTP or MSTP, depending on the MVPLS type. The MSTP option is available only if you are creating an MVPLS. See Procedure 68-10 for more information about creating an MVPLS.

Note 3 — MSTP is configurable only on the 7450 ESS and 7750 SR.

iv Click on the FIB tab button to configure FIB parameters for the site, if required. Otherwise, go to step 17.

v Configure the parameters:

- High Watermark (%)
- Low Watermark (%)
- Local Age Time (seconds)
- Remote Age Time (seconds)
- Size (entries)
- Aging Enabled
- Learning Enabled
- Discard Unknown Destinations
- MAC Flush on Fail
- Propogate MAC Flush
- MAC Subnet Length

vi Depending on the type of device being configured, the Mac Move panel appears. Configure the MAC move parameters, if required:

- Move Frequency
- Retry Timeout
- Number Of Retries
- Administrative State
- Primary Ports Cumulative Factor
- Secondary Ports Cumulative Factor

vii Click on the MAC Protection tab to configure the list of protected MAC addresses.

viii Click on the Add button. The MAC Protection (Create) form opens.

ix Configure the Protected Mac Address parameter.

x Click on the OK button to close the form and add the MAC address to the list of protected MAC addresses.

xi If you are configuring an MVPLS site that requires MSTP, click on the MSTP tab button. Otherwise, go to step 17.

Note — MSTP is configurable only on the 7450 ESS and 7750 SR.

xii Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

xiii Click on the MST Instances tab button.

xiv Click on the Add button. The MST Instance (Create) form opens with the General tab displayed.

xv Configure the parameters:

- Instance Index
- Priority

xvi Click on the VLAN Ranges tab button. Click on the Add button. The MST Instance Managed VLAN range (Create) form opens.

xvii Configure the parameters:

- Min. VLAN Tag
- Max. VLAN Tag

xviii Click on the OK button. The MST Instance Managed VLAN Range (Create) form closes, and a dialog box appears.

xix Click on the OK button. The MST Instance (Create) form refreshes with the new managed VLAN range.

xx Click on the OK button. The MST Instance (Create) form closes and a dialog box appears.

xxi Click on the OK button. The MVPLS Site (Create) form refreshes with the new MST instance.

17 Configure SHCV for the site, if required.

i Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

ii Select the SHCV Enabled parameter to enable SHCV.

iii Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source IP Address
- SHCV Source MAC Address
- SHCV Action
- SHCV Retry Timeout (seconds)
- SHCV Retry Count

18 Configure a default gateway for the site, if required.

i Click on the Default Gateway tab button.

ii Configure the parameters:

- Default Gateway IP Address
- Default Gateway MAC Address

19 Configure ingress multicast forwarding, if required.

Note — An Operational Channels tab appears when you access the VPLS Site form in the Edit mode. It displays data for the operational channels when traffic from a specific multicast source for a specific multicast group passes through the service. You must click on the Search button to refresh the data. See chapter 43 for information about listing the operational channel parameters.

i Click on the Mcast Path Mgmt tab button.

ii Click on the Select button to choose a multicast info policy. The Select Ingress Info Policy form opens.

iii Choose a policy in the list and click on the OK button. The Select Ingress Info Policy form closes and the policy identifier is displayed on the Site (Create) form.

20 Configure IGMP snooping for the site, if required.

i Click on the IGMP Snooping tab button.

ii Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Robust count
- Report source address
- Use query source address

21 Create an endpoint for redundancy (dual homing) on the site, if required.

Note — You cannot create a VPLS endpoint on a site that has an active or inactive MC ring SAP. See chapter 42 for more information.

i Click on the Endpoints tab button.

ii Click on the Add button. The VPLS Endpoint (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Name
- Description
- Revert time (seconds)
- Disable Revert Time (Infinite)
- Suppress Standby Signalling
- Ignore Standby Signalling
- MAC Pinning
- Maximum FIB Entries
- Block On Mesh Failure
- Endpoint Type

If you set the Endpoint Type parameter to Multi Chassis, go to step iv. Otherwise, go to step ix.

iv Configure the EndPoint ID parameter.

v Click on the Select button beside the Peer Name parameter. The Select Multi Chassis Endpoint Peer - VPLS Endpoint form opens.

vi Configure the filter and click on the Search button. A list of multichassis endpoint peers appears.

vii Select a multichassis endpoint peer and click on the OK button to close the Select Multi Chassis Endpoint Peer - VPLS Endpoint form. A dialog box prompts you to click on the OK or Apply button to commit the changes.

viii Click on the OK button.

ix Click on the OK button. A dialog box appears indicating changes are not committed until you click on the OK or Apply button.

x Click on the OK button. The Endpoint (Create) form closes and the Site (Create) form reappears with the new endpoint displayed in the list.

22 If you are configuring an MVPLS site, go to step 24.

23 Configure an SHG on the site, if required.

Note — You must configure an SHG or RSHG if you plan to create a spoke circuit from this VPLS site to a VLL or to another VPLS.

i Click on the Split Horizon Groups tab button.

ii Click on the Add button. The Site, New Split Horizon Group (Create) form opens.

iii Configure the parameters:

- Name
- Description
- Residential
- Restrict Protected Source
- Restrict Unprotected Destination
- Restrict Protected Source Action

iv Click on the OK button. The Site, New Split Horizon Group (Create) form closes.

24 Depending on the type of device you are configuring, the MVR tab is configurable. Configure MVR for the site, if required.

i Click on the MVR tab button. The General tab is displayed.

ii Configure the parameters:

- Administrative State

  The Administrative State parameter specifies whether a site is an MVR VPLS site.
- Description
- Use Component Package Policy
- Routing Policy Name

After the multicast package policy is applied to the MVPLS, the policy is distributed as the routing policy to all MVR-capable MVPLS sites. If you apply another package policy to the site, the new policy is distributed to the site. The previously distributed policy remains on the site.

iii If you deselect the Use Component Package Policy parameter, you must specify a multicast package policy to associate with the MVR VPLS site. Perform one of the following.

- Click on the Select button to specify a multicast package policy. The Select - VPLS Site form opens. Configure the filter criteria to choose a policy. Choose a policy and click on the OK button. The Select - VPLS Site form closes, and the VPLS Site (Create) form refreshes with the policy name.
- Manually enter a multicast package policy name as the Routing Policy Name parameter value.

iv Click on the User MVR SAPs tab button to view the VPLS SAPs that use the MVR VPLS site, if required.

- Click on the Search button to list the VPLS SAPs.

25 Configure a GSMP group on the site, if required.

i Click on the GSMP tab button.

ii Click on the Add button. The GSMP Group (Create) form opens.

iii Configure the following parameters:

- Displayed Name
- Description
- Administrative State
- Keep-Alive (seconds)
- Hold Multiplier
- OAM Administrative State
- Dynamic Topology Discovery

iv Click on the GSMP Group Neighbor tab button.

v Click on the Add button. The GSMP (Create) form opens.

vi Configure the following parameters:

- IP Address
- Description
- Administrative State
- Local Address
- Priority Type
- Priority Precedence
- Priority Dscp

vii Click on OK button. The GSMP (Create) form closes.

26 Configure L2 management interfaces, if required.

i Click on the L2 Management Interfaces tab button.

ii Click on the Add button. The VPLS L2 Management Interface Subscriber (Create) form opens.

iii Click on the General tab to configure the following parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- ARP Timeout (seconds)
- I/F MAC Address

iv Click on the Addresses tab button.

v Click on the Add button. The IP Address (Create) Form opens.

vi Configure the following parameters:

- Address ID
- IP Address
- Prefix Length
- Broadcast Address Format

vii Click on the OK button. The IP Address (Create) form closes.

27 Configure MLD snooping for the site, if required.

i Click on the MLD Snooping tab button.

ii Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Robust count
- Report source address
- Query source address

28 Depending on the type of device that you are configuring, the MVR (MLD) tab is configurable. Use the MVR (MLD) tab to use MLD snooping on the site. Configure MVR for MLD on the site, if required.

i Click on the MVR (MLD) tab button. The General tab is displayed.

ii Configure the parameters:

- Administrative State
  The Administrative State parameter specifies whether the site is an MVR VPLS site.
- Description
- Use Component Package Policy
- Routing Policy Name

The Routing Policy Name parameter is configurable when the Use Component Package Policy is disabled.

After a multicast package policy is applied to an MVPLS, the policy is distributed as the routing policy to all MVR-capable MVPLS sites. If you apply another package policy to the site, the new policy is distributed to the site and the previously distributed policy remains on the site.

iii If you deselect the Use Component Package Policy parameter, you must specify a multicast package policy to associate with the MVR VPLS site. Perform one of the following.

- Click on the Select button to specify a multicast package policy. The Select - VPLS Site form opens. Configure the filter criteria to choose a policy. Choose a policy and click on the OK button. The Select - VPLS Site form closes, and the VPLS Site (Create) form refreshes with the policy name.
- Manually enter a multicast package policy name as the Routing Policy Name parameter value.

iv Click on the User MVR SAPs tab button to view the VPLS SAPs that use the MVR VPLS site, if required.

- Click on the Search button to list the VPLS SAPs.

29 Configure IGMP host tracking, if required.

i Click on the IGMP Host Tracking tab button.

ii Configure the parameters:

- Expiry Time
- Administrative State

30 Click on the Components tab button.

31 To create an access interface for the site, perform steps 6 to 51 of Procedure 68-3.

32 To create a mesh SDP binding for the site, perform steps 6 to 26 of Procedure 68-4.

Note — You cannot create a mesh SDP binding on a 7450 ESS, 7250 SAS-ES or 7250 SAS-ESA site.

33 To create a redundant spoke SDP binding under an endpoint, perform steps 5 to 38 of Procedure 68-5.

34 To create a spoke SDP binding for the site, perform steps 8 to 38 of Procedure 68-5.

Note 1 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP, or enable MSTP on a site that has a spoke SDP binding.

Note 2 — You cannot enable MSTP on a SAP that has a non-zero encapsulation value.

35 To add a Video interface for the site, perform steps 5 to 13 of Procedure 33-3.

36 Click on the OK button. The VPLS Site (Create) form closes, and a dialog box appears.

37 Click on the OK button. The VPLS Site (Create) form displays the new site on the Components tab under VPLS Service→Sites .

38 To configure the site for BGP Auto-Discovery, BGP VPLS or as part of a BGP VPLS Multi-homing configuration, you must first complete the creation of the site and then perform either Procedure 68-6 or Procedure 68-7, as applicable.

Note — You can see a list of all current BGP VPLS Multi-homing sites in a VPLS multi-homing service on the BGP Multi-homing Sites tab.

39 Repeat steps 12 to 37 to create an additional site for the VPLS, as required.

40 Add protected MAC addresses at the service level, if required. Protected MAC addresses that you add on the site level, as performed in step 16, are automatically added to the service-level MAC protection list.

i Click on the Forwarding Control tab button.

ii Click on the MAC Protection tab button.

iii Click on the Add button. The MAC Protection (Create) form opens.

iv Configure the Protected Mac Address parameter.

v Click on the OK button. The MAC Protection (Create) form closes and the protected MAC address is listed on the VPLS (Create) form.

41 To reserve tunnel bandwidths, click on the Bandwidth tab.

Note 1 — The ability to reserve tunnel bandwidth is only applicable to B-sites on a VPLS configured as a PBB tunnel (that is, as a B-VPLS).

Note 2 — The Bandwidth tab is only available if service CAC is configured; see chapter 5 for information about enabling and disabling service CAC.

i Click on the Bandwidth Reserved Tunnel sub-tab button.

ii For each CoS, enter a value for the CoS Reserved Bandwidth (Mbps) to specify how much bandwidth this tunnel will reserve in the network.

iii Click on the Reserve Bandwidth button. This action checks to ensure that all the active links in the B-VPLS have enough bandwidth to admit the tunnel into the network and book the bandwidth. The tunnel status will be updated appropriately, based on the outcome of the action. Once the bandwidth is reserved, the BW Utilization tab on the applicable Physical Link properties form will also show this tunnel and the bandwidth information (refer to Procedure 4-39).

Note 1 — The reserved bandwidth of the tunnel can be changed at anytime after the service creation. However, if a change to the reserved bandwidth causes the used bandwidth to be greater than the requested change, or if there is insufficient bandwidth in the network to facilitate this change, then it will be denied and an appropriate message is displayed.

Note 2 — Once bandwidth is reserved on the tunnel, any changes to the topology of the B-VPLS (for example, uplinks added, STP state changes, and so forth) will be updated automatically with the correct bandwidth information on the underlying physical links. If there is insufficient bandwidth available when the changes happen, the bandwidth will still be booked on the physical links and the appropriate alarms will be raised.

Note 3 — To unreserve bandwidth of the tunnel after the service creation, you can set all of the configured Cos Reserved Bandwidth parameters back to 0. However, this can only be done when there are no longer any i-services riding on this PBB Tunnel.

Note 4 — After the service has been created, the Tunnel Usage sub-tab page shows all the i-services currently using this tunnel and the specific bandwidth usage per service.

42 Click on the OK button. The VPLS Service (Create) form closes.

Procedure 68-2 To create a VPLS on a 7210 SAS-E

1 Choose Create→Service→VPLS from the 5620 SAM main menu. The VPLS Service (Create) form opens.

2 Click on the Select button to choose a customer to associate with the VPLS. The Select Customer - VPLS Service form opens.

3 Choose a customer for the VPLS and click on the OK button. The Select Customer - VPLS Service form closes and the VPLS Service (Create) form reappears with the customer information displayed on the General tab.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Administrative State
- Automatic Mesh SDP Binding Creation
- Transport Type
- GSMP Administrative State
- PIM Snooping Enabled
- OLC State

The OLC State parameter is configurable only after you click on the Apply button.

The Profile Name and Transport Type parameters are configurable only when the Automatic Mesh SDP Binding Creation parameter is enabled.

The Transport Type parameter is configurable only when the Profile Name parameter is not configured.

5 Click on the Components tab button.

6 Right-click on the Sites icon and choose Create VPLS Site. The Select Network Elements - VPLS Service - Subscriber form opens with a list of available NEs.

7 Choose a 7210 SAS-E and click on the OK button. The VPLS Site (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- SAP Type
- Customer VID

9 Configure MFIB, STP, and FIB parameters for the site, if required.

i Click on the Forwarding Control tab button. The MFIB tab is displayed.

ii Configure the parameters:

- Table size (entries)
- High Watermark (%)
- Low Watermark (%)

iii Click on the STP tab button to configure STP parameters for the site, if required. Otherwise, go to step v.

iv Configure the parameters.

- Bridge Forward Delay (seconds)
- Bridge Hello Time (seconds)
- Bridge Max Age (seconds)
- Priority
- STP Mode
- Maximum BPDUs (PDUs/Hello Interval)
- Administrative State

Note — Alcatel-Lucent STP in a VPLS interoperates with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters balance the STP resiliency and speed of convergence. Modifying the bridge-level parameters must be done within the constraints of the following formulas:

- 2 × (Bridge Forward Delay – 1.0 s) >= Bridge Max Age
- Bridge Max Age >= 2 × (Bridge Hello Time + 1.0 s)

v Click on the FIB tab button to configure FIB parameters, if required. Otherwise, go to step 10.

vi Configure the parameters:

- High Watermark (%)
- Low Watermark (%)
- Local Age Time (seconds)
- Remote Age Time (seconds)
- Size (entries)
- Aging Enabled
- Learning Enabled
- Discard Unknown Destinations
- Move Frequency
- Retry Timeout
- Administrative State

10 Configure IGMP snooping for the site, if required.

i Click on the IGMP Snooping tab button.

ii Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Robust count
- Report source address

11 Click on the OK button. The VPLS Site (Create) form closes and a dialog box appears.

12 Click on the OK button. The VPLS Service (Create) form reappears.

13 To create a non-7210 SAS-E site for the VPLS, perform the following steps.

i Right-click on the Sites icon and choose Create VPLS Site. The Select Network Elements - VPLS Service - Subscriber form opens to display a list of available NEs.

Note 1 — The NE that you choose must be physically connected to the 7210 SAS-E by a port or LAG.

Note 2 — An NE that is physically connected to a 7210 SAS-E must be exclusively terminating.

ii Choose an NE other than a 7210 SAS-E and click on the OK button. The VPLS Site (Create) form opens with the General tab displayed.

iii Configure the site, as described in steps 14 to 37 of Procedure 68-1.

14 Create an Uplink SAP on the port or LAG of the 7210 SAS-E that is physically connected to the port or LAG of the terminating site.

a Right-click on Access Interfaces below the 7210 SAS-E site and choose Create VPLS L2 Access Interface. The VPLS L2 Access Interface (Create) form opens with the General tab displayed.

b Configure the parameters:

- Description
- Administrative State

Note — If the 7210 SAS-E sites are connected in a ring network, you must configure an uplink SAP between each pair of 7210 SAS-E sites.

15 Click on the Port tab button.

16 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - VPLS L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

17 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form displays the port information.

18 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value

19 Create an L2 access interface on each 7210 SAS-E and terminating site. Perform steps 6 to 51 in Procedure 68-3, as required.

Note — Some steps and parameters in Procedure 68-3 do not apply to the 7210 SAS-E.

20 Click on the OK button. The VPLS Service (Create) form closes.

Procedure 68-3 To create a VPLS or MVPLS L2 access interface

Perform this procedure to create a VPLS or an MVPLS L2 access interface. Depending on the device type on which you configure an MVPLS, some tabs are not available.

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 64-14 for more information about deleting MSAPs.

Note — The following tab buttons are supported on the OS 9700E and OS 9800E NEs for the creation of a VPLS L2 access interface:

- General
- Port
- Forwarding Control
- Templates
- Faults

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Navigate to the Access Interfaces icon for the required site. The path is VPLS Service→Sites→Site→Access Interfaces.

6 Right-click on Access Interfaces and choose Create VPLS L2 Access Interface. The VPLS L2 Access Interface (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Description
- Administrative State
- Calling Station ID
- MC Ring Node
- PPPoE Circuit ID

8 On the Split Horizon Group panel, choose an SHG for the interface, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - VPLS L2 Access Interface list form opens.

Note — You must configure an SHG or residential SHG for a VPLS if you plan to create a spoke circuit from this VPLS site to a VLL or another VPLS.

ii Choose an SHG and click on the OK button. The Select Split Horizon Group Name - VPLS L2 Access Interface list form closes, and the VPLS L2 Access Interface (Create) form refreshes with the SHG name.

9 Configure the SAP Sub Type parameter.

Note — When you choose Capture as the SAP Sub Type, the displayed form changes to allow configuration of the Capture SAP. To create a Capture SAP, see Procedure 64-8.

10 Select an application profile for the L2 access interface.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - VPLS L2 Access Interface form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - VPLS L2 Access Interface form closes and VPLS L2 Access Interface (Create) form refreshes with the application profile information.

Note — The Application Profile String: - VPLS L2 Access Interface service form displays only local profiles on the NE.

11 Configure the parameters in the ETH-CFM MIP panel:

- MIP
- MIP MAC Address

Note — The MIP and MIP MAC Address parameters are configurable only when a port is assigned to the interface.

12 Click on the Port tab button.

13 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - VPLS L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

14 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form displays the port information.

Note — If you select an Ethernet Tunnel Endpoint, the Port form is refreshed and an Ethernet Tunnel tab is added.

15 If the L2 access interface is on a 7250 SAS-ES or 7250 SAS-ESA, configure the following parameters; otherwise, go to step 17:

- Encapsulation Tagging
- Set Default VLAN to VPLS Tag
- VPLS Mode

The VPLS Mode parameter is configurable on the first L2 access interface associated with a port on the 7250 SAS-ES or 7250 SAS-ESA, Release 3.0 R4 or later.

16 If the L2 access interface is on a 7250 SAS-ES or 7250 SAS-ESA, go to step 49.

17 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)

When the selected port uses Dot1 Q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for Dot1 Q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form.

If the port you have chosen is an Ethernet Tunnel Endpoint, you will be able to set the Outer Encapsulation Value to 8191. This automatically enables the Ethernet Tunnel Endpoint Control SAP parameter.

If you are configuring the port for an L2 Access Interface in a Control VPLS for an ethernet ring, the Outer Encapsulation Value and Inner Encapsulation Value for the port in each L2 Access Interface must have the same value as the R-APS Tag (Outer Encapsulation Value) and R-APS Tag (Inner Encapsulation Value) respectively, that you use for the particular path endpoint. This defines the interface as a Control SAP for the ethernet ring. Refer to Procedure 30-8 for additional information.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only when the port is an ATM port.

If the port you have chosen is an Ethernet port and uses ATM, Dot1 Q or Q in Q encapsulation, you can enable ingress VLAN translation, if required. Configure the parameters:

- Translation
- Translation ID

18 Configure the Ethernet Tunnel Endpoint Control SAP parameter, if required.

Note — Enabling the Ethernet Tunnel Endpoint Control SAP parameter creates the control L2 Access Interface (also known as a Control SAP). It also automatically sets the value of the Outer Encapsulation Value parameter to 8191.

If you are currently creating a same-fate SAP or an L2 Access Interface for an ethernet ring, the Ethernet Tunnel Endpoint Control SAP parameter must not be enabled.

19 Depending on the port that you have chosen, the Egress Multicast Group tab is configurable. Configure the EMG, if required.

i Click on the Egress Multicast Group tab button. The Select Egress Multicast Group-L2 Access Interface form opens.

ii Choose an EMG and click on the OK button. The Select Egress Multicast Group-L2 Access Interface form closes, and the Egress Multicast Group tab refreshes with the EMG name.

Note — The Egress Multicast Group-L2 Interface form lists only EMGs that have the same egress filter and encapsulation type as the interface.

20 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

Note — If you select a bundle in step 14, only the Scheduling Class parameter is configurable.

21 If you are creating this L2 Access Interface for the Control VPLS of an ethernet ring or for a data service using the ring, configure the ID parameter in the Ethernet Ring Element section to select the required Ethernet Ring Element. Refer to Procedure 30-7 for additional information.

22 Click on the QoS tab button to assign ingress and egress QoS policies to the interface, if required, and perform one of the following:

a To configure a 7750 SR, 7450 ESS, 7710 SR or 7705 SAR:

i Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use Shared Queue
- Use Multipoint Shared Queue
- HSMDA Packet Byte Offset (bytes)

The Use Shared Queue and Use Multipoint Shared Queue parameters are only configurable for non-HSMDA ports.

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is Dot1 Q, BCP Dot1 Q, or Q in Q.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service components tree, choosing Properties, and configuring the parameters on the appropriate tab.

ii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - VPLS L2 Access Interface form opens.

iii Choose an ingress QoS policy and click on the OK button. The Select Ingress Policy - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the ingress QoS policy name.

Note — If you choose an access ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access ingress queue group with the same name created on it.

See Procedure 17-61 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

iv Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - VPLS L2 Access Interface form opens.

v Choose an egress QoS policy and click on the OK button. The Select Egress Policy - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress QoS policy name.

Note — If you choose an access egress policy which has a forwarding class mapped to an egress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access egress queue group with the same name created on it.

See Procedure 17-61 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

vi Click on the Select button in the HSMDA Egress Secondary Shaper panel to choose an HSMDA egress secondary shaper policy. The Select HSMDA Egress Secondary Shaper form opens.

vii Choose a secondary shaper and click on the OK button. The Select HSMDA Egress Secondary Shaper form closes and the VPLS L2 Access Interface (Create) form reappears with the egress secondary shaper information displayed.

viii Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

ix Choose a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

x Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

xi Choose a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the VPLS L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

b To configure a 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], or 7210 SAS-X24F2XFP:

i Click on the Select button in the 7210 Specific panel to choose a SAS ingress policy. The Select SAS Ingress Policy - VPLS L2 Access Interface form opens.

ii Choose a SAS ingress policy and click on the OK button. The Select SAS Ingress Policy - VPLS L2 Access Interface form closes and the information is displayed.

Note — To support H-metering, you must choose a SAS ingress policy with all meter rate modes set to trtcm2.

iii Configure the following parameters in the Aggregate Rate Limit panel:

- Ingress Meter
- Ingress Meter Rate (kbps)
- Ingress Meter Burst

Note 1 — The Ingress Meter parameter is configurable only for the 7210 SAS-X24F2XFP during creation of a SAP. The parameter must be set to True to support H-metering.

Note 2 — For the 7210 SAS-X24F2XFP, the Ingress Meter Rate (kbps) and Ingress Meter Burst parameters can be modified only after a SAP is created.

23 Click on the Schedulers tab button to configure scheduling, if required; otherwise, go to step 27.

Note — The Schedulers tab is configurable only when a port is assigned to the interface.

24 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame-Based Accounting

Note 1 — The Egress Aggregate Rate Limit (kbps) and Frame-Based Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — You cannot specify an egress scheduler when the Egress Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - VPLS L2 Access Interface form opens.

iv Choose an ingress scheduler and click on the OK button. The Select Ingress Scheduler - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - VPLS L2 Access Interface form opens.

vi Choose an egress scheduler and click on the OK button. The Select Egress Scheduler - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

vii Go to step 27.

b Specify that an access scheduler policy is applied to the interface.

i Set the Aggregation parameter to on.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - VPLS L2 Access Interface form opens.

iii Choose an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

iv Go to step 27.

25 Click on the Aggregation Rate tab button to configure the aggregation rate, otherwise, go to step 27.

Note — The Aggregation Rate tab is configurable only when a port is assigned to the HSMDA SAP.

26 Configure the Aggregate Rate Limit (kbps) parameter in the Ingress Aggregate Rate Limit and Egress Aggregate Rate Limit panels.

27 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - VPLS L2 Access Interface form opens.

iii Choose an ingress ACL filter and click on the OK button. The Select Ingress Filter - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - VPLS L2 Access Interface form opens.

v Choose an egress ACL filter and click on the OK button. The Select Egress Filter - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress ACL filter name.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - VPLS L2 Access Interface form opens.

vii Choose an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - VPLS L2 Access Interface form closes and the VPLS L2 Access Interface (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - VPLS L2 Access Interface form opens.

ix Choose an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - VPLS L2 Access Interface form closes and the VPLS L2 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

28 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab button.

ii Click on the Select button to choose an accounting policy. The Select Accounting Policy - VPLS L2 Access Interface form opens.

iii Choose an accounting policy and click on the OK button. The Select Accounting Policy - VPLS L2 Access Interface form closes, and the VPLS L2 Access Interface (Create) form refreshes with the accounting policy name.

iv Configure the Collect Accounting Statistics parameter.

v If you are configuring statistics collection for a 7210 SAS-E, go to step vi. Otherwise, go to step 29.

vi Configure the parameters:

- Enable Egress Packets Forwarding
- Ingress Counter Mode

29 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab button.

ii Click on the Select button beside the Name parameter. The Select Time Of Day Suite - VPLS L2 Access Interface list form opens.

iii Choose a time of day suite and click on the OK button. The Select Time Of Day Suite - VPLS L2 Access Interface list form closes, and the VPLS L2 Access Interface (Create) form refreshes with the time of day suite name.

Note 1 — You cannot assign a ToD suite to a L2 access interface if accounting statistics collection is enabled on the L2 access interface; you must first disable the Collect Accounting Statistics parameter in step 28.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics will only be collected if a Time Of Day Suite is applied on the SAP.

30 Configure BPDU Termination, STP and FIB parameters for the interface, if needed.

i Click on the Forwarding Control tab button. Depending on the device being configured, the BPDU Termination tab is displayed. Otherwise, go to step iii.

ii Configure the parameters:

- L2 Protocol Termination

  When the L2 Protocol Termination parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.
- BPDU Translation
- Force L2PT on Managed L2 Access Interface

  The Force L2PT on Managed L2 Access Interface parameter is only available for MVPLS L2 access interfaces. When the Force L2PT on Managed L2 Access Interface parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.

iii Click on the STP tab button.

iv Configure the parameters:

- Path Cost
- Port Number
- Priority
- Edge Port
- Edge Capability Detection
- Link Type
- Root Guard
- Administrative State

v Click on the FIB tab button.

vi Configure the parameters:

- Aging Enabled
- Learning Enabled
- Maximum Entries
- Limit Mac Move
- Limit Mac Move Level
- Discard Unknown Source
- Restrict Protected Source
- Restrict Protected Source Action
- Restrict Unprotected Destination

vii If you are creating an MVPLS to run MSTP, the MST Instances tab button is configurable. Otherwise, go to step 31.

viii Click on the MST Instances tab button to edit a SAP MST instance.

ix Select an MST instance and click on the Properties button.

x The L2 Access Interface MST Instance (Edit) form opens. Configure the parameters:

- Path Cost
- Priority

xi Click on the OK button to close the L2 Access Interface MST Instance (Edit) form. A dialog box appears.

xii Click on the OK button. The L2 Access Interface (Create) form refreshes with the new MST instance.

31 Configure residential subscriber management for the interface, if required.

i Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

ii Select the SHCV Enabled parameter to enable SHCV, if required. Otherwise, go to step x.

iii Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source IP Address
- SHCV Source MAC Address
- SHCV Action
- SHCV Retry Timeout (seconds)
- SHCV Retry Count

iv Click on the IGMP Host Tracking tab button.

v Click on the Select button to choose the import policy used to filter IGMP packets. The Select SapIgmpHostTracking form opens.

vi Configure the filter criteria and click on the Search button. A list of import policies appears.

vii Choose a policy and click on the OK button. The selected import policy name appears.

viii Configure the parameters:

- Expiry Time
- Max Number of Groups
- Max Number of Sources per Group

ix Click on the Host Tracking Info tab button to view a list of hosts that are being tracked on this L2 access interface.

x Click on the Profiles tab button.

xi Configure the parameters:

- Admin Status
- Service Model
- Subscriber Limit
- Default Subscriber Identification Type
- Default Subscriber Id
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id
- Profiled Traffic only
- Non-Subscriber Traffic Identification
- LAG link selection

xii Click on the Select button in the Default Subscriber Profile panel to choose a default subscriber profile for the interface, if required. The Select Default Subscriber Profile form opens with the list of available subscriber profiles displayed.

xiii Choose a subscriber profile and click on the OK button. The Select Default Subscriber Profile form closes, and the subscriber profile name appears in the Default Subscriber Profile panel.

xiv Click on the Select button in the Default SLA Profile panel to choose a Default SLA profile for the SAP, if required. The Select Default SLA Profile form opens with the list of available SLA profiles displayed.

xv Choose an SLA profile and click on the OK button. The Select Default SLA Profile form closes, and the SLA profile name appears in the Default SLA Profile panel.

xvi Click on the Select button in the Subscriber Identification Policy panel to choose a subscriber identification policy for the SAP, if required. The Select Subscriber Identification Policy form opens with the list of available subscriber identification policies displayed.

xvii Choose a subscriber identification policy and click on the OK button. The Select Subscriber Identification Policy form closes, and the subscriber identification policy name appears in the Subscriber Identification Policy panel.

xviii Click on the Select button in the Default Application Profile panel to choose a default application profile for the SAP, if required. The Select Default Application Profile form opens with the list of application profiles on the NE displayed.

xix Choose an application profile and click on the OK button. The Select Default Application Profile form closes, and the application profile name appears in the Default Application Profile panel.

xx Click on the Select button in the Non-Subscriber Traffic Subscriber Profile panel to choose a non-subscriber subscriber profile for the SAP, if required. The Select Non-Subscriber Traffic Subscriber Profile form opens with the list of available subscriber profiles displayed.

xxi Choose a subscriber profile and click on the OK button. The Select Non-Subscriber Traffic Subscriber Profile form closes, and the subscriber profile name appears in the Non-Subscriber Traffic Subscriber Profile panel.

xxii Click on the Select button in the Non-Subscriber Traffic SLA Profile panel to choose a Non-Subscriber Traffic SLA profile for the SAP, if required. The Select Non-Subscriber Traffic SLA Profile form opens with the list of available SLA profiles displayed.

xxiii Choose an SLA profile and click on the OK button. The Select Non-Subscriber Traffic SLA Profile form closes, and the SLA profile name appears in the Non-Subscriber Traffic SLA Profile panel.

xxiv Click on the Select button in the Non-Subscriber Traffic Application Profile panel to choose a non-subscriber traffic application profile for the SAP, if required. The Select Non-Subscriber Traffic Application Profile form opens with the list of application profiles on the NE displayed.

xxv Choose an application profile and click on the OK button. The Select Non-Subscriber Traffic Application Profile form closes, and the application profile name appears in the Non-Subscriber Traffic Application Profile panel.

32 Assign a DoS protection policy to the interface, if required.

Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - VPLS L2 Access Interface form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - VPLS L2 Access Interface form closes and the policy ID is displayed on the VPLS L2 Access Interface (Create) form.

iv Configure the MAC Monitoring parameter.

33 Configure an ethernet tunnel.

Note — You can only configure ethernet tunnel SAP path parameters if you are creating a same-fate SAP.

i Click on the Ethernet Tunnel tab.

ii If you are configuring a fate-sharing Ethernet Tunnel Endpoint SAP (also referred to as same-fate SAP) then go to step iii. Otherwise, go to step 34.

iii Click on the Add button. The Ethernet Tunnel (Create) form opens.

iv Configure the parameters:

- Path ID
- Tag (Outer Encapsulation Value)
- Tag (Inner Encapsulation Value)

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The VPLS L2 Access Interface (Create) form refreshes with the Ethernet Tunnel entry.

34 Configure a redundant VLAN range, if required.

Note — If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation. The redundant VLAN range defines the range of VC IDs for VPLS SAPs that the MVPLS manages.

i Click on the Redundancy tab button.

ii Click on the Add button. The RedundantVlanRange (Create) form opens.

iii Configure the parameters:

- Min VLAN ID
- Max VLAN ID

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The VPLS L2 Access Interface (Create) form refreshes with the redundant VLAN range entry.

35 The ATM tab is configurable when the interface port is an ATM port. Specify OAM functionality and assign ingress and egress ATM policies to the interface, if required.

i Click on the ATM tab button.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Choose an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes, and the VPLS L2 Access Interface (Create) form refreshes with the ingress ATM policy name.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Choose an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes, and the VPLS L2 Access Interface (Create) form refreshes with the egress ATM policy name.

36 Configure IGMP snooping for the interface, if required.

i Click on the IGMP Snooping tab button. The General tab is displayed.

ii Configure the parameters as they apply to a specific NE:

- Import Policy
- Fast-leave
- Mrouter attached
- Send Queries
- General Query Interval (seconds)
- Maximum Response Interval (seconds)
- Robust Count
- IGMP Version
- Last Member Query Interval (tenths of seconds)
- Maximum Number of Groups
- Max.number of sources per group

The General query interval (seconds), Max. Response interval (seconds), Robust count, and IGMP Version parameters are configurable when the Send queries parameter is enabled.

iii Click on the Select button in the Mcast CAC panel to choose a multicast CAC policy, if required. The Select Multicast CAC Policy form opens with the list of available multicast CAC policies displayed.

iv Choose a multicast CAC policy and click on the OK button. The Select Multicast CAC Policy form closes and the multicast CAC policy information appears on the VPLS L2 Access Interface (Create) form.

v Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)

vi Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 38.

vii Click on the Add button. The Access Interface Igmp Snooping Mcast Group Display (Create) form opens.

viii Configure the parameters:

- Group Address
- Source Address

ix Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step xii.

x Click on the OK button.

xi Repeat steps vii to ix to create an additional entry, if required.

xii Click on the OK button. A dialog box appears.

xiii Click on the OK button. The Static Mcast Group tab refreshes with the new multicast group entries.

37 Configure the ARP host for the interface, if required.

i Click on the ARP Host Configuration tab button.

ii Configure the parameters:

- Administrative State
- ARP Host Limit
- Minimum Authentication Interval

38 Configure DHCP for the interface, if required.

i Click on the DHCP tab button. The General tab is displayed.

ii Configure the parameters:

- Administrative State
- Description
- Snooping
- Enable
- Enable Lease Populate
- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String

The Enable Lease Populate parameter is configurable when the Enable parameter is enabled.

The Remote ID String parameter is configurable when the Remote ID parameter is set to Remote IDString.

iii Depending on the type and version of the device that you are configuring, the Subscriber Authentication Policy panel appears. Otherwise, go to step vii.

iv Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - L2 Access I/F DHCP Relay Config form opens.

v Click on the Search button.

vi Choose a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - L2 Access I/F DHCP Relay Config form closes, and the VPLS L2 Access Interface (Create) form refreshes with the subscriber authentication policy name.

vii Click on the Server tab button to configure the VPLS L2 access interface proxy server.

Note — You can configure a VPLS L2 access interface proxy server on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7450 ESS, 7750 SR, and 7710 SR.

viii Configure the parameters:

- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time RADIUS Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

39 Depending on the type of device that you are configuring, the MVR tab is configurable. Configure MVR for the SAP, if required.

i Click on the MVR tab button.

ii Click on the Select button in the Source MVR VPLS panel to associate an MVR VPLS with the SAP. The Select Source MVR VPLS form opens.

iii Choose a source MVR VPLS and click on the OK button. The Select Source MVR VPLS closes, and the VPLS L2 Access Interface (Create) form refreshes with the source MVR VPLS information.

iv Click on the Select button in the Proxy MVR SAP panel to choose a proxy MVR SAP to which the multicast traffic will be sent. The Select Proxy MVR SAP form opens.

v Choose a proxy MVR SAP and click on the OK button. The Select Proxy MVR SAP form closes, and the VPLS L2 Access Interface (Create) form refreshes with the proxy MVR SAP information.

Note — If the SAP already has an MVR proxy SAP or is the MVR proxy SAP of another SAP, the SAP cannot be an MVR proxy SAP.

40 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the parameters:

- Anti-Spoofing
- ARP Reply Agent
- MAC Pinning

The ARP Reply Agent parameter is configurable only when an IP address is specified for the static hosts on the SAP.

iii Click on the Static Hosts tab button to configure a static subscriber host entry for each subscriber host that is not managed by DHCP. Otherwise, go to step 42.

iv Click on the Add button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

v Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification
- Use SAP ID as Subscriber ID
- ANCP String
- Intermediate Destination ID

Note — You must specify at least one IP address or MAC address for each static host. The values that are specified for the Anti-Spoofing and ARP Reply Agent parameters determine the type of address entry that is required for the static host. For example, if you set the Anti-Spoofing parameter to Source Ip Addr, you must specify at least the IP address for the static host.

vi Configure residential subscriber management for the static host, if required. Otherwise, go to step 42.

vii Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with the list of available subscriber profiles displayed. Otherwise, go to step ix.

viii Choose a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

ix Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host, if required. The Select SLA Profile - AntiSpoofingStaticHosts form opens with the list of available SLA profiles displayed. Otherwise, go to step xiii.

x Choose an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

xi Click on the Select button in the Application Profile panel to choose an application profile for the static host, if required. The Select Application Profile - AntiSpoofingStaticHosts form opens with the list of application profiles on the NE displayed. Otherwise, go to step xiii.

xii Choose an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

xiii Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step xvi.

xiv Click on the OK button.

xv Repeat steps v to xiv for each additional entry that you want to create.

xvi Click on the OK button. A dialog box appears.

xvii Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes, and the VPLS L2 Access Interface (Create) form refreshes with the new static host entries in a list.

41 Specify the queue overrides.

i Click on the Override tab button.

Note — The Override tab contains four sub-tabs: Access Ingress Queue, Access Egress Queue, Access Ingress HSMDA Queue, and Access Egress HSMDA Queue. However, only two of the four are active, depending on the port type you have chosen for this interface.

If you configured an HSMDA port, then the Access Ingress HSMDA Queue and Access Egress HSMDA Queue sub-tabs are active. If you configured a non-HSMDA port, then the Access Ingress Queue and Access Egress Queue sub-tabs are active.

ii Set the queue overrides, as described in Procedure 44-40.

42 Associate a MEP with the L2 Access interface, if required.

i Click on the MEPs tab button.

ii Click on the Add button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step x.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

x Click on the OK button. The MEP (Create) form closes.

Note — If you have configured a SAP, the SAP information is filled in when you configure the MEP.

43 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button.

ii Click on the Add button. The ANCP Static Map (Create) form opens.

iii Configure the ANCP String parameter.

iv Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. The ANCP Static Map form closes.

44 Click on the MIPs tab button.

45 Perform one or more of the following, if required:

a Click the Search button to list available MIPs.

b View the current status of a specific MIP entry.

i Select a MIP from the list.

ii Click the Properties button to display the MIP information.

c Click the Resync button to resync the latest MIPs configured on the node.

46 Configure PIM snooping for the interface, if required.

i Click on the PIM Snooping tab button. The General tab is displayed.

ii Configure the Max Number of Groups parameter.

iii Click on the OK button.

47 Configure MLD snooping for the interface, if required.

i Click on the MLD Snooping tab button. The General tab is displayed.

ii Configure the parameters:

- Import Policy
- Fast-leave
- Mrouter attached
- Send queries
- General query interval (seconds)
- Max. Response interval (seconds)
- Robust count
- MLD version
- Max. Response interval group queries (tenths of seconds)
- Max. number of groups

The General query interval (seconds), Max. Response interval (seconds), Robust count, and MLD version parameters are configurable when the Send queries parameter is enabled.

iii Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 48.

iv Click on the Add button. The Access Interface Mld Snooping Mcast Group Display (Create) form opens.

v Configure the parameters:

- Group Address
- Source Address

vi Click on the Apply button if you want to create an additional entry. A dialog box appears. Otherwise, go to step ix.

vii Click on the OK button.

viii Repeat steps v to vii to create additional entries, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Static Mcast Group tab refreshes with the new multicast group entries.

48 Depending on the type of device that you are configuring, the MVR (MLD) tab is configurable. Use the MVR (MLD) tab to use MLD snooping on the SAP. Configure MVR for the SAP, if required.

i Click on the MVR (MLD) tab button.

ii Click on the Select button in the Source MVR VPLS panel to associate an MVR VPLS with the SAP. The Select Source MVR VPLS form opens.

iii Choose a source MVR VPLS and click on the OK button. The Select Source MVR VPLS closes, and the VPLS L2 Access Interface (Create) form refreshes with the source MVR VPLS information.

iv Click on the Select button in the Proxy MVR SAP panel to choose a proxy MVR SAP to which the multicast traffic will be sent. The Select Proxy MVR SAP form opens.

v Choose a proxy MVR SAP and click on the OK button. The Select Proxy MVR SAP form closes, and the VPLS L2 Access Interface (Create) form refreshes with the proxy MVR SAP information.

Note — If the SAP already has an MVR proxy SAP or is the MVR proxy SAP of another SAP, the SAP cannot be an MVR proxy SAP.

49 Click on the OK button. The VPLS L2 Access Interface (Create) form closes and a dialog box appears.

50 Click on the OK button. The VPLS (Create) form reappears.

51 Repeat steps 6 to 50 for each additional access interface that you want to create.

52 Click on the OK button. A dialog box appears.

53 Click on the Yes button. The VPLS (Create) form closes.

Procedure 68-4 To create a VPLS mesh SDP binding

The value of the Automatic Mesh SDP Binding Creation parameter in step 4 of Procedure 68-1 determines the way that mesh SDP binding creation occurs in the VPLS.

Note — The following tab buttons are supported on the OS 9700E and OS 9800E NEs for the creation of a mesh SDP binding:

- General
- Return
- States
- Frame Sizes
- Forwarding Control
- Templates
- Faults

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Navigate to the Mesh SDP Bindings icon for the required site. The path is VPLS→Site→Mesh SDP Bindings.

6 Right-click on Mesh SDP Bindings below the site and choose Create Mesh SDP Binding. The Mesh SDP Binding (Create) form opens with the General tab displayed.

7 If automatic mesh SDP binding creation is enabled on the VPLS, a dialog box appears. The message in the dialog box discourages manual mesh SDP binding creation when automatic mesh SDP binding creation is specified for a VPLS. Perform one of the following.

   a Choose not to override automatic SDP binding creation. Alcatel-Lucent recommends this action.

      i Click on the No button.

      ii Click on the cancel button to abort the operation and close the VPLS management form.

   b Choose to override automatic SDP binding creation. Alcatel-Lucent does not recommend this action.

      i Click on the Yes button. The Mesh SDP Binding (Create) form opens.

      ii Consult an Alcatel-Lucent technical representative before proceeding.

8 Specify a destination node for the mesh SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Mesh SDP Binding form opens.

ii Select a destination node and click on the OK button. The Select Destination Network Element - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

9 Configure the parameters:

- VC Type
- VLAN VC Tag
- Ingress Label
- Egress Label

10 Perform one of the following to specify a transport tunnel for the mesh SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Mesh SDP Binding form opens.

ii Select a service tunnel for the mesh SDP binding and click on the OK button. The Select Tunnel - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the service tunnel identifier.

11 Configure the parameters:

- Egress Label
- Enable Hash Label
- Force VLAN VC Forwarding

Note — The Force VLAN VC Forwarding parameter does not appear if you are creating a Mesh SDP binding for a B-site.

12 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

a Let the 5620 SAM configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Mesh SDP Binding form opens.

iii Select a service tunnel for the mesh SDP binding and click on the OK button. The Select Return Tunnel - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

13 Specify whether the mesh SDP binding is in or out of service.

i Click on the States tab button.

ii Configure the Administrative State parameter.

14 Click on the Pseudowire OAM tab button.

15 Configure the Control Word parameter.

16 Assign ingress and egress ACL filters to the mesh SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Mesh SDP Binding form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Mesh SDP Binding form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the egress ACL filter name.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - Mesh SDP Binding form opens.

vii Select an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - Mesh SDP Binding form opens.

ix Select an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - Mesh SDP Binding form closes and the Mesh SDP Binding (Create) form reappears with the IPv6 egress ACL filter information displayed.

17 Configure anti-spoofing for the mesh SDP binding, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the MAC Pinning parameter.

18 Assign an accounting policy to the mesh SDP binding, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Mesh SDP Binding form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - Mesh SDP Binding form closes, and the Mesh SDP Binding (Create) form refreshes with the accounting policy name.

19 Click on the Forwarding Control tab button if you need to add or delete MFIB allowed daughter cards or configure MRP, otherwise go to step 20.

Note 1 — The single-slot models of the 7450 ESS and 7750 SR support the addition or deletion of MFIB allowed daughter cards.

Note 2 — The MFIB Allowed Daughter Card tab does not appear if you are creating a Mesh SDP binding for a B-site.

i Click on the MFIB Allowed Daughter Card tab button.

ii Click on the Add button. The SDP Binding MFIB Allowed Daughter Card (Create) form opens.

iii Click on the Select button. The Select Daughter Card form opens. Select a daughter card and click OK. The Select Daughter Card form closes.

iv Click on the OK button. The SDP Binding MFIB Allowed Daughter Card (Create) form closes and a dialog box appears.

v Click on the OK button. The Mesh SDP Binding (Create) form displays the new allowed daughter card in the list.

vi Click on the MRP tab if you are configuring a Mesh SDP binding for a B-site.

vii Configure the parameters:

- MRP Join Time (tenths of a second)
- MRP Leave Time (tenths of a second)
- MRP Leave AllTime (tenths of a second)
- MRP Periodic Time (tenths of a second)
- MRP Periodic Enabled

viii Click on the Select button to select an PBB MRP Policy. The Select PBB MRP Policy form opens.

ix Choose the desired policy and click OK.

20 Configure DHCP for the mesh SDP binding, if required.

i Click on the DHCP tab button.

Note — The DHCP tab does not appear if you are creating a Mesh SDP binding for a B-site.

ii Configure the parameters:

- Description
- Snooping

21 Configure IGMP Snooping for the mesh SDP binding, if required.

i Click on the IGMP Snooping tab button.

Note — The IGMP Snooping tab does not appear if you are creating a Mesh SDP binding for a B-site.

ii Configure the parameters:

- Import Policy
- Fast-leave
- Mrouter attached
- Send queries
- General query interval (seconds)
- Max. Response interval (seconds)
- Robust count
- IGMP Version
- Max. Response interval group queries (tenths of seconds)
- Max. number of groups

The General query interval (seconds), Max. Response interval (seconds), Robust count, and IGMP Version parameters are configurable when the Send queries parameter is enabled.

iii Configure a multicast CAC policy, if required. Otherwise, go to step 24.

iv Click on the Select button. The Select Multicast CAC Policy form opens.

v Select a multicast CAC policy from the list and click on the OK button. The Select Multicast CAC Policy form closes.

vi Click on the Properties button to edit the existing multicast CAC policy, if required. See chapter 46 for information about creating a multicast CAC policy.

vii Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)

22 Associate a MEP with the mesh SDP binding, if required.

i Click on the MEPs tab button.

ii Click on the Add button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step x.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

x Click on the OK button. The MEP (Create) form closes.

23 Configure MLD Snooping for the mesh SDP binding, if required.

i Click on the MLD Snooping tab button. The General tab is displayed.

Note — The MLD Snooping tab does not appear if you are creating a Mesh SDP binding for a B-site.

ii Configure the parameters:

- Import Policy
- Fast-leave
- Mrouter attached
- Send queries
- General query interval (seconds)
- Max. Response interval (seconds)
- Robust count
- MLD version
- Max. Response interval group queries (tenths of seconds)
- Max. number of groups

The General query interval (seconds), Max. Response interval (seconds), Robust count, and MLD version parameters are configurable when the Send queries parameter is enabled.

iii Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 24.

iv Click on the Add button. The Circuit Mld Snooping Mcast Group Display (Create) form opens.

v Configure the parameters:

- Group Address
- Source Address

vi Click on the Apply button if you want to create an additional entry. A dialog box appears. Otherwise, go to step ix.

vii Click on the OK button.

viii Repeat steps v to vii to create additional entries, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Static Mcast Group tab refreshes with the new static multicast group entries in a list.

24 Click on the OK button. The Mesh SDP Binding (Create) form closes, and a dialog box appears.

25 Click on the OK button. The VPLS (Edit) form reappears.

26 Repeat steps 6 to 25 for each additional mesh SDP binding that you want to create.

27 Click on the OK button. A dialog box appears.

28 Click on the Yes button. The VPLS (Edit) form closes.

29 Close the Manage Services form.

Procedure 68-5 To create a VPLS spoke SDP binding

Note 1 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP. Likewise, you cannot enable MSTP for a site that has a spoke SDP binding, or on a SAP with a non-zero encapsulation value.

Note 2 — For services employing BGP AD and BGP VPLS: You should create SDP bindings manually at non-BGP AD or BGP VPLS enabled sites, or to other BGP AD or BGP VPLS sites where auto-created pseudowires are not expected to be created.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 If you are creating a redundant spoke SDP binding under an endpoint, go to step 6. Otherwise go to step 8.

Note — Redundant spoke SDP bindings under an endpoint are only valid for VPLS regular sites and B-Sites. They do not apply to I-Sites.

6 Select an endpoint for the required site.

7 Right-click on Spoke SDP Bindings below the endpoint and choose Create Spoke SDP Bindings. The Spoke SDP Binding (Create) form opens with the General tab displayed. Go to step 10.

8 Navigate to the Spoke SDP Bindings icon for the required site. The path is VPLS→Site→Spoke SDP Bindings.

9 Right-click on Spoke SDP Bindings below the site and choose Create Spoke SDP Bindings. The Spoke SDP Binding (Create) form opens with the General tab displayed.

10 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Select a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

11 Configure the parameters:

- Auto-Assign ID
- VC ID
- VC Type
- MTU
- VLAN VC Tag
- Ingress Label
- Egress Label

Note — The MTU parameter does not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site.

12 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

Note 1 — If you are creating a Spoke SDP binding for a B-site, the Tunnel Auto-Selection Transport Preference must be either MPLS:LDP or MPLS:RSVP. For I-sites, you can use MPLS:LDP, MPLS:RSVP, GRE, or Any.

Note 2 — The Auto Select Transport Tunnel parameter supports only values of Any or MPLS:RSVP on a Spoke SDP binding that originates from 7250 SAS-ES or 7250 SAS-ESA sites.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

13 If you are creating the spoke SDP binding for a B-Site or an I-Site, go to step 18.

14 If you are configuring a spoke SDP binding that originates from a 7250 SAS-ES or 7250 SAS-ESA perform the following steps:

i Configure the Active State parameter.

ii Go to step 36.

15 If you are creating the spoke SDP binding under an endpoint, go to step 17.

16 Click on the Select button in the Redundancy panel to select the desired endpoint from the drop-down menu.

17 Configure the parameters:

- Ignore Standby Signalling
- Precedence

18 Choose an SHG for the spoke SDP binding, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - Spoke SDP Binding form opens.

Note — You must configure an SHG or residential SHG on a spoke SDP binding for an HVPLS that includes another VPLS or a VLL service.

ii Select an SHG and click on the OK button. The Select Split Horizon Group Name - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the SHG name.

19 Configure the parameters:

- Enable Hash Label
- Force VLAN VC Forwarding
- MIP

Note — The Force VLAN VC Forwarding parameter do not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site.

20 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note 1 — You can create a return tunnel only between sites that are in the same service. If the sites are not in the same service, the Return tab does not appear.

Note 2 — If you are creating a Return SDP binding for a B-site, the Return Tunnel Auto-Selection Transport Preference must be either MPLS:LDP or MPLS:RSVP. For I-sites, you can use MPLS:LDP, MPLS:RSVP, GRE, or Any.

a Let the 5620 SAM configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

21 Select an application profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an Application Profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding - VPLS service form displays only local profiles on the NE.

22 Specify whether the spoke SDP binding is in or out of service.

i Click on the States tab button.

ii Configure the Administrative State parameter.

iii Configure the Block On Mesh Failure parameter.

Note — The Block On Mesh Failure parameter does not appear if you are creating a Spoke SDP binding for a B-site or an I-site.

23 Click on the Pseudowire OAM tab button.

24 Configure the Control Word parameter.

25 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the egress ACL filter name.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - Spoke SDP Binding form opens.

vii Select an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - Spoke SDP Binding form opens.

ix Select an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the IPv6 egress ACL filter information displayed.

26 Configure anti-spoofing for the spoke SDP binding, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the MAC Pinning parameter.

27 Assign an accounting policy to the spoke SDP binding, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the accounting policy name.

28 Configure BPDU Termination, STP, FIB, MRP, and MFIB Allowed Daughter Card parameters for the spoke SDP binding, if required.

i Click on the Forwarding Control tab button. Depending on the device being configured, the BPDU tab is displayed.

ii Configure the parameters:

- L2 Protocol Termination
- BPDU Translation

iii Click on the STP tab button.

iv Configure the parameters:

- Path Cost
- Port Number
- Priority
- Edge Port
- Edge Capability Detection
- Link Type
- Administrative State

v Click on the FIB tab button.

vi Configure the parameters:

- Aging Enabled
- Learning Enabled
- Maximum Entries
- Limit Mac Move
- Limit Mac Move Level
- Discard Unknown Source

Note — The Maximum Entries parameter does not appear if you are creating a Spoke SDP binding for a B-site.

vii Click on the MFIB Allowed Daughter Card tab button to configure allowed daughter cards; otherwise, go to step 29.

Note 1 — The MFIB Allowed Daughter Card tab does not appear if you are creating a Spoke SDP binding for a B-Site.

Note 2 — The single-slot models of the 7450 ESS and 7750 SR support the addition or deletion of MFIB allowed daughter cards.

viii Click on the Add button. The SDP Binding MFIB Allowed Daughter Card (Create) form opens.

ix Click on the Select button. The Select Daughter Card form opens.

x Select a daughter card in the list and click on the OK button. The Select Daughter Card form closes.

xi Click on the OK button. The SDP Binding MFIB Allowed Daughter Card (Create) form closes and the MFIB Allowed Daughter Card tab displays the newly-added daughter card in the list.

xii Click on the MRP tab if you are configuring a Spoke SDP binding for a B-site.

Note — The MRP tab does not appear if you are creating a Spoke SDP binding for an I-site.

xiii Configure the parameters:

- MRP Join Time (tenths of a second)
- MRP Leave Time (tenths of a second)
- MRP Leave AllTime (tenths of a second)
- MRP Periodic Time (tenths of a second)
- MRP Periodic Enabled

xiv Click on the Select button to select an PBB MRP Policy. The Select PBB MRP Policy form opens.

xv Choose the desired policy and click OK.

29 Configure IGMP Snooping for the spoke SDP binding, if required.

Note — The IGMP Snooping tab does not appear if you are creating a Spoke SDP binding for a B-Site.

i Click on the IGMP Snooping tab button. The General tab is displayed.

ii Configure the parameters:

- Import Policy
- Fast-leave
- Mrouter attached
- Send queries
- General query interval (seconds)
- Max. Response interval (seconds)
- Robust count
- IGMP Version
- Max. Response interval group queries (tenths of seconds)
- Max. number of groups
- Max.number of sources per group

The General query interval (seconds), Max. Response interval (seconds), Robust count, and IGMP Version parameters are configurable when the Send queries parameter is enabled.

iii If you are creating this spoke SDP binding for a B-Site or an I-Site, go to step viii.

iv Configure a multicast CAC policy, if required. Otherwise, go to step 30.

v Click on the Select button. The Select Multicast CAC Policy form opens.

vi Select a multicast CAC policy from the list and click on the OK button. The Multicast CAC Policy form closes.

vii Configure the parameters:

- Unconstrained Bandwidth (kbps)
- Mandatory Bandwidth (kbps)

viii Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 30.

ix Click on the Add button. The Circuit Igmp Snooping Mcast Group Display (Create) form opens.

x Configure the parameters:

- Group Address
- Source Address

xi Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step xiv.

xii Click on the OK button.

xiii Repeat steps x to xii to create additional entries, if required.

xiv Click on the OK button. A dialog box appears.

xv Click on the OK button. The Static Mcast Group tab refreshes with the new static multicast group entries in a list.

30 Configure DHCP for the spoke SDP binding, if required.

Note — The DHCP tab does not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site.

i Click on the DHCP tab button.

ii Configure the parameters:

- Description
- Snooping

31 Associate a MEP with the spoke SDP binding, if required.

i Click on the MEPs tab button.

ii Click on the Add button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step x.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

x Click on the OK button. The MEP (Create) form closes.

32 Click on the MIPs tab button.

33 Perform one or more of the following, if required:

a Click the Search button to list available MIPs.

b View the current status of a specific MIP entry.

i Select a MIP from the list.

ii Click the Properties button to display the MIP information.

c Click the Resync button to resync the latest MIPs configured on the node.

34 Configure PIM snooping for the spoke SDP binding, if required.

i Click on the PIM Snooping tab button. The General tab is displayed.

Note — The PIM Snooping tab does not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site.

ii Configure the Max Number of Groups parameter.

iii Click on the OK button.

35 Configure MLD Snooping for the spoke SDP binding, if required.

i Click on the MLD Snooping tab button. The General tab is displayed.

Note — The MLD Snooping tab does not appear if you are creating a Spoke SDP binding for a B-Site or an I-Site.

ii Configure the parameters:

- Import Policy
- Fast-leave
- Mrouter attached
- Send queries
- General query interval (seconds)
- Max. Response interval (seconds)
- Robust count
- MLD version
- Max. Response interval group queries (tenths of seconds)
- Max. number of groups

The General query interval (seconds), Max. Response interval (seconds), Robust count, and MLD version parameters are configurable when the Send queries parameter is enabled.

iii Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 30.

iv Click on the Add button. The Circuit Mld Snooping Mcast Group Display (Create) form opens.

v Configure the parameters:

- Group Address
- Source Address

vi Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step ix.

vii Click on the OK button.

viii Repeat steps v to vii to create additional entries, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Static Mcast Group tab refreshes with the new static multicast group entries in a list.

36 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

37 Click on the OK button. The VPLS (Edit) form reappears.

38 Repeat steps 9 to 37 for each additional spoke SDP binding that you want to create.

39 Click on the OK button. A dialog box appears.

40 Click on the Yes button. The VPLS (Edit) form closes.

41 Close the Manage Services form.

Procedure 68-6 To configure a site for BGP AD or BGP VPLS

This workflow and procedure lists the steps required to enable BGP Auto Discovery or configure BGP VPLS on a VPLS site.

- BGP AD enables a VPLS PE router to discover other PE routers that are part of the same VPLS domain. T-LDP based label signaling is used for the pseudowire.
- BGP VPLS provides the mechanism for service member auto-discovery based on Route Target. MP-BGP based label signaling is used for the pseudowire.

Note 1 — This procedure can only be performed for an existing site, not during the creation of a new site.

Note 2 — BGP AD and BGP VPLS implementations only apply to regular VPLS sites and B-Sites, but not to I-Sites. For BGP VPLS, the B-Site cannot be used as a backbone for an I-Site or Epipe.

1 Prior to configuring a site for BGP AD or BGP VPLS, you must complete the following actions:

a Create a routing policy to define the required community members. See Procedure 27-8. This defines the VSI Import/Export Routing Targets.

b Enable BGP on the routing instance of each NE in the VPLS or BGP VPLS. See Procedure 28-1 for more information.

c Configure global-level BGP on each NE in the VPLS or BGP VPLS. See Procedure 28-2 for more information. The following items are required for BGP AD implementation.

- On the VPN tab of the Routing Instance form, you must enable the L2 VPN parameter in the Family block and in the Rapid Update Address Family block.
- Create a peer group under BGP. This peer group is used to collectively define the peers involved in the VPLS.
- Create the required peers under the peer group. These peers are the NEs involved in the VPLS.

d Create a PW template. See chapter 49 for information about PW templates.

e Distribute the PW Template to each NE that is or will be a component of the VPLS or BGP VPLS.

2 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

3 Configure the filter criteria. A list of services appears.

4 Select a VPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

5 Click on the Components tab button.

6 Right-click on the required site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

7 Click on the BGP tab button.

8 Configure the Route Distinguisher parameter.

9 Click the Configuration button to configure the Route Targets and the PW Templates. The BGP Configuration form opens, with the VSI Import Policies tab page displayed.

a Select up to five import policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

b Perform one of the following:

i Enter the Import Route Target name manually in the provided field. The format be “target:x:y”.

ii Click on the Import Route Target Select button. The Select ...-BGP Info form opens. Click on the Search button to display the available import route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select ...-BGP Info form closes.

c Click on the VSI Export Policies tab and select up to five export policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

d Perform one of the following:

i Enter the Export Route Target name manually in the provided field. The format must be “target:x:y”.

ii Click on the Export Route Target Select button. The Select ...-BGP Info form opens. Click on the Search button to display the available export route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select ...-BGP Info form closes.

e Click on the PW Template Binding tab button.

f Perform one of the following:

i To use an existing PW Template Binding, go to step g.

ii To add a new PW Template Binding, go to step h.

g For an existing PW Template Binding:

i Click the Search button. A list of applicable PW Template Bindings is displayed.

ii Select the required entry or entries from the list.

iii Go to step i.

h To create a new PW Template Binding:

i Click the Add button. The PW Template Binding (Create) form opens with the General tab page displayed.

ii Enter a Split Horizon Group name, if required.

iii Click the Select button. The Select PW Template form is displayed.

iv Click the Search button. A list of applicable PW Templates is displayed.

v Select the PW Template you created in step 1.

vi Click OK to accept the selection. The Select PW Template form close and the Policy ID field is populated by your choice.

vii Click on the PW Templates Binding Route Target tab and click the Add button. The PW Template Binding Route Target (Create) form is displayed.

Note — This Route Target is used by the NE to decide which PW Template to use to create SDP bindings. If a far-end neighbor has a matching export target (that is, to the PW Template Import Target being defined here), then this PW Template is selected by the NE to create the pseudowire that is used to link both sites of the VPLS. If nothing is entered, and multiple PW Templates are defined, the first one found by the NE is used (most likely the one with the lowest PW Template Policy ID).

Enter the required Route Target in the field and click OK. The PW Template Binding Route Target (Create) form closes and the entered Route Target is displayed in the table on the PW Template Binding Route Target tab.

viii Click OK to accept the selection. The PW Template Binding (Create) form closes and the new PW Template Binding is displayed in the table on the PW Template Binding tab.

ix Repeat steps i to viii to create additional PW Template Bindings, as required.

x Select the required entry or entries from the list.

i Click the OK button to apply the configuration changes you have made. The BGP Configuration form closes.

10 If you are configuring a BGP VPLS, go to step 11. Otherwise go to step 13.

11 Enable the Enable BGP VPLS parameter. The BGP VPLS section is displayed.

12 Configure the parameters:

- VE Name
- Max VE ID
- VE ID
- Administrative State

13 If you are configuring BGP AD, go to step 14. Otherwise go to step 17.

14 Enable the Enable BGP AD parameter. The BGP AD section is displayed.

15 Configure the parameters:

- VPLS ID
- Formatted VSI ID Prefix
- Administrative State

Note 1 — The Global Service VPLS ID is set to the value defined at the service level.

Note 2 — If VPLS ID is defined at the service level, then the 5620 SAM ensures that each site has the same VPLS ID. If a site has a different VPLS ID, an alarm is raised and the ID mismatch is indicated in the Status panel of the VPLS site properties form.

The same VPLS ID value is propagated to each site in a VPLS. If you change the VPLS ID of a site without using the 5620 SAM, the 5620 SAM displays a warning message.

16 Click on the OK button. The VPLS Site (Edit) form closes.

17 Click on the OK button. A dialog box appears.

18 Close the VPLS Service (Edit) form.

Procedure 68-7 To configure a site for BGP VPLS Multi-homing

This workflow and procedure lists the steps required to configure a site for BGP VPLS Multi-homing.

BGP VPLS Multi-homing provides redundancy support through the configuration of a number of multi-homed sites, rather than through the use of MC-LAG or MC-Ring as access mechanisms. Dual-homing between a CE device and a pair of VPLS PE devices (potentially in different autonomous systems) is an example of such a configuration.

Note 1 — This procedure can only be performed for an existing site, not during the creation of a new site.

Note 2 — Only regular VPLS sites and B-Sites can be configured for BGP VPLS Multi-homing. However, the B-Sites cannot be used as a backbone for an I-Site or Epipe.

Note 3 — I-VPLS and MVPLS services cannot be configured for this application.

Note 4 — An RD or RT configured under the BGP of a VPLS site cannot be removed as long as there is a multi-homing site ID configured whose administration state is up.

Note 5 — You can see a list of all current BGP VPLS Multi-homing sites in a multi-homing VPLS service by viewing the BGP Multi-homing Sites tab on the service configuration form.

1 Prior to configuring a site for BGP VPLS Multi-homing, you must complete the following actions:

a Create a routing policy to define the required community members. See Procedure 27-8. This defines the VSI Import/Export Routing Targets.

b Enable BGP on the routing instance of each NE in the VPLS or BGP VPLS. See Procedure 28-1 for more information.

c Configure global-level BGP on each NE in the VPLS or BGP VPLS. See Procedure 28-2 for more information. The following items are required:

- On the VPN tab of the Routing Instance form, you must enable the L2 VPN parameter in the Family block.

Note — For optimal processing while a BGP multi-homing site is activated or de-activated, or the system is rebooted, you should also:

- Enable the L2 VPN parameter in the Rapid Update Address Family block on the BGP site's VPN tab.
- Enable the Enable Rapid Withdrawal parameter on the BGP site's Behavior tab.

- Create a peer group under BGP. This peer group is used to collectively define the peers involved in the VPLS.
- Create the required peers under the peer group. These peers are the NEs involved in the VPLS.

d Create a PW template. See chapter 49 for information about PW templates.

e Distribute the PW Template to each NE that is or will be a component of the VPLS or BGP VPLS.

f Create SDPs for the BGP VPLS Multi-homing site(s), if manually-provisioned service tunnels are required. Refer to Procedure 30-1.

2 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

3 Configure the filter criteria. A list of services appears.

4 Select the required VPLS or HVPLS and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

5 Click on the Components tab button.

6 Right-click on the required site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

7 Click on the BGP tab button. The General sub-tab page is displayed.

8 Configure the Route Distinguisher parameter.

9 Click the Configuration button to configure the Route Targets and the PW Templates. The BGP Configuration form opens, with the VSI Import Policies tab page displayed.

a Select up to five import policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

b Perform one of the following:

i Enter the Import Route Target name manually in the provided field. The format must be “target:x:y”.

ii Click on the Import Route Target Select button. The Select... -BGP Configuration form opens. Click on the Search button to display the available import route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select... -BGP Configuration form closes.

c Click on the VSI Export Policies tab and select up to five export policies, as required. Alternatively, you can enter the policy names manually in the provided fields.

d Perform one of the following:

i Enter the Export Route Target name manually in the provided field. The format must be “target:x:y”.

ii Click on the Export Route Target Select button. The Select... -BGP Configuration form opens. Click on the Search button to display the available export route targets. The community members you defined when creating a routing policy in step 1 appear in the list. Select the required target and click OK. The Select... -BGP Configuration form closes.

e Click on the PW Template Binding tab button.

f Perform one of the following:

i To use an existing PW Template Binding, go to step g.

ii To create a new PW Template Binding, go to step h.

g For an existing PW Template Binding:

i Click the Search button. A list of applicable PW Template Bindings is displayed.

ii Select the required entry or entries from the list.

iii Go to step i.

h To create a new PW Template Binding:

i Click the Add button. The PW Template Binding (Create) form opens with the General tab page displayed.

ii Enter a Split Horizon Group name, if required.

iii Click the Select button. The Select PW Template form is displayed.

iv Click the Search button. A list of applicable PW Templates is displayed.

v Select the PW Template you created in step 1.

vi Click OK to accept the selection. The Select PW Template form close and the Policy ID field is populated by your choice.

vii Click on the PW Templates Binding Route Target tab and click the Add button. The PW Template Binding Route Target (Create) form is displayed.

Note — This Route Target is used by the NE to decide which PW Template to use to create SDP bindings. If a far-end neighbor has a matching export target (that is, to the PW Template Import Target being defined here), then this PW Template is selected by the NE to create the pseudowire that is used to link both sites of the VPLS. If nothing is entered, and multiple PW Templates are defined, the first one found by the NE is used (most likely the one with the lowest PW Template Policy ID).

Enter the required Route Target in the field and click OK. The PW Template Binding Route Target (Create) form closes and the entered Route Target is displayed in the table on the PW Template Binding Route Target tab.

viii Click OK to accept the selection. The PW Template Binding (Create) form closes and the new PW Template Binding is displayed in the table on the PW Template Binding tab.

ix Repeat steps i to viii to create additional PW Template Bindings, as required.

x Select the required entry or entries from the list.

i Click the OK button to apply the configuration changes you have made. The BGP Configuration form closes.

10 Click on the Multi-homing sub-tab button.

11 Click on the Add button. The BGP Multi-homing VPLS Site (Create) form opens.

12 Configure the parameters:

- Multi-homing Site Name
- Multi-homing ID
- Enable Multi-homing to

13 Click the Select button to specify a SAP, Spoke SDP, or a Split Horizon Group, based on the option you selected for the Enable Multi-homing to parameter.

14 Configure the parameters:

- Failed Threshold
- Use Node Level Boot Timer
- Boot Timer (seconds)
- Use Node Level Site Activation Timer
- Activation Timer (seconds)
- Administrative State

If you enable either the Use Node Level Boot Timer and/or Use Node Level Site Activation Timer parameters, then the associated Boot Timer (seconds) and/or Activation Timer (seconds) parameters will not be configurable. These parameter values will be inherited from the network element configuration.

The Boot Timer (seconds) and Activation Timer (seconds) parameters can be configured for an NE on the BGP Multi-homing sub-tab under the Redundancy tab in the Network Element (Edit) form. See Procedure 17-8 for more information on changing device properties.

15 Click on the Apply button. A dialog box appears.

16 Click on the OK button. The BGP Multi-homing VPLS Site (Create) form refreshes.

17 Check the following indicators:

- Operational State: indicates the operational status of the multi-homing site.
- Designated Forwarder: indicates whether this site has been declared as designated forwarder, depending on the result of the BGP election.

18 Click on the OK button. The BGP Multi-homing VPLS Site (Create) form closes.

19 Click on the OK button. The VPLS Site (Edit) form closes.

20 Close the VPLS Service (Edit) form.

Procedure 68-8 To re-evaluate PW Templates

Use this procedure to re-evaluate changes made to the Route Targets associated with the PW Template bindings of an existing site with BGP configuration. This procedure can only be performed on an existing VPLS that has been configured with BGP AD or BGP VPLS. The procedure allows you to make configuration changes and propagate them to the service without having to shutdown and then turn up a site.

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria. A list of services appears.

3 Select the required VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on the required site and choose Properties. The VPLS Site (Edit) form opens with the General tab displayed.

6 Click on the BGP tab button.

7 Click the Configuration button to open the BGP Configuration form.

8 Make any required changes to the Route Targets or PW Template bindings. Refer to Procedures 68-6 or 68-7 as required, for detailed instructions on configuring these items.

9 Click the PW Template Binding tab and click the Apply button to apply the changes you have made.

10 Perform one of the following:

i If you need to update the PW Templates under other sites for this service, repeat steps 5 to 9 as required, then go to step 14.

ii If you do not need to update the PW Templates under other sites for this service go to step 11.

11 Click the Re-evaluate PW Template button to run an evaluation of the PW Template bindings. A pop-up window appears indicating if the re-evaluation was successful. If it was not, the reason for the failure is displayed.

If you make any subsequent modifications, you can re-evaluate the template again.

12 Click OK. The BGP Configuration form closes.

13 Click the OK button to close the VPLS Service (Edit) form. The procedure is complete.

14 Return to the VPLS (Edit) form.

15 Click the Re-evaluate PW Template button. The Add form opens to allow you to select one of the PW Templates you modified.

16 Click the Search button to display a list of PW Templates and select the required one.

17 Click the OK button to run an evaluation of the selected PW Template. A pop-up window appears indicating if the re-evaluation was successful. If it was not, the reason for the failure is displayed.

18 Repeat steps 15 to 17 for any other sites that you want to re-evaluate a PW Template for.

19 Click the OK button to close the VPLS Service (Edit) form.

Procedure 68-9 To create an HVPLS

Perform this procedure to create an HVPLS. An HVPLS consists of a VPLS in which one or more sites connect to other sites in the same VPLS, different VPLS, or to VLL services.

Note — One VPLS site in an HVPLS must be configured with an SHG. See "Split horizon groups" in this chapter for more information.

1 Add a VPLS to the HVPLS.

a Create a new VPLS.

i Perform Procedure 68-1.

Caution — If you are creating an HVPLS that includes two sites in the same VPLS connected by spoke SDPs, do not create mesh SDP bindings between the sites. Mesh SDP binding functionality is available in the spoke SDP bindings between the sites.

ii Go to step 2.

b Use an existing VPLS. Go to step 3.

2 Create another service for inclusion in the HVPLS, if required.

a Create a VPLS.

i Perform Procedure 68-1.

ii Go to step 3.

b Create a VLL.

i Perform the appropriate VLL creation procedure in chapter 67.

ii Go to step 3.

3 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens with the General tab displayed.

4 Configure the filter criteria. A list of services appears.

5 Select a VPLS that you want to include in the HVPLS and click on the OK button. The VPLS (Edit) form opens.

6 Right-click on Spoke SDP Bindings below the site and choose Create Spoke SDP Bindings. The Spoke SDP Binding (Create) form opens with the General tab displayed.

7 Perform Procedure 68-5 beginning with step 10. Choose the destination node for the site that you want to include in the HVPLS as the Tunnel Termination Site.

8 Perform this procedure as required to add sites to the HVPLS.

Procedure 68-10 To create an MVPLS

An MVPLS runs RSTP or MSTP to manage traffic blocking on the associated VPLS. Perform this procedure to create an MVPLS to run MSTP, or to run RSTP and manage traffic on the associated VPLS SAPs or redundant spoke SDPs. The procedure also applies to the I-Sites and B-Sites used in PBB.

1 Choose Create→Service→MVPLS from the 5620 SAM main menu. The MVPLS (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the MVPLS. The Select Customer - MVPLS form opens.

3 Select a customer for the MVPLS and click on the OK button. The Select Customer - MVPLS form closes, and the MVPLS (Create) form refreshes with the customer name.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Administrative State
- Default Mesh VC ID
- Inherit Service ID Value
- Per Service Hashing for LAG Enabled

5 Click on the Components tab button.

6 Right-click on Sites under MVPLS and choose one of the following, as required:

- Create MVPLS B-Site
- Create MVPLS I-Site
- Create MVPLS Site

The Select Network Elements - MVPLS form opens with a list of available sites.

7 Select a site and click on the OK button. Depending on your selection in step 6, the MVPLS B-Site (Create), MVPLS I-Site (Create), or MVPLS Site (Create) form opens with the General tab displayed.

8 Perform one of the following:

a Create an RSTP site for the MVPLS.

i For regular VPLS sites, perform steps 14 to 36 of Procedure 68-1. Specify RSTP as the value for the STP Mode parameter in step 16. Go to step iv when completed.

ii For B-Sites, perform steps 9 to 22 of Procedure 68-11. Specify RSTP as the value for the STP Mode parameter in step 12iv. Go to step iv when completed.

iii For I-Sites, perform steps 9 to 21 of Procedure 68-12. Specify RSTP as the value for the STP Mode parameter in step 13 iv. Go to step iv when completed.

iv Repeat step i, ii, or iii, as required, for each site that you want to create in the MVPLS.

b Create an MSTP site for the MVPLS.

Note — MSTP is configurable only on the 7450 ESS and 7750 SR.

i For regular VPLS sites, perform steps 14 to 36 of Procedure 68-1. Specify MSTP as the value for the STP Mode parameter in step 16. Go to step iv when completed.

ii For B-Sites, perform steps 9 to 22 of Procedure 68-11. Specify MSTP as the value for the STP Mode parameter in step 12iv. Go to step iv when completed.

iii For I-Sites, perform steps 9 to 21 of Procedure 68-12. Specify MSTP as the value for the STP Mode parameter in step 13iv. Go to step iv when completed.

iv Repeat step i, ii, or iii, as required, for each site that you want to create in the MVPLS.

9 Click on the OK button. The MVPLS (Create) form reappears.

10 If the MVPLS site is to manage traffic on associated VPLS SAPs, create a SAP for the MVPLS with a defined redundant VLAN range.

Note — If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation in the MVPLS.

i For regular VPLS sites, perform steps 6 to 49 of Procedure 68-3. Ensure that you perform step 34 to specify a redundant VLAN range. Go to step iv when completed.

ii For B-Sites, perform steps 6 to 29 of Procedure 68-13. Ensure that you perform step 24 to specify a redundant VLAN range. Go to step iv when completed.

iii For I-Sites, perform steps 6 to 32 of Procedure 68-14. Ensure that you perform step 26 to specify a redundant VLAN range. Go to step iv when completed.

iv Click on the OK button. The MVPLS (Create) form reappears.

11 Click on the OK button. The MVPLS (Create) form closes.

Procedure 68-11 To create a B-site for VPLS or MVPLS

1 Choose Create→Service→VPLS from the 5620 SAM main menu. The VPLS (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VPLS. The Select Customer - VPLS form opens.

3 Select a customer for the VPLS and click on the OK button. The Select Customer - VPLS form closes, and the VPLS (Create) form displays the customer information.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Administrative State
- Default Mesh VC ID
- Automatic SDP Binding Creation
- Transport Type
- Use Bandwidth-Reserved Paths
- OLC State

The OLC State parameter is configurable after you click on the Apply button.

The Transport Type and Use Bandwidth-Reserved Paths parameters are configurable when the Automatic SDP Binding Creation parameter is enabled.

5 Perform one of the following.

a Create a B-site for the VPLS. Go to step 6.

b Complete service creation if B-sites, B-L2 access interfaces, and SDP bindings for the VPLS are to be created later. Go to step 25.

6 Click on the Components tab button.

7 Right-click on the Sites icon and choose Create B-Site from the contextual menu. The Select Network Elements - VPLS form opens with a list of available sites.

8 Select a site and click on the OK button. The B-Site (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- MTU
- Default Mesh VC ID
- Administrative State
- Monitor Access Interface Operational State
- Per Service Hashing for LAG Enabled

10 Click on the Backbone tab button.

11 Configure the backbone parameters:

- Source MAC Address
- Use SAP Backbone MAC Address
- Administrative State
- Notification Interval (seconds)
- Notification Count

Note 1 — The Source MAC Address should not be duplicated for other B-sites within the same B-VPLS.

Note 2 — The Use SAP Backbone MAC Address is configurable only in chassis mode D, or on a Release 8.0 R1 or later 7750 SR-c12.

12 Configure MFIB, STP, FIB, and MRP parameters for the B-site, if required.

i Click on the Forwarding Control tab button. The MFib tab is displayed.

ii Configure the parameters:

- Table size (entries)
- High Watermark (%)
- Low Watermark (%)

iii Click on the STP tab button to configure STP parameters for the B-site, if required. Otherwise, go to step v.

iv Configure the bridge-level STP parameters for the B-site.

Alcatel-Lucent STP in a VPLS interoperates with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters balance the STP resiliency and speed of convergence. Modifying the bridge-level parameters must be done within the constraints of the following formulas:

- 2 × (Bridge Forward Delay – 1.0 s) >= Bridge Max Age
- Bridge Max Age >= 2 × (Bridge Hello Time + 1.0 s)

Note 1 — If you are configuring an MVPLS B-site, set the STP Mode parameter to RSTP or MSTP, depending on the MVPLS type. The MSTP option is available only if you are creating an MVPLS. See Procedure 68-10 for more information about creating an MVPLS.

Note 2 — MSTP is configurable only on the 7450 ESS, 7710 SR, and 7750 SR.

- Bridge Forward Delay (seconds)
- Bridge Hello Time (seconds)
- Bridge Max Age (seconds)
- Priority
- STP Mode
- Maximum BPDUs (PDUs/Hello Interval)
- Administrative State

v Click on the FIB tab button to configure FIB parameters for the B-site, if required. Otherwise, go to step 13.

vi Configure the parameters:

- High Watermark (%)
- Low Watermark (%)
- Local Age Time (seconds)
- Remote Age Time (seconds)
- Size (entries)
- Aging Enabled
- Learning Enabled
- Discard Unknown Destinations
- MAC Flush on Fail
- Propogate MAC Flush

vii Depending on the type of device being configured, the Mac Move panel appears. Configure the MAC move parameters, if required:

- Move Frequency
- Retry Timeout
- Number of Retries
- Administrative State
- Primary Ports Cumulative Factor
- Secondary Ports Cumulative Factor

viii If you are configuring an MVPLS B-site that requires MSTP, click on the MSTP tab button. Otherwise, go to step 13.

Note — MSTP is configurable only on the 7450 ESS, 7710 SR, and 7750 SR.

ix Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

x Click on the MST Instances tab button.

xi Click on the Add button. The MST Instance (Create) form opens with the General tab displayed.

xii Configure the parameters:

- Instance Index
- Priority

xiii Click on the VLAN Ranges tab button. Click on the Add button. The MST Instance Managed VLAN range (Create) form opens.

xiv Configure the parameters:

- Min. VLAN Tag
- Max. VLAN Tag

xv Click on the OK button. The MST Instance Managed VLAN Range (Create) form closes, and a dialog box appears.

xvi Click on the OK button. The MST Instance (Create) form refreshes with the new managed VLAN range.

xvii Click on the OK button. The MST Instance (Create) form closes and a dialog box appears.

xviii Click on the OK button. The MVPLS Site (Create) form refreshes with the new MST instance.

xix Click on the MRP tab button.

xx Configure the parameters:

- MRP Admin Status
- MRP Max Attributes
- MRP Flood Time (seconds)
- MRP Attribute-Table-Low-Watermark (%)
- MRP Attribute-Table-High-Watermark (%)

Note — You can view information regarding MMRP Entries for the access interface and/or SDP Binding by clicking on the MMRP Entries tab button.

13 Create an endpoint for redundancy (dual homing) on the B-site, if required.

i Click on the Endpoints tab button.

ii Click on the Add button. The Endpoint (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Name
- Description
- Revert time (seconds)
- Suppress Standby Signalling
- Ignore Standby Signalling
- MAC Pinning

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Endpoint (Create) form closes and the B-Site (Create) form reappears with the new endpoint displayed in the list.

14 If you are configuring an MVPLS B-site, go to step 19.

15 Configure an SHG on the site, if required.

Note — You must configure an SHG or RSHG if you plan to create a spoke circuit from this VPLS B-site to a VLL or to another VPLS.

i Click on the Split Horizon Groups tab button.

ii Click on the Add button. The Site, New Split Horizon Group (Create) form opens.

iii Configure the parameters:

- Name
- Description

iv Click on the OK button. The Site, New Split Horizon Group (Create) form closes.

Note — You can view information about the I-Sites and Epipe sites associated with the B-Site by clicking on the Associated Sites tab button.

16 Click on the Components tab button.

17 To create a B-L2 access interface for the site, perform steps 5 to 31 of Procedure 68-13.

18 To create a mesh SDP binding for the site, perform steps 6 to 26 of Procedure 68-4.

19 To create a redundant spoke SDP binding under an endpoint, perform steps 5 to 38 of Procedure 68-5.

20 To create a spoke SDP binding for the site, perform steps 8 to 38 of Procedure 68-5.

Note 1 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP, or enable MSTP on a site that has a spoke SDP binding.

Note 2 — You cannot enable MSTP on a SAP that has a non-zero encapsulation value.

21 Create a virtual MEP on the site, if required. For more information about virtual MEPs, see chapter 43.

i Click on the Virtual MEP tab button.

ii Click on the Add button. The MEP (Create) form opens.

iii Click on the Select button. The Select Maintenance Entity Group form opens.

iv Choose a MEG from the list.

Note — The B-VPLS site must be added to the MEG during MEG configuration. Otherwise, the virtual MEP cannot be created on the B-site. See chapter 35 for more information.

v Configure the parameters:

- Auto-Assign ID
- ID
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- Mac Address
- Fault Propagation
- Fault Alarm Time
- Fault Reset Time

vi Click on the OK button. The Select Maintenance Entity Group form closes, and the MEG information is displayed on the MEP (Create) form.

vii Click on the OK button. The MEP (Create) form closes, and the virtual MEP is created on the B-VPLS site.

22 Click on the OK button. The B-Site (Create) form closes, and a dialog box appears.

23 Click on the OK button. The VPLS (Create) form displays the new site on the Components tab under VPLS.

24 Repeat steps 7 to 23 to create additional sites for the B-VPLS.

25 Click on the OK button. The VPLS (Create) form closes.

26 Close the Manage Services form.

Procedure 68-12 To create an I-VPLS

1 Choose Create→Service→VPLS from the 5620 SAM main menu. The VPLS (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VPLS. The Select Customer - VPLS form opens.

3 Select a customer for the VPLS and click on the OK button. The Select Customer - VPLS form closes, and the VPLS (Create) form displays the customer information.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Administrative State
- Default Mesh VC ID
- Automatic SDP Binding Creation
- Transport Type
- Use Bandwidth-Reserved Paths
- OLC State

The OLC State parameter is configurable after you click on the Apply button.

The Transport Type and Use Bandwidth-Reserved Paths parameters are configurable when the Automatic SDP Binding Creation parameter is enabled.

5 Perform one of the following.

a Create an I-site for the VPLS. Go to step 6.

b Complete service creation if I-sites, I-L2 access interfaces, and SDP bindings for the VPLS are to be created later. Go to step 26.

6 Click on the Components tab button.

7 Right-click on the Sites icon and choose Create I-Site from the contextual menu. The Select Network Elements - VPLS form opens with a list of available sites.

8 Select a site and click on the OK button. The I-Site (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- MTU
- Administrative State
- Monitor Access Interface Operational State
- Per Service Hashing for LAG Enabled

10 Click on the Backbone tab button.

11 Select the Backbone VPLS site.

i Click on the Select button. The Select Backbone VPLS Site - I-Site form is displayed.

ii Click the Search button. A list with all the B-VPLSs that can be used by the I-VPLS is displayed. You can narrow the search by using the using the filtered properties shown in the form. Only B-VPLSs that are present in PEs that have the I-Sites of the VPLS is shown.

iii Select a B-VPLS and click on OK. The Select Backbone VPLS Site - I-Site form closes and the Service ID of the chosen B-VPLS appears on the I-Site (Create) form.

Note — The selection of the B-site in this step must be repeated for each I-site you create, since you must select the B-VPLS site that is within the same site as the I-site.

12 Configure the parameters:

- Send Flush All From Me
- Send Flush All But Mine
- Administrative ISID
- Backbone STP
- Force Q Tag Forwarding

Note — The Force Q Tag Forwarding parameter is only displayed if the NE for this site is in chassis mode D or higher or Sparrow.

13 Configure MFib, STP, FIB, and MAC Protection parameters for the I-site, if required.

i Click on the Forwarding Control tab button. The MFib tab is displayed.

ii Configure the parameters:

- Table size (entries)
- High Watermark (%)
- Low Watermark (%)

iii Click on the STP tab button to configure STP parameters for the I-site, if required. Otherwise, go to step v.

iv Configure the bridge-level STP parameters for the I-site.

Alcatel-Lucent STP in a VPLS interoperates with customer STP implementations as a mechanism for loop detection and prevention. The bridge-level parameters balance the STP resiliency and speed of convergence. Modifying the bridge-level parameters must be done within the constraints of the following formulas:

- 2 × (Bridge Forward Delay – 1.0 s) >= Bridge Max Age
- Bridge Max Age >= 2 × (Bridge Hello Time + 1.0 s)

Note 1 — If you are configuring an MVPLS I-site, set the STP Mode parameter to RSTP or MSTP, depending on the MVPLS type. The MSTP option is available only if you are creating an MVPLS. See Procedure 68-10 for more information about creating an MVPLS.

Note 2 — MSTP is configurable only on the 7450 ESS, 7710 SR, and 7750 SR.

- Bridge Forward Delay (seconds)
- Bridge Hello Time (seconds)
- Bridge Max Age (seconds)
- Priority
- STP Mode
- Maximum BPDUs (PDUs/Hello Interval)
- Administrative State

v Click on the FIB tab button to configure FIB parameters for the I-site, if required. Otherwise, go to step 17.

vi Configure the parameters:

- High Watermark (%)
- Low Watermark (%)
- Local Age Time (seconds)
- Remote Age Time (seconds)
- Size (entries)
- Aging Enabled
- Learning Enabled
- Discard Unknown Destinations
- MAC Flush on Fail
- Propogate MAC Flush

vii Depending on the type of device being configured, the Mac Move panel appears. Configure the MAC move parameters, if required:

- Move Frequency
- Retry Timeout
- Number Of Retries
- Administrative State
- Primary Ports Cumulative Factor
- Secondary Ports Cumulative Factor

viii Click on the MAC Protection tab to configure the list of protected MAC addresses.

ix Click on the Add button. The MAC Protection (Create) form opens.

x Configure the Protected Mac Address parameter.

xi Click on the OK button to close the form and add the MAC address to the list of protected MAC addresses.

xii If you are configuring an MVPLS I-site that requires MSTP, click on the MSTP tab button. Otherwise, go to step 16.

Note — MSTP is configurable only on the 7450 ESS, 7710 SR, and 7750 SR.

xiii Configure the parameters:

- Region Name
- Region Revision
- Bridge Max Hops

xiv Click on the MST Instances tab button.

xv Click on the Add button. The MST Instance (Create) form opens with the General tab displayed.

xvi Configure the parameters:

- Instance Index
- Priority

xvii Click on the VLAN Ranges tab button. Click on the Add button. The MST Instance Managed VLAN range (Create) form opens.

xviii Configure the parameters:

- Min. VLAN Tag
- Max. VLAN Tag

xix Click on the OK button. The MST Instance Managed VLAN Range (Create) form closes, and a dialog box appears.

xx Click on the OK button. The MST Instance (Create) form refreshes with the new managed VLAN range.

xxi Click on the OK button. The MST Instance (Create) form closes and a dialog box appears.

xxii Click on the OK button. The MVPLS Site (Create) form refreshes with the new MST instance.

14 Configure ingress multicast forwarding, if required.

Note — An Operational Channels tab appears when you access the VPLS I-Site form in the Edit mode. It displays data for the operational channels when traffic from a specific multicast source for a specific multicast group passes through the service. You must click on the Search button to refresh the data. See chapter 43 for information about listing the operational channel parameters.

i Click on the Mcast Path Mgmt tab button.

ii Click on the Select button to choose a multicast info policy. The Select Ingress Info Policy form opens.

iii Select a policy in the list and click on the OK button. The Select Ingress Info Policy form closes and the policy identifier is displayed on the Site (Create) form.

15 Configure IGMP snooping for the site, if required.

i Click on the IGMP Snooping tab button.

ii Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Robust count
- Report source address
- Use Query source address
- Query source address

The Query source address parameter is configurable when the Use Query source address parameter is enabled.

16 If you are configuring an MVPLS I-site, go to step 18.

17 Configure an SHG on the site, if required.

Note — You must configure an SHG or RSHG if you plan to create a spoke circuit from this VPLS I-site to a VLL or to another VPLS.

i Click on the Split Horizon Groups tab button.

ii Click on the Add button. The Site, New Split Horizon Group (Create) form opens.

iii Configure the parameters:

- Name
- Description
- Restrict Protected Source
- Restrict Protected Source Action
- Restrict Unprotected Destination

iv Click on the OK button. The Site, New Split Horizon Group (Create) form closes.

18 Click on the Components tab button.

19 To create an I-L2 access interface for the I-site, perform steps 4 to 34 of Procedure 68-14.

20 To create a spoke SDP binding between the I-site and regular VPLS sites, click on the Components tab and perform steps 9 to 38 of Procedure 68-5, as required. I-sites can only use spoke SDP bindings.

Note 1 — You cannot create a spoke SDP binding on an MVPLS site that runs MSTP, or enable MSTP on a site that has a spoke SDP binding.

Note 2 — You cannot enable MSTP on an access interface that has a non-zero encapsulation value.

21 Click on the OK button. The I-Site (Create) form closes, and a dialog box appears.

22 Click on the OK button. The VPLS (Create) form displays the new I-site on the Components tab under VPLS.

23 Repeat steps 6 to 22 to create additional I-sites for the I-VPLS.

24 Add protected MAC addresses at the service level, if required. Protected MAC addresses that you add on the site level, as performed in step 13, are automatically added to the service-level MAC protection list.

i Click on the Forwarding Control tab button.

ii Click on the MAC Protection tab button.

iii Click on the Add button. The MAC Protection (Create) form opens.

iv Configure the Protected Mac Address parameter.

v Click on the OK button. The MAC Protection (Create) form closes and the protected MAC address is listed on the VPLS (Create) form.

25 To configure bandwidth for the service if required, click on the Bandwidth tab. The Required Bandwidth sub-tab page is displayed. Proceed as follows:

Note 1 — The Bandwidth tab is only available if service CAC is configured; see chapter 5 for information about enabling and disabling service CAC.

Note 2 — The ability to configure required bandwidth is only applicable to I-sites.

i For each CoS, enter the value for the CoS Bandwidth (Mbps), as required.

ii Click on the General tab to determine the CAC status.

If the Verify CAC button is enabled, the CAC has not been verified. The Probable Cause and CAC Status fields provide details.

The CAC Status field describes the current CAC status of the service. CAC statuses are as follows.

- CAC Verified indicates that all tunnels have sufficient bandwidth to admit service and that requested bandwidth for the service is booked on the appropriate physical links.
- CAC Failed indicates that the attempt made to admit service into the network was unsuccessful. The most likely cause for this is insufficient bandwidth. See the Probable Cause field for more specific information.
- BW Defined, No CAC Request indicates that the required bandwidth is defined on the service; however, a CAC request has not occurred.
- CAC To be Verified indicates that a tunnel has been configured on the service either manually or through the CLI; however, the required bandwidth has not been verified in the network.

The Probable Cause field describes possible reasons for the current CAC state. Probable causes are as follows.

- No Candidate Tunnels Found indicates that the autobind tunnel function was found, but no suitable tunnels were found.
- Different PBB Tunnels Applied to Service indicates that two or more different PBB tunnels are configured on this service.
- Not Enough Bandwidth on any Candidate Tunnels indicates that one or more candidate tunnels were found, but the available bandwidth was insufficient to admit the service.
- Automatic PBB Tunnel Selection Failed indicates that a suitable PBB tunnel was found, but there were errors when attempting to assign the tunnel to the service. A dialog box will provide more details.
- Site Missing Tunnel indicates that at least one selected site is not configured with a PBB tunnel.
- All PBB Tunnels have not been Verified indicates that all sites within the service have a tunnel configured, but the available bandwidth has not been booked or verified in the network.

iii To manually verify the CAC, click on the Verify CAC button if it is enabled. The 5620 SAM will attempt to find the most appropriate PBB tunnel for the service based on available bandwidth, and to automatically bind the tunnel to the service if one has not already been assigned.

26 Click on the OK button. The VPLS (Create) form closes.

27 Close the Manage Services form.

Procedure 68-13 To create a VPLS or MVPLS B-L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Navigate to the Access Interfaces icon for the required site. The path is VPLS→Site→Access Interfaces.

6 Right-click on Access Interfaces and choose Create B-L2 Access Interface. The B-L2 Access Interface (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Description
- Administrative State
- MC Ring Node

8 Choose an SHG for the interface, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - B-L2 Access Interface list form opens.

Note — You must configure an SHG or residential SHG for a VPLS if you plan to create a spoke circuit from this VPLS site to a VLL or another VPLS.

ii Select an SHG and click on the OK button. The Select Split Horizon Group Name - B-L2 Access Interface list form closes, and the B-L2 Access Interface (Create) form refreshes with the SHG name.

9 Click on the Port tab button.

10 Click on the Select button to choose a port for the B-L2 access interface. The Select Terminating Port - VPLS B-L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

11 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPLS B-L2 Access Interface form closes, and the VPLS B-L2 Access Interface (Create) form displays the port information.

12 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 64-14 for more information about deleting MSAPs.

For a B-L2 access interface, only Null, Dot1 Q, and Q in Q encapsulation are supported.

When the selected port uses Dot1 Q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for Dot1 Q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form.

13 Depending on the port that you have chosen, the Egress Multicast Group tab is configurable. Configure the EMG, if required.

i Click on the Egress Multicast Group tab button. The Select Egress Multicast Group-B-L2 Access Interface form opens.

ii Select an EMG and click on the OK button. The Select Egress Multicast Group-B-L2 Access Interface form closes, and the Egress Multicast Group tab refreshes with the EMG name.

Note — The Egress Multicast Group-L2 Interface form lists only EMGs that have the same egress filter and encapsulation type as the interface.

14 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

15 Assign ingress and egress QoS policies to the interface, if required.

i Click on the QoS tab button.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service components tree, choosing Properties, and configuring the parameters on the appropriate tab.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use Shared Queue
- Use Multipoint Shared Queue
- HSMDA Packet Byte Offset (bytes)

The Use Shared Queue and Use Multipoint Shared Queue parameters are only configurable for non-HSMDA ports.

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is Dot1 Q or Q in Q.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - B-L2 Access Interface form opens.

iv Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the ingress QoS policy name.

Note — If you select an access ingress policy that has a forwarding class mapped to an ingress queue group, the port that you choose for the VPLS L2 access interface must use the same access ingress queue group.

See Procedure 17-61 for information about configuring Ethernet ports. See chapter 43 for information about queue group template policies.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - B-L2 Access Interface form opens.

vi Select an egress QoS policy and click on the OK button. The Select Egress Policy - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the egress QoS policy name.

Note — If you select an access egress policy that has a forwarding class mapped to an egress queue group, the port that you choose for the VPLS L2 access interface must use the same access egress queue group.

See Procedure 17-61 for information about configuring Ethernet ports. See chapter 43 for information about queue group template policies.

vii Click on the Select button in the HSMDA Egress Secondary Shaper panel to choose an HSMDA egress secondary shaper policy. The Select HSMDA Egress Secondary Shaper form opens.

viii Select a secondary shaper and click on the OK button. The Select HSMDA Egress Secondary Shaper form closes and the B-L2 Access Interface (Create) form reappears with the egress secondary shaper information displayed.

ix Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

x Select a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the B-L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

xi Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

xii Select a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the B-L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

16 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 18.

Note 1 — The Schedulers tab is configurable only when a port is assigned to the interface.

Note 2 — The Schedulers tab only appears when a non-HSMDA port is assigned. If you are using an HSMDA port, go to step 18.

17 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame Base Accounting

Note 1 — The Egress Aggregate Rate Limit (kbps) and Frame Base Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — You cannot specify an egress scheduler when the Egress Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - B-L2 Access Interface form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - B-L2 Access Interface form opens.

vi Select an egress scheduler and click on the OK button. The Select Egress Scheduler - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

vii Go to step 20.

b Specify that an access scheduler policy is applied to the interface.

i Set the Aggregation parameter to on.

ii Configure the Frame Base Accounting parameter.

iii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - B-L2 Access Interface form opens.

iv Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

v Go to step 20.

18 Click on the Aggregation Rate tab button to configure the aggregation rate, otherwise, go to step 20.

Note — The Aggregation Rate tab is configurable only when a port is assigned to the HSMDA SAP.

19 Configure the Aggregate Rate Limit (kbps) parameter in the Ingress Aggregate Rate Limit and Egress Aggregate Rate Limit panels.

20 Assign ingress and egress ACL filters to the interface, if required.

Note — Only MAC filters are allowed for B-L2 Access Interfaces.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - B-L2 Access Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - B-L2 Access Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the egress ACL filter name.

21 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - B-L2 Access Interface form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - B-L2 Access Interface form closes, and the B-L2 Access Interface (Create) form refreshes with the accounting policy name.

22 Configure BPDU Termination, STP, FIB, and MRP parameters for the interface, if required.

i Click on the Forwarding Control tab button. Depending on the device being configured, the BPDU Termination tab is displayed. Otherwise, go to step iii.

ii Configure the parameters:

- L2 Protocol Termination

  When the L2 Protocol Termination parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.
- BPDU Translation
- Force L2PT on Managed L2 Access Interface

  The Force L2PT on Managed L2 Access Interface parameter is only available for MVPLS B-L2 access interfaces. When the Force L2PT on Managed L2 Access Interface parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.

iii Click on the STP tab button.

iv Configure the parameters:

- Path Cost
- Port Number
- Priority
- Edge Port
- Edge Capability Detection
- Link Type
- Root Guard
- Administrative State

v Click on the FIB tab button.

vi Configure the parameters:

- Aging Enabled
- Learning Enabled
- Limit Mac Move
- Limit Mac Move Level
- Discard Unknown Source

vii If you are creating an MVPLS to run MSTP, the MST Instances tab button is configurable. Otherwise, go to step xiv.

viii Click on the MST Instances tab button to edit a SAP MST instance.

ix Select an MST instance and click on the Properties button.

x The B-L2 Access Interface MST Instance (Edit) form opens. Configure the parameters:

- Path Cost
- Priority

xi Click on the OK button to close the B-L2 Access Interface MST Instance (Edit) form. A dialog box appears.

xii Click on the OK button. The B-L2 Access Interface (Create) form refreshes with the new MST instance.

xiii If you are configuring an MVPLS B-L2 access interface, go to step 23.

xiv Click on the MRP tab button.

xv Configure the parameters:

- MRP Join Time (tenths of a second)
- MRP Leave Time (tenths of a second)
- MRP Leave AllTime (tenths of a second)
- MRP Periodic Time (tenths of a second)
- MRP Periodic Enabled

Note — You can view information regarding MMRP Entries by clicking on the MMRP tab button.

xvi Click on the Select button to select an PBB MRP Policy. The Select PBB MRP Policy form opens.

xvii Choose the desired policy and click OK.

23 Assign a DoS protection policy to the interface, if required.

Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - B-L2 Access Interface form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - B-L2 Access Interface form closes and the policy ID is displayed on the B-L2 Access Interface (Create) form.

iv Configure the MAC Monitoring parameter.

24 Configure a redundant VLAN range, if required.

Note — If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation. The redundant VLAN range defines the range of VC IDs for VPLS SAPs that the MVPLS manages.

i Click on the Redundancy tab button.

ii Click on the Add button. The RedundantVlanRange (Create) form opens.

iii Configure the parameters:

- Min VLAN ID
- Max VLAN ID

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The B-L2 Access Interface (Create) form refreshes with the redundant VLAN range entry.

25 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the MAC Pinning parameter.

26 Specify the queue overrides.

i Click on the Override tab button.

Note — The Override tab contains four sub-tabs: Access Ingress Queue, Access Egress Queue, Access Ingress HSMDA Queue, and Access Egress HSMDA Queue. However, only two of the four are active, depending on the port type you have chosen for this interface.

If you have configured an HSMDA port, then the Access Ingress HSMDA Queue and Access Egress HSMDA Queue sub-tabs are active. If you have configured a non-HSMDA port, then the Access Ingress Queue and Access Egress Queue sub-tabs are active.

ii See Procedure 44-40 for information about setting queue overrides.

27 Associate a MEP with the B-L2 Access interface, if required.

i Click on the MEPs tab button.

ii Click on the Add button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Maintenance Entity Group list form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group list form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- SAP, BINDING or PATH ENDPOINT

Note — The SAP, BINDING or PATH ENDPOINT parameter is automatically selected based on whether the MEP is created on a SAP, SDP binding, or Ethernet Tunnel Path Endpoint.

vi Click on the Select button. The Select SAP - MEP form opens.

vii Select a SAP in the list and click on the OK button. The MEP form displays the SAP information.

viii If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step xii.

ix Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

x Click on the AIS tab button.

xi Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

xii Click on the OK button. The MEP (Create) form closes.

28 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button. The ANCP Static Map (Create) form opens.

ii Configure the ANCP String parameter.

iii Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

iv Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

v Click on the OK button. The ANCP Static Map form closes.

29 Click on the OK button. The B-L2 Access Interface (Create) form closes and a dialog box appears.

30 Click on the OK button. The VPLS (Edit) form reappears.

31 Repeat steps 5 to 30 for each additional B-L2 access interface that you want to create.

32 Click on the OK button. A dialog box appears.

33 Click on the Yes button. The VPLS (Edit) form closes.

34 Close the Manage Services form.

Procedure 68-14 To create a VPLS I-L2 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Navigate to the Access Interfaces icon for the required site. The path is VPLS→Site→Access Interfaces.

6 Right-click on Access Interfaces and choose Create I-L2 Access Interface. The I-L2 Access Interface (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Description
- Administrative State
- MC Ring Node

8 Choose an SHG for the interface, if required.

i Click on the Select button in the Split Horizon Group panel. The Select Split Horizon Group Name - I-L2 Access Interface list form opens.

Note — You must configure an SHG or residential SHG for a VPLS if you plan to create a spoke circuit from this VPLS site to a VLL or another VPLS.

ii Select an SHG and click on the OK button. The Select Split Horizon Group Name - I-L2 Access Interface list form closes, and the I-L2 Access Interface (Create) form refreshes with the SHG name.

9 Click on the Port tab button.

10 Click on the Select button to choose a port for the I-L2 access interface. The Select Terminating Port - VPLS I-L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

11 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPLS I-L2 Access Interface form closes, and the VPLS I-L2 Access Interface (Create) form displays the port information.

Note — If you select an Ethernet Tunnel Endpoint, the Port form is refreshed and an Ethernet Tunnel tab is added.

12 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 64-14 for more information about deleting MSAPs.

For an I-L2 access interface, only Null, Dot1 Q, and Q in Q encapsulations are supported. In the case of I-MPVLS L2-access interfaces, Null encapsulation is not supported. I-MPVLS L2-access interfaces with MSTP configured support Q in Q. These ports must also be of Ethernet type PBB.

When the selected port uses Dot1 Q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. If you choose this, the system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for Dot1 Q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter in the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet with Q in Q encapsulation.

If the port you have chosen is an Ethernet Tunnel Endpoint, you will be able to set the Outer Encapsulation Value to 8191. This automatically enables the Ethernet Tunnel Endpoint Control SAP parameter.

13 Configure the Ethernet Tunnel Endpoint Control SAP parameter, if required.

Note — Enabling the Ethernet Tunnel Endpoint Control SAP parameter creates the control L2 Access Interface (also known as a Control SAP). It also automatically sets the value of the Outer Encapsulation Value parameter to 8191.

If you are currently creating a same-fate SAP, the Ethernet Tunnel Endpoint Control SAP parameter must not be enabled.

14 Depending on the port that you have chosen, the Egress Multicast Group tab is configurable. Configure the EMG, if required.

i Click on the Egress Multicast Group tab button. The Select Egress Multicast Group-I-L2 Access Interface form opens.

ii Select an EMG and click on the OK button. The Select Egress Multicast Group-I-L2 Access Interface form closes, and the Egress Multicast Group tab refreshes with the EMG name.

Note — The Egress Multicast Group-L2 Interface form lists only EMGs that have the same egress filter and encapsulation type as the interface.

15 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

16 Assign ingress and egress QoS policies to the interface, if required.

i Click on the QoS tab button.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service components tree, choosing Properties, and configuring the parameters on the appropriate tab.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use Shared Queue
- Use Multipoint Shared Queue
- HSMDA Packet Byte Offset (bytes)

The Use Shared Queue and Use Multipoint Shared Queue parameters are only configurable for non-HSMDA ports.

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is Dot1 Q or Q in Q.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - I-L2 Access Interface form opens.

iv Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the ingress QoS policy name.

Note — If you select an access ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access ingress queue group with the same name created on it.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - I-L2 Access Interface form opens.

vi Select an egress QoS policy and click on the OK button. The Select Egress Policy - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the egress QoS policy name.

Note — If you select an access egress policy which has a forwarding class mapped to an egress queue group, you must ensure that port that you are configuring for the VPLS L2 access interface has the access egress queue group with the same name created on it.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

vii Click on the Select button in the HSMDA Egress Secondary Shaper panel to choose an HSMDA egress secondary shaper policy. The Select HSMDA Egress Secondary Shaper form opens.

viii Select a secondary shaper and click on the OK button. The Select HSMDA Egress Secondary Shaper form closes and the I-L2 Access Interface (Create) form reappears with the egress secondary shaper information displayed.

ix Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

x Select a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the I-L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

xi Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

xii Select a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the I-L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

17 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 19.

Note 1 — The Schedulers tab is configurable only when a port is assigned to the interface.

Note 2 — The Schedulers tab only appears when a non-HSMDA port is assigned. If you are using an HSMDA port, go to step 19.

18 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame Base Accounting

Note 1 — The Egress Aggregate Rate Limit (kbps) and Frame Base Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — You cannot specify an egress scheduler when the Egress Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - I-L2 Access Interface form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - I-L2 Access Interface form opens.

vi Select an egress scheduler and click on the OK button. The Select Egress Scheduler - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the egress scheduler information displayed.

vii Go to step 21.

b Specify that an access scheduler policy is applied to the interface.

i Set the Aggregation parameter to on.

ii Configure the Frame Base Accounting parameter.

iii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - I-L2 Access Interface form opens.

iv Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

v Go to step 21.

19 Click on the Aggregation Rate tab button to configure the aggregation rate, otherwise, go to step 21.

Note — The Aggregation Rate tab is configurable only when a port is assigned to the HSMDA SAP.

20 Configure the Aggregate Rate Limit (kbps) parameter in the Ingress Aggregate Rate Limit and Egress Aggregate Rate Limit panels.

21 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - I-L2 Access Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the ingress ACL filter name.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - I-L2 Access Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the egress ACL filter name.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an IPv6 ingress ACL filter. The Select IPv6 Ingress Filter - I-L2 Access Interface form opens.

vii Select an IPv6 ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - I-L2 Access Interface form closes and the I-L2 Access Interface (Create) form reappears with the IPv6 ingress ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - I-L2 Access Interface form opens.

ix Select an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - I-L2 Access Interface form closes and the I-L2 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

22 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - I-L2 Access Interface form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - I-L2 Access Interface form closes, and the I-L2 Access Interface (Create) form refreshes with the accounting policy name.

23 Configure BPDU Termination, STP, and FIB parameters for the interface, if required.

i Click on the Forwarding Control tab button. Depending on the device being configured, the BPDU Termination tab is displayed. Otherwise, go to step iii.

ii Configure the parameters:

- L2 Protocol Termination

  When the L2 Protocol Termination parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.
- BPDU Translation
- Force L2PT on Managed L2 Access Interface

  The Force L2PT on Managed L2 Access Interface parameter is only available for MVPLS I-L2 access interfaces. When the Force L2PT on Managed L2 Access Interface parameter is set to Enabled, a list of L2PT protocols is displayed. Select all that are required.

iii Click on the STP tab button.

iv Configure the parameters:

- Path Cost
- Port Number
- Priority
- Edge Port
- Edge Capability Detection
- Link Type
- Root Guard
- Administrative State

v Click on the FIB tab button.

vi Configure the parameters:

- Aging Enabled
- Learning Enabled
- Maximum Entries
- Limit Mac Move
- Limit Mac Move Level
- Discard Unknown Source
- Restrict Protected Source
- Restrict Protected Source Action
- Restrict Unprotected Destination

vii If you are creating an MVPLS to run MSTP, the MST Instances tab button is configurable. Otherwise, go to step 24.

viii Click on the MST Instances tab button to edit a SAP MST instance.

ix Select an MST instance and click on the Properties button.

x The I-L2 Access Interface MST Instance (Edit) form opens. Configure the parameters:

- Path Cost
- Priority

xi Click on the OK button to close the I-L2 Access Interface MST Instance (Edit) form. A dialog box appears.

xii Click on the OK button. The I-L2 Access Interface (Create) form refreshes with the new MST instance.

24 Assign a DoS protection policy to the interface, if required.

Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - I-L2 Access Interface form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - I-L2 Access Interface form closes and the policy ID is displayed on the I-L2 Access Interface (Create) form.

iv Configure the MAC Monitoring parameter.

25 Configure an ethernet tunnel.

Note — You can only configure ethernet tunnel SAP path parameters if you are creating a same-fate SAP.

i Click on the Ethernet Tunnel tab.

ii If you are configuring a fate-sharing Ethernet Tunnel Endpoint SAP (also referred to as same-fate SAP) then go to step iii. Otherwise, go to step 26.

iii Click on the Add button. The Ethernet Tunnel (Create) form opens.

iv Configure the parameters:

- Path ID
- Tag (Outer Encapsulation Value)
- Tag (Inner Encapsulation Value)

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The L2 Access Interface (Create) form refreshes with the Ethernet Tunnel entry.

26 Configure a redundant VLAN range, if required.

Note — If an MVPLS site has SAPs that manage traffic on the associated VPLS SAPs, you must define a redundant VLAN range during SAP creation. The redundant VLAN range defines the range of VC IDs for VPLS SAPs that the MVPLS manages.

i Click on the Redundancy tab button.

ii Click on the Add button. The RedundantVlanRange (Create) form opens.

iii Configure the parameters:

- Min VLAN ID
- Max VLAN ID

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The I-L2 Access Interface (Create) form refreshes with the redundant VLAN range entry.

27 Configure IGMP snooping for the interface, if required.

i Click on the IGMP Snooping tab button. The General tab is displayed.

ii Configure the parameters:

- Import Policy
- Fast-leave
- Mrouter attached
- Send queries
- General query interval (seconds)
- Max. Response interval (seconds)
- Robust count
- IGMP Version
- Max. Response interval group queries (tenths of seconds)
- Max. number of groups
- Max.number of sources per group

The General query interval (seconds), Max. Response interval (seconds), Robust count, and IGMP Version parameters are configurable when the Send queries parameter is enabled.

iii Click on the Static Mcast Group tab button to configure a static multicast group, if required. Otherwise, go to step 28.

iv Click on the Add button. The Access Interface Igmp Snooping Mcast Group Display (Create) form opens.

v Configure the parameters:

- Group Address
- Source Address

vi Click on the Apply button if you want to create additional entries. A dialog box appears.

vii Click on the OK button.

viii Repeat steps iv to vii to create an additional entry, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Static Mcast Group tab refreshes with the new multicast group entries.

28 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the MAC Pinning parameter.

29 Specify the queue overrides.

i Click on the Override tab button.

Note — The Override tab contains four sub-tabs: Access Ingress Queue, Access Egress Queue, Access Ingress HSMDA Queue, and Access Egress HSMDA Queue. However, only two of the four are active, depending on the port type you have chosen for this interface.

If you have configured an HSMDA port, then the Access Ingress HSMDA Queue and Access Egress HSMDA Queue sub-tabs are active. If you have configured a non-HSMDA port, then the Access Ingress Queue and Access Egress Queue sub-tabs are active.

ii See Procedure 44-40 for information about setting queue overrides.

30 Associate a MEP with the I-L2 Access interface, if required.

i Click on the MEPs tab button.

ii Click on the Add button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Maintenance Entity Group list form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group list form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- SAP, BINDING or PATH ENDPOINT

Note — The SAP, BINDING or PATH ENDPOINT parameter is automatically selected based on whether the MEP is created on a SAP, SDP binding, or Ethernet Tunnel Path Endpoint.

vi Click on the Select button beside the Name parameter. The Select SAP - MEP form opens with a list of service access interfaces for the MEP.

vii Choose a service access interface from the list.

viii Click on the OK button. The MEP form is refreshed with the SAP information.

ix If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step xiii.

x Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

xi Click on the AIS tab button.

xii Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

xiii Click on the OK button. The MEP (Create) form closes.

31 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button.

ii Click on the Add button. The ANCP Static Map (Create) form opens.

iii Configure the ANCP String parameter.

iv Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. The ANCP Static Map form closes.

32 Click on the OK button. The I-L2 Access Interface (Create) form closes and a dialog box appears.

33 Click on the OK button. The VPLS (Edit) form reappears.

34 Repeat steps 5 to 33 for each additional I-L2 access interface that you want to create.

35 Click on the OK button. A dialog box appears.

36 Click on the Yes button. The VPLS (Edit) form closes.

37 Close the Manage Services form.

Procedure 68-15 To add or modify FIB entries

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Forwarding Control tab button.

5 Click on the FIB Entries tab button.

6 Click on the Find button. A list of FIB entries appears.

7 Add or modify FIB entries as required.

a To add a FIB entry:

i Click on the Add button. The FibEntry (Create) form opens.

ii Configure the parameters:

- MAC Address
- Auto Complete

iii Choose an interface, service circuit, or endpoint from the list on the L2 Interfaces, Service Circuits, or Endpoints tab.

iv Click on the OK button. The FibEntry (Create) form closes, and the FIB Entries form refreshes with the new FIB entry.

b To modify FIB entries:

i Select a FIB entry on the FIB Entries tab and click on the Properties button. The FibEntry (Edit) form opens.

ii Configure the parameters and view the information as required.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button to close the VPLS (Edit) form.

Procedure 68-16 To list FIB entries

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Sites tab button.

5 Click on the VPLS, B-VPLS, or I-VPLS tab buttons, if required.

6 Select the site can click on the Properties button. The VPLS Site (Edit) form opens with the General tab displayed.

7 Click on the Forwarding Control tab button.

8 Click on the FIB Entries tab button.

9 Click on the Resync button for the FIB entries on the right side of the form. The Resync button on the bottom of the form is for re synchronizing the entire VPLS site.

10 Click on the Find button. A list of FIB entries appears.

Procedure 68-17 To force a switchover to a redundant spoke SDP binding

This procedure can only be performed on a VPLS that has been configured with endpoints that are associated redundant spoke SDP bindings.

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria. A list of services appears.

3 Select the required VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on the redundant spoke SDP binding under an endpoint for the site that you want to perform the switchover for.

6 Select Force Switchover from the popup menu.

7 You can clear the switchover at a later time by performing steps 1 to 5 again and then select the Clear Forced Switchover item from the popup menu.

Note — You must clear a manually forced switchover by using the Clear Forced Switchover button when the active spoke SDP binding is restored. The 5620 SAM cannot automatically switch to another active spoke SDP binding if this is not done.

8 Click on the OK button to close the Spoke SDP Binding (Edit) form.

9 Click on the OK button to close the VPLS (Edit) form.

Procedure 68-18 To view IGMP snooping queriers

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on a site and select Properties. The Site (Edit) form opens with the General tab displayed.

6 Click on the IGMP Snooping tab button. The General tab is displayed.

7 Click on the MRouters tab button. The MRouters table displays a list of IGMP snooping queriers and their properties.

8 Click on the Refresh button to view periodic updates to the Mrouters table.

9 Close the Site (Edit) form.

10 Close the VPLS (Edit) form.

Procedure 68-19 To view MLD snooping queriers

1 Choose Manage→Service→Services from the 5620 SAM main menu.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on a site and select Properties. The Site (Edit) form opens with the General tab displayed.

6 Click on the MLD Snooping tab button. The General tab is displayed.

7 Click on the MRouters tab button. The MRouters table displays a list of MLD snooping queriers and their properties.

8 Click on the Refresh button to view periodic updates to the Mrouters table.

9 Close the Site (Edit) form.

10 Close the VPLS (Edit) form.

Procedure 68-20 To navigate and modify a VPLS

Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

The following tabs contain parameter information for the service:

- General tab—displays the general service properties
- Components tab—displays the various service components in a tree format. You can display the property forms for the components and also navigate to associated components from this view.
- MVR tab—displays multicast package policy information for the service
- Tests tab—allows the creation and execution of service-specific diagnostic tests
- Forwarding Control tab—lists the FIB and STP instances
- Sites tab—lists the sites that belong to the service
- L2 Access Interfaces tab—lists the L2 access interfaces that belong to the service
- L2 Management Interfaces tab—lists the L2 management interfaces that belong to the service
- Mesh SDP Bindings tab—displays the mesh SDP bindings that belong to the service
- Spoke SDP Bindings tab—displays the spoke SDP bindings that belong to the service, including active and backup SDP bindings associated with endpoints.
- Endpoints tab—displays the endpoints associated with the service
- Template tab—displays the template used to create the service, if applicable
- Faults tab—displays the faults associated with the service

Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Navigate to related components for the service using the component tree, as required.

Certain service components have related objects that can be easily examined using the component tree. For such objects, right-clicking them in the component tree offers a “Navigate to ...” option in the contextual menu. If you select this option, the properties form for the related object is displayed. This can be very convenient, especially for complex services containing many sites and components.

The VPLS components for which you can navigate to such related objects include:

- I-Sites: you can navigate to the associated B-VPLS or B-(M)VPLS
- L2 Access Interfaces: you can navigate to the opposite SAP in a VLAN Uplink configuration
- Redundant L2 Access Interfaces: you can navigate to the opposite SAP.
- Mesh SDP Bindings: you can navigate to the opposite (return) mesh SDP
- Spoke SDP Bindings: you can navigate to the opposite (return) spoke SDP

5 Modify the components and parameters for the service, as required.

- To configure an item on the Components tab, right-click on the item and choose Properties from the contextual menu.
- To configure one or more items listed on another tab, select the items and click on the Properties button.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The VPLS (Edit) form closes, and the Manage Services form reappears.

8 Close the Manage Services form.

Procedure 68-21 To view the service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VPLS (Edit) form opens.

4 View the Aggregated Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab button to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab button to view the aggregated alarms for the object, if required.

8 Click on the Tests tab button if the OAM Validation Failed indicator is enabled. You can view the OAM validation test suite results by clicking on the Validation Result tab.

Note — You can run the OAM Validation test suite for this service from this form by clicking on the Validate button.

9 Close the VPLS (Edit) form.

10 Close the Manage Services form.

Procedure 68-22 To run an OAM validation test

An OAM validator test suite must be created for the tested entity. See chapter 75 for more information about how to create a validator test suite.

Note — OAM validation tests are not supported for HVPLS.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPLS and click on the Properties button. The VPLS (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

- **i** Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form appears.
- **ii** Configure the filter criteria. A list of OAM validator test suites appears.
- **iii** Select an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failed indicator.

6 Click on the Tests tab button. The Test Suite tab is displayed.

7 Click on the Validation Result tab button.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab button to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result form.

14 Close the VPLS (Edit) form.

15 Close the Manage Services form.

Procedure 68-23 To view the service topology

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPLS and click on the Topology View button. The Service Topology map opens.

See chapter 4 for more information about service topology views.

Note — In the VPLS topology map view, a redundant spoke SDP binding under an endpoint displays differing colors, depending on whether it is in the active or backup state. Backup spoke SDP bindings are shown in purple.

4 Close the Service Topology form.

5 Close the Manage Services form.

Procedure 68-24 To modify a VLPS using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the component tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPLS and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains a number of sub-procedures describing the various components that can be created and modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating site components. Go to step 10.
- Creating SDP bindings. Go to step 23.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. You can choose to create one of the following:

- VPLS Site
- VPLS B-Site
- VPLS I-Site

5 Select the required option. The Select Network Elements form appears.

6 Select one or more sites to add to the service and click OK. The VPLS Site (Create), VPLS I-Site (Create), or VPLS B-Site (Create) form is displayed, depending on your menu item selection. If you selected more than one site, the VPLS Site (Multiple Instances) (Create), VPLS I-Site (Multiple Instances) (Create), or VPLS B-Site (Multiple Instances) (Create) form is displayed, depending on your menu item selection.

7 Click on OK. The VPLS Site (Create) (or VPLS Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

8 If you want to perform detailed configuration of site properties for the new site, right-click the site icon and select Properties from the contextual menu. The VPLS Site (Edit) form opens. Refer to Procedure 68-1 for detailed site configuration information.

9 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

Creating site components

10 Right-click on any site icon in the service topology map. A contextual menu is displayed. You can choose to create one of the following:

- VPLS L2 Access Interface (this choice will actually display as either a regular L2 Access Interface, or a B-L2 or I-L2 variant, depending on the site you select). Go to step 11.
- VPLS L2 Management Interface. Go to step 15.
- VPLS Endpoint. Go to step 19.

11 If you choose to create a VPLS L2 Access Interface, then the VPLS L2 Access Interface (Create) form is displayed. If the selected site is a B-Site or I-Site, then the B-L2 or I-L2 Access Interface (Create) form is displayed accordingly.

12 Click on the Port tab and assign a port to the interface.

Refer to Procedure 68-3 (or Procedure 68-13 or 68-14 for B-L2 or I-L2 Access Interfaces respectively) for detailed information on further configuring the interface, if required.

13 Click OK. The VPLS L2 Access Interface (Create) form closes.

14 Go to step 22.

15 If you choose to create a VPLS L2 Management Interface, then the VPLS L2 Management Interface (Create) form is displayed.

16 Click on the Port tab and assign a port to the interface.

Refer to Procedure 68-3 for detailed information on further configuring the interface, if required.

17 Click OK. The VPLS L2 Management Interface (Create) form closes.

18 Go to step 22.

19 If you choose to create a VPLS Endpoint, then the Endpoint (Create) form is displayed.

20 Configure the Name parameter for the endpoint.

Refer to Procedure 68-1 (or 68-11 for B-Sites) for detailed information on further configuring the endpoint, if required.

21 Click OK. The Endpoint (Create) form closes and the new endpoint is displayed in the topology view.

22 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

Creating SDP bindings

23 Select the sites you want to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.

Note 1 — If you intend to create either a spoke or a mesh binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

Note 2 — If you intend to create a full mesh between sites, then the order in which you select the sites is not important.

Note 3 — If you intend to add a service site to an existing mesh of sites, then the first site you select must be the one that is not currently a part of the mesh. The second site you select can be any member of the existing mesh.

24 Select Connect from the contextual menu. Depending on the sites you selected, one or more of the following options are available:

- Create Spoke SDP Binding. Go to Step 25.
- Create Mesh SDP Binding. Go to Step 32.
- Create Full Mesh. Go to Step 39.
- Add To Existing Mesh. Go to Step 46.

25 If you choose the Create Spoke SDP Binding option, then the Spoke SDP Binding (Create) form is displayed.

Note 1 — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

Note 2 — You can also create a spoke SDP binding between a site icon and an endpoint icon, or between two endpoint icons in the topology view. Appropriate endpoints must first exist or be created to enable this.

26 Enable the Auto Select Transport Tunnel parameter.

27 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedure 68-5 for more detailed information on creating and configuring spoke SDP bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 30 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

28 Assuming that the spoke SDP binding was successfully created in step 27, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a spoke binding for the return tunnel.

29 Right-click on the second site you selected and choose the Create Spoke SDP Binding ... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

30 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 30 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

31 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

32 If you choose the Create Mesh SDP Binding option, then the Mesh SDP Binding (Create) form is displayed.

Note — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

33 Enable the Auto Select Transport Tunnel parameter.

34 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Mesh SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedure 68-4 for more detailed information on creating and configuring mesh bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 30 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

35 Assuming that the mesh SDP binding was successfully created in step 34, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a mesh binding for the return tunnel.

36 Right-click on the second site you selected and choose the Create Mesh SDP Binding ... option from the contextual menu. The Mesh SDP Binding (Create) form is displayed.

37 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Mesh SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 30 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

38 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

39 If you choose the Create Full Mesh option, the Complete Vpls Mesh for Service Component form is displayed.

40 Configure the Transport Type parameter.

41 Click the Select button to display the Tunnel Selection Profiles form, if required.

42 Click Search to display a list of available Tunnel Selection Profiles.

43 Click on the desired profile entry and click OK. The Tunnel Selection Profiles form closes and your selection is displayed in the Complete Vpls Mesh for Service Component form.

44 Click OK to accept your selection and close the Complete Vpls Mesh for Service Component form. One of the following will result:

- If available transport tunnels exist between the selected sites, then the new mesh bindings between the sites are created and displayed in the topology view. Refer to Procedure 68-4 for more detailed information on creating and configuring mesh bindings, if required.
- If available transport tunnels do not exist between all the sites, then the new bindings that can be created are displayed, and an error message is also displayed informing you that the full mesh could not be completed. Refer to Chapter 30 for information on how to create the required tunnels. Once the tunnels are created, you can repeat this sub-procedure.

45 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

46 If you choose the Add To Existing Mesh option, the Complete Vpls Mesh for Service Component form is displayed.

47 Configure the Transport Type parameter.

48 Click the Select button to display the Tunnel Selection Profiles form, if required.

49 Click Search to display a list of available Tunnel Selection Profiles.

50 Click on the desired profile entry and click OK. The Tunnel Selection Profiles form closes and your selection is displayed in the Complete Vpls Mesh for Service Component form.

51 Click OK to accept your selection and close the Complete Vpls Mesh for Service Component form. One of the following will result:

- If available transport tunnels exist between the selected sites, then the new mesh bindings between the sites are created and displayed in the topology view. Refer to Procedure 68-4 for more detailed information on creating and configuring mesh bindings, if required.
- If available transport tunnels do not exist between the selected sites, then an error message is displayed to that affect. Refer to Chapter 30 for information on how to create the required tunnels. Once the tunnels are created, you can repeat this sub-procedure.

52 Return to step 3 for a list of other functions you can perform from the topology view or go to step 53 to finish.

53 Close the Service Topology form.

54 Close the Manage Services form.

Procedure 68-25 To delete a VPLS

Note — A VPLS cannot be deleted if the L2 access interface has MSAPs that are in an active state. See chapter 64 for more information about MSAPs.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPLS from the list.

4 Click on the Delete button. A dialog box appears and prompts you to confirm that you understand the implications of deleting the service.

5 Click on the Yes button. The service is deleted and removed from the list.

6 Close the Manage Services form.

69 — Mirror service management

69.1 Mirror service overview

The 5620 SAM GUI implementation of service mirroring provides mirroring of service traffic packets from any service type.

Caution — Service mirroring can affect performance across the network and in the source and destination devices, so must be planned accordingly.

In a mirror service, packets from one or more sources are forwarded to their normal destinations and a copy of the entire packet, or a specified portion of the packet, is sent to the mirror destination. The mirrored packet can be viewed using a packet-decoding device, typically called a sniffer, that is attached to the destination port. The 5620 SAM does not limit the number of destination and source sites added under a mirror service. The mirrored packets are transported unidirectionally through the core network using IP or MPLS tunneling.

With pseudo-wire redundancy support, an ICB can be enabled in the mirror service spoke and remote source, which can provide bidirectional service that enables support for active and standby PE redundancy. An endpoint can be used to group the redundant objects, which may be of mirror SDP bindings or SDP and SAP. In the mirror map view, the color for the active and backup states of the redundant mirror SDP differ.

Service mirroring can be used to do the following:

- Troubleshoot problems with customer packet delivery and content.
- Help service providers meet regulations by providing itemized call records and wiretaps, as authorized by investigative authorities.
- Simplify the complex traffic-analysis networks that are often implemented as overlays to the customer-facing network.

The 5620 SAM supports end-to-end mirror service configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Preconfigured template. A user that is assigned the admin role, or mirror service management with the template management role can create a mirror service template.
- A separate lawful intercept management scope of command role allows a LI user to view and configure LI sources on existing mirror services. Information that is mirrored is hidden from all users who do not have LI user privileges. See chapter 31 for more information about configuring a LI user.

The mirror service operational status is aggregated based on the status of each site.

- Aggregate status is down if all destination sites are down.
- Aggregate status is up if one of the redundant destination site is up.
- Aggregate status is down if all source sites are down.
- Aggregate status is up if one of the redundant source sites is up.
- Aggregate status is unknown if no sites are added to the service.

Consider the following information before you implement a mirror service:

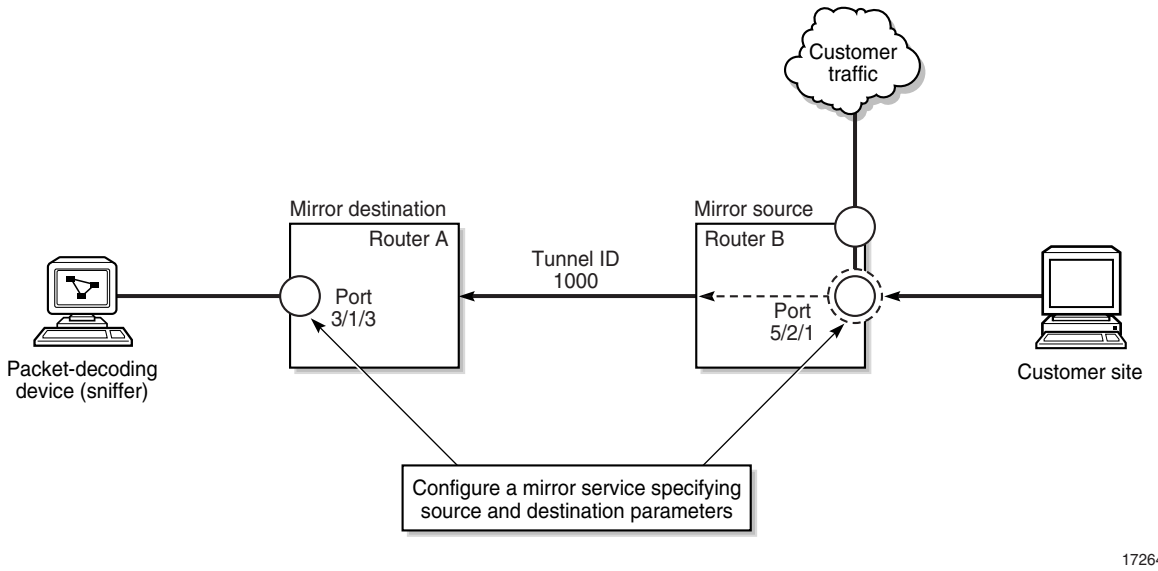
- The default customer is automatically associated with a mirror service. You cannot associate a different customer with a mirror service.
- You can configure one endpoint per mirror site.
- You can configure the endpoint in the destination site with SAP and SDP with ICB.
- An endpoint cannot have more than one SAP.
- You can create a mirror SDP under the endpoint in the destination site.
- You can create up to four mirror SDPs under the endpoint in the source site. One mirror SDP must have ICB. Another option is to create one mirror SDP under the source site.
- When the mirror SDP binding is under an endpoint, the STP cannot be enabled on the spoke.
- Mirror sites with valid SAP are considered as destination sites during discovery.
- You can configure site as destination without SAP in the mirror service. During re-synchronization, site type will be kept as destination.
- Auto-SDP creation is restricted to one destination.
- You can change the redundancy setting of a mirror SDP binding by deleting and adding the mirror SDP binding on an endpoint.
- You cannot delete an MC-LAG SAP if an ICB is on the same endpoint.
- You cannot have a SAP with non-ICB mirror spoke on the same endpoint.
- The destination of a mirror service must be an L2 SAP.
- You must be assigned the administrator or mirror service management scope of command role to create or modify a mirror service, or to view any mirror-related objects in the 5620 SAM.
- You can mirror the ingress or egress traffic on SAPs and ports.
- You can mirror the ingress or egress traffic that is associated with one or more subscriber hosts.
- You can specify match criteria, such as IP addresses, MAC addresses, or MPLS ingress labels, to filter the mirrored traffic.
- Mirror service IDs are obtained from the same pool of IDs that is used by other services. When you manually assign an ID value, ensure that you do not assign an ID that belongs to another service.
- Use the packet-slicing option to copy a specific packet size from each frame. This option is useful for monitoring network usage without copying the customer data. It also limits the amount of mirrored traffic that travels through the core network.
- When the mirror destination is not on the same NE as the mirror source, a mirror service requires a service tunnel between the source and destination NEs.
- The 5620 SAM can automatically create a service tunnel between the source and destination sites when the following conditions are met:
  - Automatic mesh SDP binding creation is enabled.
  - GRE or LDP is the transport type.
  - No other service tunnel is available between the source and destination sites.
- The mirror service source and destination encapsulation types must be the same.

- After an NE reboot or CPM activity switch, the debug configuration file for a mirror service is not by default reloaded on the NE. The 5620 SAM raises an alarm when this occurs. To ensure that the NE reloads the debug configuration file, you must specify the location of the file in the base 5620 SAM configuration. See chapter 5 for more information.
- When multiple mirror services reference the same packet, for example, from a SAP and from a port, the packet is mirrored only once, based on the following criteria in the following non-configurable order:
  - MAC or IP filters
  - MPLS ingress label
  - SAP
  - port
- For IP-only mirroring:
  - Requires chassis mode C or D to be enabled.
  - By using "IP Only" as the encapsulation type, users can specify that only the IP packet is mirrored, without its original ATM/FR/POS/Ethernet DLC header.
  - When IP-only is configured on the source site, users can configure various mirroring sources, including subscribers and SAPs from Ipipe, IES, VPRN, VPLS, and MVPLS services. However, source ports and VLL services including Apipe, Epipe, and Fpipe cannot be configured.
  - For local IP-only mirroring, the source and destination MAC addresses must be configured.
  - For remote IP-only mirroring in a VPRN service, an IP mirror interface on the VPRN destination node is used to receive the IP mirror packets and route them to the appropriate sniffer. If there are multiple sniffers connected to the VPRN using L3 interfaces, users need to configure the routing policy to have IP mirror packets routed to the correct sniffer.
- For LI source configuration:
  - You must be assigned the lawful intercept management scope of command role to view, create or modify any LI-related objects in the 5620 SAM.
  - LI source configurations are saved on an NE when the poller policy for the NE specifies LI Local Save Allowed. See chapter 12 for information about configuring in-band and out-of-band polling policies.

69.2 Sample mirror service configuration

Figure 69-1 shows a sample mirror service configuration.

Figure 69-1 Sample mirror service configuration



In this sample, Router B is the mirror source that carries the customer packets. Router A is the mirror destination. The ingress and egress traffic on Port 5/2/1 is mirrored on the destination, Port 3/1/3. Table 69-1 lists the high-level tasks to configure the sample mirror service.

Table 69-1 Sample mirror service configuration

Task	Description
1. Connect the packet sniffer to the mirror destination.	The packet sniffer is attached to Router A, Port 3/1/3.
2. Configure the mirror destination parameters.	Port 3/1/3 on Router A is specified as the mirror destination. Specify the Tunnel ID 1000 as the transport tunnel to the mirror destination. All the parameters required to configure the type of mirroring, for example, slicing and mirror classification, are specified in the destination parameters.
3. Specify the source entity that is to be mirrored.	The egress and ingress traffic on Port 5/2/1 is to be mirrored.

69.3 Workflow to create a mirror service

1. Verify that an existing service for a customer is configured, available, and turned up.
2. Set up a packet-sniffing device at the L2 SAP that is the destination of the mirror service.
3. Specify the SAP with the attached packet-sniffing device as the mirror destination.

4 Configure the source of the packets to be mirrored.

5 Turn up the mirror service.

69.4 Mirror service procedures

Use the following procedures to create, delete, view, and modify mirror services.

Procedure 69-1 To create a mirror service

1 Choose Create→Service→Mirror from the 5620 SAM main menu. The Mirror Service (Create) form opens with the General tab displayed.

2 Configure the parameters.

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Administrative State
- OLC State

  The OLC State parameter is configurable after you click on the Apply button.

3 Perform one of the following:

a Leave the Automatic SDP Binding Creation parameter disabled.

When you leave the Automatic SDP Binding Creation parameter disabled, you must create SDP bindings for the service and bind the SDPs to a service tunnel in step 46 of this procedure.

b Enable the Automatic SDP Binding Creation parameter.

When you enable the Automatic SDP Binding Creation parameter, SDP bindings for the service are automatically created and bound to service tunnels.

i Configure the Transport Type parameter.

Note 1 — You must select GRE or LDP as the transport type to allow the 5620 SAM to automatically create SDP bindings between the source and destination sites. Automatic creation of SDP bindings cannot be configured if a service tunnel already exists between the source and destination sites.

Note 2 — To use MPLS:RSVP as the transport type, you must bind LSPs to service tunnels during service tunnel configuration. See chapter 30 for more information.

ii Configure the Use Bandwidth-Reserved Paths parameter, if applicable.

The Use Bandwidth-Reserved Paths parameter is configurable only when the Transport Type parameter is set to MPLS:RSVP or Any.

4 Click on the Components tab button.

5 Right click on Destination Site in the service components tree, and choose Create Destination Site from the contextual menu. The Select Network Elements - Mirror Service form opens with a list of available sites displayed.

6 Select a site and click on the OK button. The Select Network Elements - Mirror Service form closes and the Mirror Site (Create) form opens with the system identifier of the selected site displayed in the Network Element panel.

7 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- Encapsulation Type

8 Click on the Mirroring Configuration tab button.

9 Configure the parameters.

- Source Administrative State
- Slice Size
- Forwarding Class
- Enable Port ID Mirroring

Choose the default of 0 for the Slice Size parameter when you configure a destination mirror site, unless slicing at the destination is necessary. Packet slicing reduces the amount of mirrored traffic that traverses the network.

Note — The Slice Size parameter is not displayed if the Encapsulation Type parameter is set to IP Only.

The Port Id Mirroring and remote source are mutually exclusive. If Enable Port ID Mirroring is set to true on the destination site, then a remote source site cannot be added to the service. If a remote source site is already on the service, then Enable Port ID Mirroring cannot be set to true. Also, if remote mirror is used, then Enable Port ID Mirroring must be configured on all source sites.

10 Click on the Source Far Ends tab button.

11 Click on the Add button. The Remote Source (Create) form appears.

12 Configure the parameters.

- Remote Site ID
- Ingress Label
- Remote VC ID
- Remote ICB

13 Click on the OK button. The Remote Source (Create) form closes and a dialog box appears.

14 Click on the OK button. The Mirror Site (Create) form displays the remote source information.

15 Click on the OK button. The Site (Create) form closes and a dialog box appears.

16 Click on the OK button. The Mirror Service (Edit) form reappears with the service components tree displayed.

17 Expand the Destination Site object to reveal the newly created site.

18 Expand the newly created destination site object.

19 Configure an L2 access interface as the mirror destination by selecting L2 Access Interface (Test Equipment Interface) under the destination site in the service components tree, right-clicking on it and choosing Create L2 Access Interface from the contextual menu. The L2 Access Interface (Create) form opens with the General tab displayed.

20 Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

21 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

22 Configure the parameters.

- Outer Encapsulation Value
- Auto-Assign ID
- Inner Encapsulation Value

The Auto-Assign ID parameter is configurable if the port uses Dot1 Q encapsulation. When the parameter is enabled, the 5620 SAM automatically configures the Outer Encapsulation Value parameter using the lowest unassigned value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

23 Assign an egress QoS policy to the interface, if required.

i Click on the QoS tab button.

ii Configure the Egress Mark QinQ Top Bits Only parameter.

iii Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - L2 Access Interface form opens.

iv Configure the filter criteria. A list of egress policies appear at the bottom of the Select Egress Policy - L2 Access Interface form.

v Select an egress policy and click on the OK button. The Select Egress Policy - L2 Access Interface form closes and the L2 Access Interface (Create) form refreshes with the egress QoS policy information displayed.

24 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab button.

ii Click on the Select button beside the Name parameter. The Select Time Of Day Suite - L2 Access Interface form opens.

iii Select a time of day suite and click on the OK button. The Select Time Of Day Suite - L2 Access Interface form closes and the L2 Access Interface (Create) form refreshes with the time of day suite information displayed.

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Mirror (Create) form refreshes with the L2 access interface information displayed below L2 Access Interface (Test Equipment Interface) in the service components tree.

25 Click on the Schedulers tab button, if required.

26 Configure the Egress Aggregate Rate Limit (kbps) parameter.

27 Click on the IP Mirror MAC Addresses tab, if you are configuring local mirroring and you chose IP Only as the encapsulation type in step 7. Otherwise, go to step 29.

Note — If you want to configure remote mirroring in a VPRN service, you must create an IP Mirror Interface in that service. See chapter 71 for more information.

28 Configure the parameters:

- Destination MAC Address
- Source MAC Address

Note — The Source and Destination MAC addresses on L2 Access Interface must be both null or neither null. Both null means that there are no source or destination MAC addresses configured on the interface.

29 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button.

ii Click on the Add button. The ANCP Static Map (Create) form opens.

iii Configure the ANCP String parameter.

iv Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. The ANCP Static Map form closes.

30 Create an endpoint on the mirror site for redundancy support, if required.

i Right-click on the Endpoints object below the site in the service components tree and choose Create Endpoints from the contextual menu. The Endpoint (Create) form opens.

ii Configure the parameters.

- Name
- Description
- Revert Time (seconds)
- Disable Revert Time (Infinite)

iii Click on the Ok button.

For the destination site, the L2 Access Interface (Test Equipment Interface) and Mirror SDP Binding objects appear under the Endpoints object.

For the source site, the Mirror SDP Binding object now appears under the Endpoints object.

iv To create an L2 access interface as the mirror destination, right-click on the L2 Access Interface (Test Equipment Interface) object under the Endpoints object and choose Create L2 Access Interface from the contextual menu. The L2 Access Interface (Create) form opens with the General tab displayed.

v Click on the Port tab button.

vi Click on the Select button to choose a port for the L2 access interface. The Select Terminating Port - L2 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

vii Use the configurable filter and Search button to choose a port, and click on the Search button. The Select Terminating Port - L2 Access Interface form closes, and the L2 Access Interface (Create) form displays the port information.

viii Configure other parameters, as required.

ix Click on the OK button on the L2 Access Interface (Create) form. The form closes and a dialog box appears.

x Click on the OK button. The SAP object appears under the L2 Access Interface object.

xi To create a mirror SDP binding on the endpoint, right-click on the Mirror SDP Binding object under the Endpoints object in the service components tree and choose Create Mirror SDP Binding from the contextual menu. The Mirror SDP Binding (Create) form opens.

xii Configure the parameters.

- Tunnel Termination Site
- VC ID
- Auto-Assign ID
- Ingress Label
- Egress Label
- Inter-Chassis Backup
- Precedence

xiii Click on the OK button. The Mirror SDP Binding (Create) form closes and a dialog box appears.

xiv Click on the OK button. The Mirror Service (Edit) form reappears with the service components tree displayed.

31 A mirror source can be on the same site as the mirror destination. If no mirror sources are on the destination site, go to step 38.

32 Specify a SAP on the site as a mirror source, if required. Perform one of the following:

a Right-click on the Source SAPs object below the site in the service components tree and choose Create Source Interface from the contextual menu. The Source Interface (Create) form opens. Go to step i.

b Right-click on the LI Source SAPs object below the site in the service components tree and choose Create LI Source Interface from the contextual menu. The LI Source Interface (Create) form opens. Go to step i.

Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

i Click on the Select button to choose an access interface to associate with the source interface. The Select Mirrored Interface - Source Interface form opens.

ii Use the configurable filter and Search button to choose an access interface, and click on the OK button. The Select Mirrored Interface - Source Interface form closes and the Source Interface (Create) form refreshes with the selected interface information displayed.

iii Configure the parameters.

- Enable Egress
- Enable Ingress

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Mirror Service (Create) form refreshes with the source SAP displayed below Source SAPs in the service components tree.

vi Repeat steps i to v to specify an additional source SAP for the site.

33 Specify a port on the site as a mirror source, if required.

i Right-click on the Source Ports object below the site in the service components tree and choose Create Source Port from the contextual menu. the Source Port (Create) form opens

ii Click on the Select button to choose a port. The Select - Source Port form opens.

A source port can be one of the following:

- physical port
- channel
- LAG
- bundle
- CCAG

iii Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Source Port form closes and the Source Port (Create) form displays the port information.

iv Configure the parameters.

- Enable Egress
- Enable Ingress

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Mirror Service (Create) form refreshes with the source port displayed below Source Ports in the service components tree.

vii Repeat steps i to v to specify an additional source port for the site.

34 Specify an IP filter entry for the mirror source, if required. Perform one of the following:

a Right-click on the Source IP Filters object below the site in the service components tree and choose Create Source IP Filter from the contextual menu. The Source IP Filter (Create) form opens. Go to step i.

b Right-click on the LI Source IP Filters object below the site in the service components tree and choose Create LI Source IP Filter from the contextual menu. The LI Source IP Filter (Create) form opens. Go to step i.

Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

i Click on the Select button to choose an IP filter entry. The Select Filter - Source IP Filter form opens.

ii Use the configurable filter and Search button to choose an IP filter entry, and click on the OK button. The Select Filter - Source IP Filter form closes and the Source IP Filter (Create) form refreshes with the selected IP filter ID and IP filter entry ID displayed.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The Mirror (Create) form refreshes with the source IP filter displayed below Source IP Filters in the service components tree.

v Repeat steps i to iv to specify an additional source IP filter.

35 Specify a MAC filter entry for the mirror site, if required. Perform one of the following:

a Right-click on the Source MAC Filters object below the site in the service components tree and choose Create Source MAC Filter from the contextual menu. The Source MAC Filter (Create) form opens. Go to step i.

b Right-click on the LI Source MAC Filters object below the site in the service components tree and choose Create LI Source MAC Filter from the contextual menu. The LI Source MAC Filter (Create) form opens. Go to step i.

Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

i Click on the Select button to choose a MAC filter entry. The Select Filter - Source Mac Filter form opens.

ii Use the configurable filter and Search button to choose a MAC filter entry, and click on the OK button. The Select Filter - Source Mac Filter form closes and the Source MAC Filter (Create) form refreshes with the selected MAC filter ID and MAC filter entry ID displayed.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The Mirror (Create) form refreshes with the source MAC filter displayed below Source MAC Filters in the service components tree.

v Repeat steps i to iv to specify an additional source MAC filter.

36 Specify an MPLS ingress label for the mirror, if required.

i Right-click on the Source MPLS Ingress Labels object below the site in the service components tree and choose Create Source Ingress Label from the contextual menu. The Source Ingress Label (Create) form opens.

ii Configure the Ingress Label parameter.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The Mirror (Create) form refreshes with the MPLS ingress label displayed below Source MPLS Ingress Labels in the service components tree.

v Repeat steps i to iv to specify an additional source MPLS ingress label.

37 Specify a subscriber as a mirror source, if required. Perform one of the following:

a Right-click on the Source Subscribers object below the site in the service components tree and choose Create Source Subscriber from the contextual menu. The Source Subscriber (Create) form opens. Go to step i.

b Right-click on the LI Source Subscribers object below the site in the service components tree and choose Create LI Source Subscriber from the contextual menu. The LI Source Subscriber (Create) form opens. Go to step i.

Note 1 — A 5620 SAM operator with LI privileges can view, create, and delete LI source objects.

Note 2 — A mirror site can be configured with debug or LI sources, but not both. LI source configuration takes priority over debug source configuration.

i Configure the following parameters:

- Subscriber Identification String
- Forwarding Classes
- Enable Egress
- Enable Ingress

ii You can further restrict the mirrored subscriber host traffic associated with the subscriber identification string by specifying SAP or SLA-profile criteria. To specify an SLA profile as a match criterion, go to step viii.

Note — You can configure parameters in the SAP/Subscriber Host Match Criteria panel or the SLA Profile Match Criteria panel, but you cannot configure parameters in both panels.

iii Click on the Select button in the SAP/Subscriber Host Match Criteria panel to specify a SAP on which to mirror subscriber host traffic. The Select SAP ID/Encap Value - Source Subscriber form opens.

iv Configure the filter criteria and click on the Select button. A list of SAPs is displayed.

Note — The form lists only Dot1Q- or QinQ-encapsulated SAPs that have subscriber management enabled.

v Select a SAP in the list and click on the OK button. The Select SAP ID/Encap Value - Source Subscriber form closes and the SAP information is displayed on the Source Subscriber (Create) form.

vi Configure the parameters in the SAP/Subscriber Host Match Criteria panel to specify the subscriber host match criteria for the SAP:

- Host IP Address
- Host MAC Address

Note — The 5620 SAM does not accept the parameter values unless a SAP is specified in step v.

vii Go to step x.

viii Click on the Select button in the SLA Profile Match Criteria panel. The SLA Profile - Source Subscriber form opens.

ix Select an SLA profile in the list and click on the OK button. The Select SLA Profile - Source Subscriber form closes and the SLA profile name is displayed on the Source Subscriber (Create) form.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The Mirror Service (Create) form refreshes with the source subscriber listed below Source Subscribers in the service components tree.

xii Repeat steps viii to xi to specify an additional source subscriber, if required.

38 To configure a mirror source on a site other than the destination site, right-click on Source Sites in the service components tree and choose Create Source Site from the contextual menu. Otherwise, go to step 60.

39 The Select Network Elements - Mirror form opens with a list of available sites displayed. Select a site and click on the OK button. The Select Network Elements - Mirror form closes and the Mirror Site (Create) form opens with the system identifier of the selected site displayed.

40 Configure the parameters.

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- Encapsulation Type

41 Click on the Mirroring Configuration tab button.

42 Configure the parameters.

- Source Administrative State
- Slice Size
- Forwarding Class
- Enable Port ID Mirroring

Note — The Slice Size parameter is not displayed if the Encapsulation Type parameter is set to IP Only.

The Port Id Mirroring and remote source are mutually exclusive. If Enable Port ID Mirroring is set to true on the destination site, then a remote source site cannot be added to the service. On the other hand, if a remote source site is already on the service, then Enable Port ID Mirroring cannot be set to true. Also, if remote mirror is used, then Enable Port ID Mirroring must be configured on all source sites.

43 Click on the OK button. A dialog box appears.

44 Click on the OK button. The Mirror Site (Create) form closes, and the Mirror Service (Create) form reappears with the Components tab displayed. The service components tree is refreshed with the selected site displayed under Source Sites.

45 Expand the newly created site object.

46 Perform one of the following:

a If the Automatic SDP Binding Creation parameter was disabled in step 3, choose an SDP binding for the mirror source by selecting Mirror SDP Binding under the source site in the service components tree and then right-clicking and choosing Create Mirror SDP Binding from the contextual menu.

b Go to step 52.

47 The Mirror SDP Binding (Create) form opens. Specify a destination node for the mesh SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter to choose a destination for the SDP binding. The Select Destination Network Element - Mirror SDP Binding form opens.

ii Select a node and click on the OK button. The Select Destination Network Element - Mirror SDP Binding form closes and the Mirror SDP Binding (Create) form refreshes with the destination node ID displayed in the Tunnel Termination Site panel.

b If the destination node is not managed by the 5620 SAM, specify the system ID of the destination node for the Tunnel Termination Site parameter.

48 Configure the parameters.

- VC ID
- Auto-Assign ID
- Ingress Label
- Egress Label
- Inter-Chassis Backup
- Precedence

49 Perform one of the following to specify a transport tunnel for the mirror SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Mirror SDP Binding form opens.

ii Select a service tunnel for the mirror SDP binding and click on the OK button. The Select Tunnel - Mirror SDP Binding form closes, and the Mirror SDP Binding (Create) form refreshes with the service tunnel identifier.

50 Click on the OK button. A dialog box appears.

51 Click on the OK button. The Mirror SDP Binding (Create) form closes and the Mirror (Create) form refreshes with the mirror SDP binding displayed under Mirror SDP Binding for the site.

52 To specify an endpoint on the site as a mirror source, perform step 30.

53 To specify one or more SAPs on the site as mirror sources, perform step 32.

54 To specify one or more ports on the site as mirror sources, perform step 33.

55 To specify one or more IP filters for the source site, perform step 34.

56 To specify one or more MAC filters for the source site, perform step 35.

57 To specify one or more MPLS ingress labels for the source site, perform step 36.

58 To specify one or more subscribers or subscriber hosts as mirror sources, perform step 37.

59 Perform one of the following:

a Configure an additional source site for the mirror service. Perform steps 38 to 57.

b Complete the mirror service configuration. Go to step 60.

60 Click on the OK button. A dialog box appears.

61 Click on the Yes button. The Mirror Service (Create) form closes.

Procedure 69-2 To modify a mirror service

Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria. A list of mirror services appears at the bottom of the Manage Mirror Services form.

3 Select a mirror service and click on the Properties button. The Mirror *Service Name* (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the other tab buttons to edit additional properties, as required.

5 Modify the parameters on the appropriate tab, as required.

To configure items in the Components tab, select and right-click on the items and choose Properties from the contextual menu.

To configure items in the tabs that contain lists of service elements, select the items and click on the Properties button.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button to confirm the action. The Mirror *Service Name* (Edit) form closes and the Manage Mirror Services form reappears.

8 Click on the Close button to close the Manage Mirror Services form.

Procedure 69-3 To view LI mirrored subscriber hosts configured with a RADIUS server

Note 1 — You must have 5620 SAM LI user privileges to perform this procedure.

Note 2 — Before you can perform this procedure, at least one LI user account must exist on the NE.

Note 3 — Before you can perform this procedure, a 5620 SAM LI user must enable LI discovery for the NE using Procedure 31-6.

Note 4 — Only PPPoE subscriber hosts can be mirrored with RADIUS.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria, if required, and click on the Search button. A list of mirror services appears.

3 Choose a mirror service and click on the Properties button. The Mirror *Service Name* (Edit) form opens with the General tab displayed.

4 Click on the Sites tab button. A list of mirror service sites are displayed.

5 Choose a site and click on the Properties button. The Mirror Site (Edit) form opens with the General tab displayed.

6 If an LI source configuration object has not been created, the LI Source Configuration tab button is dimmed. Click on the Create LI Source Configuration button at the bottom of the form. A dialog box appears.

Note 1 — You must create an LI source configuration object for the NE to mirror subscriber hosts for LI.

Note 2 — The Create LI Source Configuration button is a toggle that also lets you delete an LI source configuration object. If you delete an LI source configuration object, all associated LI source objects are deleted.

Note 3 — An LI source configuration object is automatically created when an LI source object is created.

7 Click on the OK button. The LI Source Configuration tab button is enabled, and an LI source configuration object is created.

8 Click on the LI Source Subscribers Via RADIUS tab button.

9 Configure the filter criteria, if required, and click on the Search button. A warning box appears.

10 Click on the OK button. A list of subscribers appears.

11 Choose a subscriber and click on the Properties button. The LI Source Subscriber Host form opens.

12 View the information on the form.

13 Close the LI Source Subscriber Host form.

Procedure 69-4 To view the service operational status

The Aggregated Service Site Operational State and State Cause indicators on the General tab of the mirror service management form display information about service faults.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria. A list of mirror services appears at the bottom of the Manage Mirror Services form.

3 Select a mirror service and click on the Properties button. The Mirror *Service Name* (Edit) form opens.

4 View the Aggregated Service Site Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab button to view the alarms for the object. The alarms are grouped into various categories.

7 Close the Mirror Service (Edit) form.

8 Close the Manage Mirror Services form.

Procedure 69-5 To run an OAM validation test

An OAM validator test suite must be created for the tested entity. See chapter 75 for more information about how to create an OAM validator test suite.

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Mirror Services form.

3 Select a service and click on the Properties button. The Mirror Service (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

   i Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form appears.

   ii Configure the filter criteria. A list of OAM validator test suites appears.

   iii Select an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab button.

7 Click on the Validation Result tab button.

8 Select an entry and click on the Properties button. The Tested Entity Result form opens and displays information about the validation test.

9 Close the Tested Entity Result form.

10 Close the Mirror Service (Edit) form.

11 Close the Manage Mirror Services form.

Procedure 69-6 To view the service topology

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter parameters and click on the Search button. A list of services appears at the bottom of the Manage Mirror Services form.

3 Select a mirror service and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - *Service Name* map opens.

See chapter 4 for more information about service topology views.

Procedure 69-7 To delete a mirror service

1 Choose Manage→Service→Mirror Services from the 5620 SAM main menu. The Manage Mirror Services form opens.

2 Configure the filter criteria. A list of mirror services appears at the bottom of the Manage Mirror Services form.

3 Choose a mirror service.

4 Click on the Delete button. A dialog box appears and prompts you to confirm that you understand the implications of deleting the service.

5 Click on the Yes button to confirm the action. The mirror service is deleted and removed from the list.

6 Close the Manage Mirror Services form.

70 — IES management

70.1 IES management overview

An IES is a routed connectivity service in which the customer traffic passes through an L3 IP router interface to the Internet.

IES allows customer-facing IP interfaces in the same routing instance to be used for service network core-routing connectivity. IES requires that the IP addressing scheme that is used by the customer be unique among other provider addressing schemes and potentially the entire Internet.

Packets that arrive at the edge device are associated with an IES based on the access interface on which they arrive. An access interface is uniquely identified using:

- port
- service ID
- IP address

IES configuration

The 5620 SAM supports end-to-end IES configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Preconfigured template. A user that is assigned the template management role can create a service template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

The 5620 SAM supports the configuration in IES of an L3 aggregation mechanism called routed CO. Routed CO uses DHCP relay to manage dynamic subscriber hosts; the network resources for static subscriber hosts are explicitly provisioned. Routed CO supports all residential subscriber management functions of the 5620 SAM. See chapter 64 for more information about residential subscriber management and routed CO.

Routed CO uses a subscriber interface that defines up to 16 subnets for NE releases earlier than 7.0, or up to 256 subnets for NEs at Release 7.0 or later. A subscriber interface has child objects called group interfaces. A group interface supports the configuration of multiple SAPs as child objects. A SAP in a group interface supports all residential subscriber management functions. A group interface does not allow the specification of IP subnets or addresses, but inherits the addressing scheme of the parent subscriber interface. The 5620 SAM service topology map displays IES subscriber interfaces, group interfaces, and the associated SAPs.

You can configure Network Address Translation, or NAT, for dynamic subscriber hosts in a routed CO deployment. NAT implementation in an IES requires a NAT configuration on the NE base routing instance and a NAT policy that is associated with a subscriber profile. See chapter 27 for information about configuring and deploying NAT on a base routing instance. See chapter 43 for information about configuring a NAT policy. See chapter 64 for information about associating a NAT policy with a subscriber profile.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default Service Tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology views. See chapter 72 for more information about the hierarchical organization of composite services.

Common to all device services, such as IES, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces or circuits, when the service is configured or modified. The following policies are common to all device services:

- QoS policies define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy form, the Access Egress Policy form, and the ATM QoS Policy form.
- Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy form.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy form.
- Filter policies control network traffic into or out of an interface or circuit based on IP or MAC matching criteria. Filter policies are configured using the ACL IP Filter form and the ACL MAC Filter form.
- Accounting policies measure the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy form.
- ANCP policies provide status and control information based on port-up and port-down messages and current line rate changes between the edge device and the access node. ANCP policies are configured using the Manage Subscriber Policies form.
- Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination. Routing policies are configured using the Routing Policy Manager.
- Time of day suites specify time and day restriction policies that are assigned to QoS policies and schedulers, ACL filters, and aggregation schedulers. Time of day suites and time range policies are configured using the Time of Day Suite form and Time Range form, respectively.

See chapter 43 for more information about policies.

Although IES is part of the routing domain, the usable IP address space may be limited. IES allows a portion of the service provider address space to be reserved for service IP provisioning and to be administered by a separate, but subordinate, address authority.

Multiple IESs can be created to separate customer-owned IP interfaces. More than one IES can be created for one customer. More than one IP interface can be created in one IES. All IP interfaces created in an IES belong to the same customer.

The IES IP interfaces are restricted to the routing protocols that can be defined on the interface based on the fact that the customer has a different routing domain for this service. The IP interfaces support the following routing protocols:

- RIP
- OSPF
- BGP
- IS-IS
- PIM
- IGMP

Customer routes can be advertised to the network core using static routes, RIP, or BGP. BGP and static routes are the most commonly used routing methods.

IPCP extensions allow you to configure IP addresses and DNS names of remote devices to enable inter-operability with other networks. Specifically setting an IPCP extension is necessary to connect to a mobile service provider network. Routers for mobile services rely on other network routers to provide IP addresses and DNS names (primary and secondary) for a PPP link.

When an IPCP extension is configured, an edge device configured with PPP/MLPPP can signal a far end device.

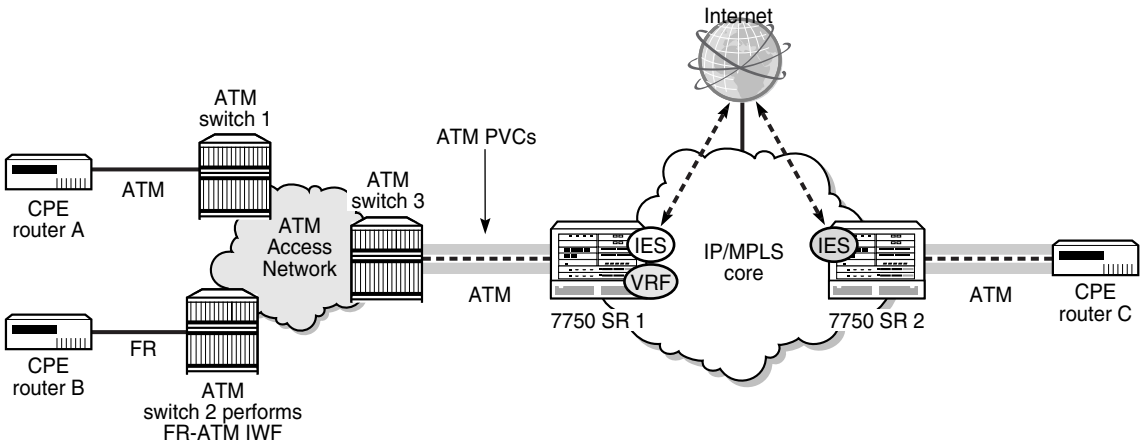
An IES can be connected to a VLL service or to a VPLS by an internal cross-connect through a CCAG adapter. This configuration eliminates the need for the physical port, cable, and other MDA-specific components and results in a less costly and more reliable interconnection. See chapter 72 for information about joining services to form composite services.

ATM SAP terminations for IES

CE routers that have access to an ATM network can connect with an IES service using ATM SAP terminations on a 7750 SR or 7710 SR. The interconnection between ATM point-to-point and L3 services uses RFC 2684-encapsulated IPv4 traffic over an ATM PVC that terminates on a specially configured SAP. All RFC 2684-encapsulated traffic can be routed over ATM networks, frame relay, and directly through ATM connections.

Figure 70-1 shows how CPE router A in an existing ATM network can access L3 IP services, such as an IES, using a statically configured ATM PVC on a 7750 SR (SR #1). CPE router B is connected to a Frame Relay, which connects to ATM switch 2 through IWF (service interworking). The RFC 2684-encapsulated traffic moves from both CPE routers through the ATM access network to a SAP configured on a 7750 SR #1 to serve a specific IES. At the same time, SDPs on the router are configured to a service to forward traffic over the IP/MPLS core. Destination CPE router C can receive RFC 2684-encapsulated traffic over an IP network over an ATM switch connected directly using 7750 SR #2.

Figure 70-1 ATM SAP network connection to an IES

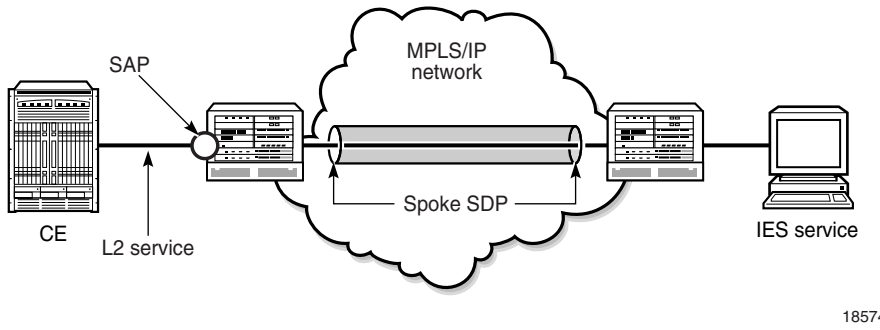


The two connection methods used between an ATM network and the IES router: LLC/SNAP encapsulation and VC multiplexing.

A VLL Epipe service can terminate directly on an IES service using an SDP spoke on the 7750 SR or 7450 ESS. Traffic that terminates on an IES service is identified by the interface ID of the SDP on the L2 access router and the VC ID label in the service packet. All routing protocols supported by IES are also supported for spoke SDP termination.

Figure 70-2 shows a spoke SDP terminating directly on an IES. The spoke SDP could be tied to VLL Epipe or VPLS. No configuration is required for the CE-to-PE connection on the SAP.

Figure 70-2 SDP spoke termination on an L2 service



Routed CO dual homing using SRRP

Subscriber Router Redundancy Protocol (SRRP) allows two separate connections to an access NE such as DSLAM to operate in an active/standby configuration similar to the way in which VRRP interfaces operate. SRRP is a collection of functions and messaging protocols that allows a system to create a set of redundant gateway IP addresses that are shared by a local and remote NE.

Each SRRP instance is created within the context of a subscriber group IP interface and is identified by a unique SRRP instance ID. This SRRP instance ID only needs to be unique in the context of a specific NE. This SRRP instance controls the redundant routing for all subscriber subnets configured or associated with the group interface. One SRRP instance is supported for each group interface and the SRRP ID must be the same as the SRRP instance ID on the group IP interface on the redundant NE.

A subscriber subnet redundant gateway IP host address is assigned at the subscriber IP interface level and is used for all SRRP instances associated with the subscriber subnet. The redundant IP host address must be configured for a subscriber subnet before it can be associated with an SRRP instance.

When SRRP is active on a group interface, the SRRP instance advertises to a remote NE using in-band messaging on the group-interface SAPs and out-of-band messaging on the group-interface redundant interface. If the remote NE uses the same SRRP instance ID, one NE enters a master state, while the other NE enters a backup state. Since the NEs share a common SRRP gateway MAC address (used for the SRRP gateway IP address and for proxy ARP functions), either NE can act as the default gateway for the attached subscriber hosts. This functionality helps to preserve subscriber QoS enforcement. The master state allows routing to and from the subscriber hosts associated with the group IP interface. The backup state stops ingress forwarding for packets destined to the SRRP gateway MAC and causes all packets destined to subscriber hosts on the group IP interface to be forwarded to a redundant IP interface associated with the group IP interface.

Normally, when anti-spoofing is enabled on a group-interface SAP, the SAP drops SRRP packets because they do not contain a subscriber MAC or IP address. However, you can use a configuration option to enable anti-spoofing for subscriber hosts on a group-interface SAP that participates in SRRP advertisements.

The underlying mechanism to control master/backup state transitions is based on a dynamic priority level maintained by the SRRP instance. The SRRP instance with the highest priority level assumes the master operating state. An SRRP instance with a higher current priority level always preempts an SRRP instance with a lower priority level. If the priority levels are equal, the SRRP instance with the lowest source SRRP host IP address assumes the master state. The local SRRP instance priority may also be controlled by associating the instance with an existing VRRP policy.

The redundant IP interface is a special interface that connects two systems with one or more common SRRP instances. The interface is configured with a /31 address and a spoke SDP binding, creating an Ethernet pseudowire shortcut between the redundant NEs. When the SRRP instance is in backup state, the group interface associated with this instance is not allowed to forward or route traffic downstream towards the subscriber. As a result of this, the packets are shunted across the redundant interface so that the active group interface does the forwarding or routing.

If the redundant IP interface goes down, the system allows the group IP interfaces associated with the down interface to forward locally downstream, when they are in the backup SRRP state. While forwarding downstream in the backup state, the system uses the MAC address associated with the group IP interface, not the SRRP redundant gateway MAC address.

SRRP is supported on the 7450 ESS in mixed mode, 7710 SR and 7750 SR.

DoS protection

The 7450 ESS-7, 7450 ESS-12, 7750 SR-7, and 7750 SR-12 support DoS protection policies.

To protect an IES from a high incoming packet rate that characterizes a DoS attack, you can use the 5620 SAM to create DoS protection policies for the IES L3 access interfaces. A DoS protection policy limits the number of control-plane packets that an interface receives each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

You can configure a DoS protection policy to control the following on an IES L3 access interface:

- the control-plane packet arrival rate per subscriber host on the interface
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

Each IES L3 access interface on an NE that supports DoS protection is automatically assigned a default DoS protection policy. This default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified. See Procedure 18-3 for information about creating a DoS protection policy.

Local DHCP servers

The 5620 SAM supports configuring local DHCP servers on the 7710 SR, 7750 SR, and the 7450 ESS. The local DHCP server leases IP addresses to clients in the network. Options are configured to define the IP address properties, such as, the length of time an IP address is active and which DNS server must be used. A local user database is used to authenticate and authorize clients requesting IP addresses from the local DHCP server. If the local DHCP server does not use the local user database, the server can use the GI address to assign free IP addresses, however it is not possible to configure match or authentication parameters.

Three applications are targeted for the Local DHCP server.

- Subscriber aggregation in a single node or TPSDA.
- Business services running VPRN and locally attached to the host can request and obtain IP addresses directly from the server.
- The DHCP server identifies an IP request from a PPPoE client and provides an IP address and options.

DHCP servers can be integrated with Enhanced Subscriber Management for DHCP and PPPoE clients. A local DHCP server can be created in the routing instance window or VPRN service site window. A local DHCP server created in the VPRN service site can be associated with the L3 access interface on a VPRN service only. A local DHCP server created in the routing instance window can be associated with a network interface or L3 access interface on IES.

Local user database

The 5620 SAM supports the configuration of a local user database on the 7450 ESS, 7750 SR, and 7710 SR. A local database is configured and associated with the local DHCP server to provide local authentication. The local DHCP server must have a pool of IP addresses configured or it is not able to lease IP addresses.

A create local user database configuration form is available from the Manage Residential Subscribers form. After a local user database is configured, it can be associated with a local DHCP server and PPPoE configurations on group interfaces.

When a local user database is not configured, you can use GI addresses to access free IP addresses, however the clients requesting the IP address are not authenticated.

PPPoE protocol on IES

An IES can be configured to support PPPoE. PPPoE is used in subscriber networks to encapsulate PPP frames inside Ethernet frames. PPPoE combines the point-to-point protocol used by DSL sessions with Ethernet framing to support multiple subscribers in a LAN. Using the group interface configuration form, you can assign a PPPoE policy and a local user database to authenticate PPPoE subscribers.

L2TP configuration for IES

An IES group interface can be configured to terminate LNS PPP sessions. L2TP is a session-layer protocol that extends the PPP model by allowing L2 and PPP endpoints to reside on different devices that are interconnected by a PSN. L2TP extends the PPP sessions between the CPE and PPP/L2TP termination points on the L2TP network server (LNS), via an intermediate L2TP access concentrator (LAC). The LAC is the initiator of session-generated L2TP tunnels; the LNS is the server that waits for new tunnels. Manually configured and initiated L2TP tunnels can be initiated or stopped from either the LNS or LAC.

After a tunnel is established, the network traffic between the peers is bidirectional. If a tunnel carrying a session fails, another tunnel from the same tunnel group re-establishes the session. Within each L2TP tunnel, one or more L2TP sessions can exist. Each L2TP session transports PPP packets.

At least one ISA-LNS group must be configured for the LNS NE.

On an LNS NE, L2TP destinations configured for L2TP tunnel profiles can include the following:

- loopback L3 access interfaces for a VPRN or IES service
- loopback interfaces configured for a base routing instance

Note — On the LAC NE, each L2TP tunnel must have the local IP address set to the system interface IP address. This restriction applies only to the 7750 SR, Release 7.0.

See chapter 15 for more information about ISA-LNS groups. See Procedure 17-19 for information about creating and configuring an ISA-LNS group. See chapter 28 for more information about L2TP. See Procedure 70-8 for information about configuring an IES group interface to terminate LNS PPP sessions.

70.2 Sample IES configuration

Figure 70-3 shows a sample IES configuration.

Figure 70-3 Sample IES configuration

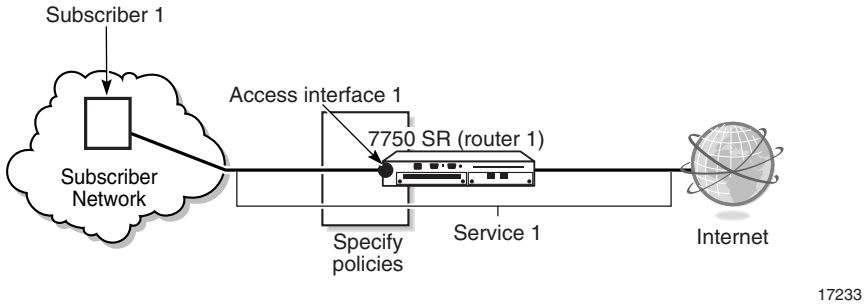


Table 70-1 lists the high-level tasks necessary to configure this sample IES.

Table 70-1 Sample IES configuration

Task	Description
1. Configure policies as required	Policies should be configured prior to creating a service. Participation in policies by access interfaces is defined when you configure or modify access interfaces during service creation or modification. The following key policies can be applied to resources that are part of an IES. • QoS access ingress and egress interface policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress to open these forms. • Scheduler policy. Choose Policies→QoS→SROS QoS→Scheduler to open the scheduler policy form. • ACL IP filter policies. Choose Policies→Filter→ACL IP Filter to open the IP filter form. • Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form. • ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form.
2. Create and configure Subscriber 1	Choose Manage→Service→Customers to open the customer manager form and create a customer.

(1 of 2)

Task	Description

3. Create and configure Service 1	Ensure that the operator creating the service has Service Mgmt and Interface Mgmt user group privileges. See chapter 8 for more information about user and user group privileges.
	Choose Create→Service→IES. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure Service 1.
	• Choose Subscriber 1 as the customer for the IES.
	• Choose router 1 as the site for the IES.
	• Create and configure Access interface 1. You do the following to configure an access interface:
	  • Configure general parameters such as a name, ID, and MAC address.
	  • Specify a port that is in access or hybrid mode.
	  • Add unicast routing protocols as required.
	  • Assign ingress and egress QoS policies, as required.
	  • Add multicast routing protocols as required.
	  • Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
	  • Assign ACL filter policies as required.
	  • Assign an accounting policy, if required.
	  • Specify a local DHCP server, if required.
	  • Specify a ToD suite, if required.
	  • Configure subscriber management parameters, if required.
	  • Specify a DoS protection policy, if required.
	  • Specify one or more IP addresses for the IES access interface: one primary IP address and, optionally, multiple secondary IP addresses.
	  • Specify BFD parameters as required.
	  • Configure the ARP timeout and proxy ARP settings, if required.
	  • Configure IPCP parameters, if required.
	  • Configure ICMP parameters, if required.
	  • Configure DHCP parameters, if required.
	  • Configure ARP host configuration, if required.
	  • Configure VRRP parameters, if required.
	  • Configure anti-spoofing parameters, if required.
	  • Create a MEP, if required.
	  • Configure router advertisement parameters.
	  • Create QoS policy overrides, if required.
	  • Configure ANCP parameters, if required.

(2 of 2)

70.3 Workflow to create an IES

1 Set up group and user access privileges.

2 Configure the network.

i Build the IP core network. You do not need an IP/MPLS network for IESs.

ii Configure routing protocols.

Note 1 — PIM and IGMP are applied to an IES after the service is created. For information about how to apply PIM to an IES, see Procedure 70-5. For information about how to apply IGMP to an IES, see Procedure 70-4.

Note 2 — RIP, IS-IS and OSPF are applied to an IES after the service is created. For information about how to apply RIP, IS-IS, or OSPF to an IES, see Procedure 70-2. For information about how to apply RIP, IS-IS, or OSPF to an IES L3 interface, see Procedure 70-3.

iii Make access ports available on the router.

3 Configure policies, as required.

4 Provision the service.

i Create a new customer or use an existing customer for the new service.

ii Configure customer-specific QoS, filter, scheduling, accounting, and time of day suite policies, or use pre-defined policies.

iii Create the IES.

- Define the service type as IES.
- Choose a router as the IES site.
- Create an L3 access interface.
- Apply policies to the service, as required.

iv Apply routing protocols, such as OSPF, RIP, or IS-IS, to the IES site or interface, if required.

v Add IGMP or PIM interfaces to the IES, if required.

5 Turn up the service.

70.4 IES management procedures

Use the following procedures to perform IES creation and management tasks.

Procedure 70-1 To create an IES using configuration forms

1 Choose Create→Service→IES from the 5620 SAM main menu. The IES Service (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the IES. The Select Customer - IES form opens.

3 Select a customer for the IES and click on the OK button. The Select Customer - IES form closes, and the IES Service (Create) form reappears with the customer information displayed in the Customer panel.

4 Configure the parameters:

- Service ID
- Auto-Assign ID
- Service Name
- Description
- Service Tier
- Administrative State
- OLC State

Note — The OLC State parameter is configurable after you click on the Apply button.

5 Perform one of the following:

a Create a site for the IES. Go to step 6.

b Complete service creation if sites and access interfaces for the IES are to be created later. Go to step 62.

6 Click on the Components tab button.

7 Select and then right-click on IES Service and choose Create IES Site. The Select Network Elements - IES Service form opens with a list of available sites.

8 Select a site and click on the OK button. The IES Site (Create) form opens with general information about the site displayed in the Network Element panel.

9 Configure the parameters:

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State

10 Click on the IGMP Host Tracking tab button.

11 Configure the parameters:

- Administrative State
- Expiry Time

12 Perform one of the following steps.

a Create an access interface for the site. Go to step 13.

b Complete site creation if access interfaces for the site are to be created later. Go to step 52.

13 Click on the Components tab button.

14 Select and then right-click on Access Interfaces and choose Create IES L3 Access Interface. The IES L3 Access Interface (Create) form opens with the General tab displayed.

15 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- MAC Address
- Allow Directed Broadcasts
- Loopback Enabled
- Cflowd Type
- Class
- Trusted
- IPv6 Allowed
- Admin Link Local Address
- Admin Link Local Address Preferred
- Calling Station ID
- Configured IP MTU (Octets)
- Unnumbered Type
- IP Address
- Interface Name

Note 1 — The Unnumbered Type parameter is configurable when the Class parameter is set to Unnumbered.

Note 2 — The IP Address parameter is configurable when the Unnumbered Type parameter is set to IP Address.

Note 3 — The Interface Name parameter is configurable when the Unnumbered Type parameter is set to Name.

Note 4 — The Admin Link Local Address and Admin Link Local Address Preferred parameters are only configurable when the IPv6 Allowed parameter is enabled.

16 If the Loopback Enabled parameter in step 15 is enabled, you cannot associate a port with the L3 interface. Go to step 38.

17 Click on the Select button beside the Application Profile parameter. The Application Profile String: - IES L3 Access Interface list form opens.

18 Select a profile from the list and click on the OK button. The Application Profile String: - IES L3 Access Interface list form closes and the L3 Access Interface (Create) form is refreshed with the Application Profile information.

Note — The Application Profile String: - IES L3 Access Interface list form only displays local profiles that already exist on the node.

19 Click on the Port tab button.

20 Click on the Select button to choose a port for the L3 access interface. The Select Terminating Port - IES L3 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

21 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form displays the port information.

22 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

If the port uses Dot1 Q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. The system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

23 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

Note — If a bundle was selected in step 21, only the Scheduling Class parameter are configurable.

24 Bind an IES L3 access interface to a VPLS site, if required.

Note 1 — The operational state of the IP interface binding will not be turned up until the parameter Enable IP Interface Binding is set to true.

Note 2 — You can create and manage a routed VPLS connector from the Components tab on the Composite Service (Edit) form.

i Click on the Routed VPLS tab button.

ii Enter a VPLS site name or click on the Select button next to the VPLS Name parameter to choose a VPLS site with a configured site name. The Routed VPLS String - IES L3 Access Interface form opens.

iii Select a VPLS site and click on the OK button. The VPLS site is displayed.

iv In the Ingress - IPv4 Filter panel, click on the Select button. The Select IPv4 Filter - IES L3 Access Interface form opens.

v Select an IPv4 filter and click on the OK button. The IPv4 filter information is displayed.

vi In the Ingress - IPv6 Filter panel, click on the Select button. The Select IPv6 Filter - IES L3 Access Interface form opens.

vii Select an IPv6 filter and click on the OK button. The IPv6 filter information is displayed.

viii In the Egress - QoS Policy panel, click on the Select button. The Select QoS Policy - IES L3 Access Interface form opens.

ix Select a QoS Policy and click on the the OK button. The QoS Policy information is displayed.

25 Some devices support the application of QoS and accounting policies, queue schedulers, ANCP policies, ACL filters to interfaces and associating a local DHCP server.

a If your device supports these functions, go to step 26.

b If your device does not support these functions, the QoS, Schedulers, ACL, ANCP policies, Local DHCP server and Accounting tabs are not present. Go to step 38.

26 Assign ingress and egress QoS policies to the interface, if required.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service components tree, choosing Properties, and configuring the parameters on the appropriate tab.

i Click on the QoS tab button.

Note — The QoS tab is configurable only when a port is assigned to the interface.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use Shared Queue
- Use Multipoint Shared Queue
- HSMDA Packet Byte Offset (bytes)

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - IES L3 Access Interface form opens.

iv Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the ingress QoS policy information displayed.

Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port selected in step 21 uses the same access ingress queue group.

See Procedure 17-61 in chapter 17 for information about configuring Ethernet ports. See chapter 43 for information about queue group template policies.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - IES L3 Access Interface form opens.

vi Select an egress QoS policy and click on the OK button. The Select Egress Policy - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the egress QoS policy information displayed.

Note — If you select an egress policy that has a forwarding class mapped to an egress queue group, you must ensure that the port selected in step 21 uses the same access egress queue group.

See Procedure 17-61 in chapter 17 for information about configuring Ethernet ports. See chapter 43 for information about queue group template policies.

vii Click on the Select button in the HSMDA Egress Secondary Shaper panel to choose an HSMDA egress secondary shaper policy. The Select HSMDA Egress Secondary Shaper form opens.

viii Select a secondary shaper and click on the OK button. The Select HSMDA Egress Secondary Shaper form closes. The IES L3 Access Interface (Create) form refreshes with the egress secondary shaper information displayed.

ix Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

x Select a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the L3 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

xi Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

xii Select a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the L3 Access Interface (Create) form reappears with the egress policer control policy information displayed.

27 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 31.

Note — The Schedulers tab is configurable only when a port is assigned to the interface.

28 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame Base Accounting

Note 1 — The Egress Aggregate Rate Limit (kbps) and Frame Base Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — You cannot specify an egress scheduler when the Egress Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - IES L3 Access Interface form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - IES L3 Access Interface form opens.

vi Select an egress scheduler and click on the OK button. The Select Egress Scheduler - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the egress scheduler information displayed.

vii Go to step 31.

b Specify that an aggregation scheduler policy is applied to the interface.

i Set the Aggregation parameter to on.

ii Configure the Frame Base Accounting parameter.

iii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - IES L3 Access Interface form opens.

iv Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - IES L3 Access Interface form closes. The IES L3 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

v Go to step 31.

29 Click on the Aggregation Rate tab button to configure the aggregation rate, otherwise, go to step 31.

Note — The Aggregation Rate tab is configurable only if a port is assigned to the HSMDA SAP earlier in the procedure.

30 Configure the Aggregate Rate Limit (kbps) parameter in the Ingress Aggregate Rate Limit and Egress Aggregate Rate Limit panels.

31 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - IES L3 Access Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - IES L3 Access Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the egress ACL filter information displayed.

vi Click on the Select button in the IPv6 Ingress Filter panel to choose an ingress IPv6 ACL filter. The Select IPv6 Ingress Filter - IES L3 Access Interface form opens.

vii Select an ingress IPv6 ACL filter and click on the OK button. The Select IPv6 Ingress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the ingress IPv6 ACL filter information displayed.

viii Click on the Select button in the IPv6 Egress Filter panel to choose an IPv6 egress ACL filter. The Select IPv6 Egress Filter - IES L3 Access Interface form opens.

ix Select an IPv6 egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the IPv6 egress ACL filter information displayed.

32 Associate a local DHCP server to the IES L3 interface, if required.

i Click on the Local DHCP tab button

ii Click on the Select button in the Local DHCP Server panel to choose a local DHCP server. The Select Local DHCP Server - IES L3 Access Interface form opens.

iii Select a local DHCP server and click on the OK button. The Select Local DHCP Server - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the local DHCP server information displayed.

Note — You cannot associate a local DHCP server to the L3 group Interface if the Administrative State parameter in the Local Proxy Service panel is up. Go to step 45 to set the Administrative State.

33 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - IES L3 Access Interface form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - IES L3 Access Interface form closes, and the IES L3 Access Interface (Create) form reappears with the accounting policy information displayed.

34 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button.

ii Click on the Add button. The ANCP Static Map (Create) form opens.

iii Configure the ANCP String parameter.

iv Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. The ANCP Static Map form closes.

35 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab button.

ii Click on the Select button beside the Name parameter. The Select Time Of Day Suite - IES L3 Access Interface list form opens.

iii Select a time of day suite and click on the OK button. The Select Time Of Day Suite - IES L3 Access Interface list form closes, and the IES L3 Access Interface (Create) form refreshes with the time of day suite name.

Note 1 — You cannot assign a ToD suite to a L3 access interface if accounting statistics collection is enabled on the L3 access interface. You must first disable the Collect Accounting Statistics parameter in step 33.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics will only be collected if a Time Of Day Suite is applied on the SAP.

36 Configure residential subscriber management for the interface, if required.

i Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

ii Select the SHCV Enabled parameter to enable SHCV, if required. Otherwise, go to step 37.

iii Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source
- SHCV Action

iv Click on the Profiles tab button. If the Profiles tab is not enabled, go to step 37.

v Configure the parameters:

- Admin Status
- Service Model
- Subscriber Limit
- Default Subscriber Identification Type
- Default Subscriber Id
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id
- Profiled Traffic only
- Non-Subscriber Traffic Identification
- LAG link selection

37 Assign a DoS protection policy to the interface, if required.

Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - IES L3 Access Interface form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - IES L3 Access Interface form closes and the policy ID is displayed on the IES L3 Access Interface (Create) form.

38 Assign an IP address to the interface.

i Click on the Address tab button.

ii Click on the Add button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Broadcast Address Format
- EUI-64
- IP Address Preferred

Note 1 — The Broadcast Address Format parameter only appears if the IP Address parameter is set to an IPv4 address.

Note 2 — The EUI-64 and IP Address Preferred parameters only appear if the IP Address parameter is set to an IPv6 address.

Note 3 — The secondary IP addresses must not overlap with the primary IP address.

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The IES L3 Access Interface (Create) form reappears with the assigned IP addresses displayed.

39 Configure Bi-directional Forwarding Detection for the interface, if required.

i Click on the BFD tab button.

ii Click on the Configuration tab button.

iii Configure the parameters:

- Administrative Status
- Transmit Interval
- Receive interval
- Echo Interval
- Multiplier

iv To view local and remote session peers, click on the BFD Session tab button. 5620 SAM retrieves information from local and remote nodes and displays a list of BFD current sessions on router interfaces or L3 interfaces.

v Click on a session. A properties form opens for the session. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

vi Click on the OK button.

Note — You cannot enable BFD on an interface, if BFD is not configured on the interface. You cannot set the administration status of an interface to disabled, when protocols using the interface have BFD enabled. See chapter 28 for information about enabling and disabling BFD for routing protocols.

40 Configure IPv4 ICMP for the interface, if required.

i Click on the ICMP tab button.

ii Configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

41 If the IPv6 Allowed parameter in step 15 is enabled, the ICMPv6 tab is configurable. Configure IPv6 ICMP, if required. Otherwise, go to step 42.

Configure the parameters:

- Redirects
- Unreachables
- Packet Too Big
- Param Problem
- Time Exceeded
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of Packet Too Big
- Packet Too Big Time
- Number of Param Problem
- Param Problem Time
- Number of Time Exceeded
- Time Exceeded Time

42 Configure IPCP for the interface, if required. IPCP is available only on the ASAP MDA of 7750 SR, and 7710 SR.

i Click on the IPCP tab button.

ii Configure the parameters:

- Peer Address
- Primary DNS IP Address
- Secondary DNS IP Address

Note — Primary and secondary DNS addresses have similar functionality. However, they are assigned independently. When both are present, the primary DNS address is used to resolve address names. If the primary DNS address cannot be used the secondary DNS address is used.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button to confirm the action.

The IPCP tab is available when the SAP and port is configured with Null or IPCP encapsulation.

43 Configure ARP for the interface, if required.

i Click on the ARP tab button. The General tab is displayed.

ii Configure the Timeout (seconds) parameter.

iii To add a static ARP entry, click on the Add button. The Static ARP (Create) form opens.

iv Configure the parameters:

- IP Address
- Physical Address

v Click on the OK button. A dialog box appears.

vi Click on the OK button. The Static ARP (Create) form closes, and the General tab refreshes with the configured static hosts displayed in a list.

vii Repeat steps iii to vi to create additional entries, if required.

viii Click on the OK button. A dialog box appears.

ix Click on the Proxy ARP tab button.

x Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1
- Proxy ARP Policy 2
- Proxy ARP Policy 3
- Proxy ARP Policy 4
- Proxy ARP Policy 5

44 If the IPv6 Allowed parameter in step 15 is enabled, the Neighbor Discovery tab is configurable. Configure neighbor discovery, if required. Otherwise, go to step 45.

i Click on the Neighbor Discovery tab button.

ii Click on the Add button. The Neighbor Discovery (Create) form opens.

iii Configure the parameters:

- IP Address
- Physical Address

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Neighbor Discovery (Create) form closes, and the IES L3 Access Interface (Create) form refreshes with the neighbor entry.

vi If the Proxy ND tab is present, click on the Proxy ND tab button. Otherwise, go to step viii.

vii Configure the parameters:

- Enable Local Proxy
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Note — Do not leave an empty policy parameter between two configured policy parameters. For example, do not configure the Policy 1 and Policy 3 parameters and leave the Policy 2 parameter unconfigured, or the 5620 SAM reorders the policies and move the policy specified for the Policy 3 parameter to the Policy 2 parameter.

viii Repeat steps i to vii for each neighbor entry you want to create.

45 Configure IPv4 DHCP for the interface, if required.

i Click on the DHCP tab button. The General tab is displayed.

ii Configure the parameters:

- Enable DHCP Relay
- Description
- Trusted
- Lease Populate
- Enable
- Relay Plain BOOTP
- Use ARP

Note — The Lease Populate parameter is configurable when the Enable parameter is enabled.

iii Depending on the type and version of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step viii.

iv Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form opens.

v Configure the filter criteria.

vi Select a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form closes, and the L3 Access Interface (Create) form refreshes with the subscriber authentication policy name.

vii Configure the parameters:

- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP Address
- Use as source

Note — The Remote ID String parameter is configurable when the Remote ID parameter is set to Remote IDString.

viii Click on the Server tab button.

ix Configure the parameters:

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

Note — The following parameters are configurable when the Lease Time parameter is set to Specified Time Period.

- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

46 The ATM tab is configurable when the interface port is an ATM port. Specify OAM functionality and assign ingress and egress ATM policies to the interface, if required.

i Click on the ATM tab button.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- Periodic ATM OAM Loopback

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Select an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes, and the L3 Access Interface (Create) form refreshes with the ingress ATM policy information displayed.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Select an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes, and the L3 Access Interface (Create) form refreshes with the egress ATM policy information displayed.

47 Click on the VRRP tab button to create a VRRP instance on the current L3 interface for a virtual router. You must know the VRID for an existing virtual router and ensure that the interface is a member of the same subnet as the virtual router.

Note — The following configurations are required for the operation of the IPv6 VRRP instance:

- Two sub-tabs are available under the VRRP tab, one for IPv4 instances and the other for IPv6 instances. You can only create an IPv6 VRRP Instance if you enable the IPv6 Allowed parameter in step 15.
- The Link Local Address on the parent interface has to be set to preferred and configured as one of the backup addresses (or same subnet) for the IPv6 VRRP instance. To do this, the Admin Link Local Address and Admin Link Local Address Preferred parameters in step 15 must be set accordingly.
- The IPv6 address on the parent interface must be set to preferred to be used as a backup address (on same subnet) for the IPv6 VRRP instance. The IP Address and IP Address Preferred parameters in step 38 must be set accordingly.
- The Send Advertisement and Use Virtual MAC Address parameters must be enabled in step 49 for the router advertisement on the parent interface.

See chapter 36 for additional configuration information about VRRP instances and virtual routers.

i Click on the Add button. The VRRP Instance (Create) form opens with the General tab displayed.

ii Configure the Virtual Router Id parameter.

iii Perform steps 8 to 14 of Procedure 36-2.

Note — You can use the VR Instances tab to create, modify, and view VR instances.

iv Click on the OK button. The VRRP Instance (Create) form closes and the L3 Access Interface- Subscriber (Create) form reappears.

48 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the parameters:

- Anti-Spoofing
- ARP Populate

Note — The ARP Populate parameter is configurable when all of the IP addresses of the defined static hosts on the interface are in one of the subnets configured for the interface.

iii Click on the Static Hosts tab button to configure static subscriber host entries, if subscriber entries are not available through DHCP lease management. Otherwise, go to step 52.

iv Click on the Add button. The Access Interface Anti-Spoofing Static Host (Create) form opens.

v Configure the parameters:

- IP Address
- MAC Address

Note 1 — At least one IP address or MAC address must be specified for each static host. The values specified for the Anti-Spoofing and ARP Populate parameters determine the type of address entry that is required for the static host. For example, when you set the Anti-Spoofing parameter to Source Ip Addr, you must specify at least the IP address for the static host.

Note 2 — You can configure a static host on a SAP only when no static ARP entries exist on the IP interface.

Note 3 — When the ARP Populate parameter is enabled, the IP address of the new static host must be in one of the subnets that is configured for the interface in step 38.

vi Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step ix.

vii Click on the OK button.

viii Repeat steps v to vii to create additional entries, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes, and the Static Hosts tab refreshes with the configured static hosts displayed in a list.

49 Configure router advertisement, if required.

i Click on the Advertisement tab button.

ii Click on the Add button to add a router advertisement entry. The Router Advertisement (Create) form opens.

iii Configure the parameters:

- Send Advertisement
- Min Interval (seconds)
- Reachable Time (milliseconds)
- Managed Address Config
- MTU
- Use Virtual MAC Address
- Max Interval (seconds)
- Retransmit Time (milliseconds)
- Other Stateful Config
- Current Hop Limit
- Lifetime (seconds)

Note — If you are configuring the L3 interface for an IPv6 VRRP instance, then the Send Advertisement and Use Virtual MAC Address parameters must both be enabled.

iv Click on the Prefix tab button.

v Click on the Add button. The Router Advertisement Prefix (Create) form opens.

vi Configure the parameters:

- IPv6 Prefix
- On-Link Determination
- Prefix Length
- Autonomous Address Configuration
- Lifetime (seconds) in Preferred Lifetime panel
- No Expiry in Preferred Lifetime panel
- Lifetime (seconds) in Valid Lifetime panel
- No Expiry in Valid Lifetime panel

Note — Each Lifetime (seconds) parameter is configurable when the associated No Expiry parameter is disabled.

50 Click on the OK button. A dialog box appears.

51 Click on the OK button. The Router Advertisement Prefix (Create) form closes.

52 Click on the OK button. A dialog box appears.

53 Click on the OK button. The IES L3 Access Interface (Create) form refreshes with the router advertisement entry.

54 Specify queue overrides by clicking on the Override tab button. See Procedure 44-40 for information about how to set queue overrides.

Note 1 — The Override tab contains four sub-tabs: Access Ingress Queue, Access Egress Queue, Access Ingress HSMDA Queue, and Access Egress HSMDA Queue. However, only two of the four are active, depending on the port type you have chosen for this interface.

Note 2 — If you have configured an HSMDA port, then the Access Ingress HSMDA Queue and Access Egress HSMDA Queue sub-tabs are active. If you have configured a non-HSMDA port, then the Access Ingress Queue and Access Egress Queue sub-tabs are active.

55 If the IPv6 Allowed parameter in step 15 is enabled, the DHCPv6 tab is configurable. Configure IPv6 DHCP, if required. Otherwise, go to step 56.

i Click on the DHCPv6 tab button. The DHCPv6-Prefix tab is displayed.

ii Click on the Add button. The DhcpRelayV6PrefixDelegation (Create) form opens.

iii Configure the parameters:

- Prefix Address
- Prefix Length
- Prefix DUID
- Prefix IAID
- Prefix Life Time (seconds)
- Prefix Valid Life Time (seconds)

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The L3 Access Interface (Create) form reappears.

vi Click on the DHCPv6-Relay tab button.

vii Configure the parameters:

- Enable DHCPv6 Relay
- Description
- Lease Populate
- Maximum Number of Leases
- Interface Id Option
- Interface Id String
- Remote ID
- Source IP Address
- Neighbor Resolution
- Prefix Option

viii Click on the Server tab button.

ix Configure the Server 1 through Server 8 parameters.

x Configure the interface name for each DHCPv6 server that you configured in step ix by clicking on the Select button in the Zone Index panel. The Select Zone Index - DhcpRelayV6Configuration form opens with a list of configured interfaces.

xi Select an interface from the list and click on the OK button. The Select Zone Index - DhcpRelayV6Configuration list form closes and the L3 Access Interface form refreshes with the interface information.

xii Click on the OK button. A dialog box appears.

xiii Click on the OK button. The L3 Access Interface (Create) form reappears.

56 Configure Unicast RPF if required.

i Click on the Unicast RPF tab button.

ii Configure the parameters:

- URPF Check State
- URPF Check Mode

Note — The URPF Check State parameter must be enabled to display the URPF Check Mode parameter.

57 Click on the OK button. A dialog box appears.

58 Click on the OK button. The IES L3 Access Interface (Create) form closes, and the IES Site (Create) form displays the new access interface.

59 Add a Video interface to the IES site, if required. See Procedure 33-2 for more information.

60 Click on the OK button. The IES Site (Create) form closes, and the IES Service (Create) form reappears with the new site information displayed in the service components tree.

61 Perform one of the following steps.

a Create an additional site for the IES. Go to step 6.

b Complete service creation. Go to step 62.

62 Click on the OK button. A dialog box appears.

63 Click on the Yes button to confirm the action. The IES Service (Create) form closes.

Procedure 70-2 To apply OSPF, RIP, or IS-IS to an IES

Note — OSPF, RIP, or IS-IS must be enabled at the routing instance level before you can apply OSPF, RIP, or IS-IS to an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES in the list and click on the Properties button. The IES Site (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the Sites tab button.

5 Select a site in the list and click on the Properties button. The IES Site (Edit) form opens.

6 Click on the Protocols tab button.

7 Click on the Add button. The Create Interface form opens.

8 Specify the interface type by configuring the What type of interface would you like to create? parameter.

9 Click on the OK button. The Interface (Create) form opens. See section 28.2 for information about configuring specific routing protocols.

Procedure 70-3 To apply OSPF, RIP, or IS-IS to an IES L3 interface

Note — OSPF, RIP, or IS-IS must be enabled at the routing instance level before you can apply OSPF, RIP, or IS-IS to an L3 interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria.A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the L3 Access Interfaces tab button.

5 Select an L3 interface in the list and click on the Properties button. The L3 Access Interface (Edit) form opens.

6 Click on the Protocols tab button.

7 Click on the Add button. The Create Interface form opens.

8 Specify the interface type by configuring the What type of interface would you like to create? parameter.

9 Click on the OK button. The Interface (Create) form opens. See section 28.2 for information about configuring specific routing protocols.

Procedure 70-4 To add an IGMP interface to an IES

Note — IGMP must be enabled on the NE routing instance before you can create an IGMP interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the Sites tab button.

5 Select a site in the list and click on the Properties button. The IES Site (Edit) form opens.

6 Click on the Multicast tab button.

7 Click on the Interfaces tab button.

8 Click on the Add button. The Create Interface form opens.

9 Set the What type of interface would you like to create? parameter to IGMP.

10 Click on the OK button. The IGMP Interface (Create) form opens with the General tab displayed.

11 Click on the Select button to specify an interface. The Select Interface form opens.

12 Click the Search button. A list of interfaces appears at the bottom of the Select Interface form.

13 Select an interface and click the OK button. The Select Interface form closes and the Interface panel refreshes with the interface parameters.

14 Configure the parameters:

- Description
- Administrative State
- Administrative Version
- Maximum Number of Groups
- Subnet Check

15 Click on the Behavior tab button.

16 Configure the Import Policy parameter.

17 Click on the Multicast CAC tab button to add a multicast CAC policy, if required. The General tab is displayed.

18 Click on the Select button in the Select Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - IGMP Interface form opens.

19 Choose a multicast CAC policy from the list and click on the OK button. The Select Multicast CAC Policy - IGMP Interface form closes and the IGMP Interface, Routing Instance (Create) form appears.

20 Configure the parameters:

- Unconstrained Bandwidth
- Mandatory Bandwidth
- Constraint Admin State

21 Click on the Static Group/Source tab button to add a static multicast group or source, if required.

22 Click on the Add button to add a new entry. The StaticGrpSrc, Interface ID - 6, Routing Instance (Create) form opens.

23 Configure the parameters:

- Static Multicast Group
- Static Source

24 Click on the OK button. The StaticGrpSrc, Routing Instance (Create) form closes and a dialog box appears.

25 Click on the OK button to confirm the action. The IGMP Interface, Routing Instance (Create) form reappears.

26 Click on the OK button to close the IGMP Interface, Routing Instance (Create) form.

27 Click on the OK button to close the IGMP Interface (Create) form.

28 Click on the Group Interfaces tab button to identify an IGMP group interface for the IES service, if required.

29 Click on the Add button and configure the parameters in the IGMP Group Interface - Routing Instance (Create) form:

- Description
- Administrative State
- Name

30 Click on the Select button next to the Interface ID field to select a group interface from the Select IGMP Group Interface - IGMP Group Interface - Routing Instance form.

31 Click on the OK button to close the Site (Edit) form.

32 Click on the OK button to close the IES (Edit) form. A dialog box appears.

33 Click on the Yes button to confirm the action. The IES (Edit) form closes.

34 Close the Manage Services form.

Procedure 70-5 To add a PIM interface to an IES

Note — Before you can add a PIM interface to an IES, PIM must be applied to All or IES during the PIM configuration at the routing instance level. See Procedure 28-32 for more information.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES in the list and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the Sites tab button.

5 Select a site in the list and click on the Properties button. The IES Site (Edit) form opens.

6 Click on the Multicast tab button.

7 Click on the Add button. The Create Interface form opens.

8 Set the What type of interface would you like to create? parameter to PIM.

9 Click on the OK button. The PIM Interface (Create) form opens with the General tab displayed.

10 Click on the Select button to specify an interface. The Select Interface - PIM Interface form opens.

11 Configure the filter criteria. A list of available L3 access interfaces appears at the bottom of the Select Interface - PIM Interface form.

12 Select an interface and click on the OK button. The Select Interface - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the L3 access interface information.

13 Configure the parameters:

- Description
- Administrative State
- Administrative State IPv4
- BFD Enabled

14 Click on the Behavior tab button.

15 Configure the parameters:

- Hello Interval (seconds)
- Tracking Support
- BSM Check Router Alert
- Improved assert
- Max Groups
- Three Way Hello
- Multicast Senders
- Hello Multiplier
- Assert Period
- DR Priority
- Sticky DR
- Operational DR Priority

Note — The Operational DR Priority parameter is configurable when the Sticky DR parameter is enabled.

16 Click on the Neighbor tab button, if present, to view and edit information. The Neighbor tab is present only when a neighbor PIM interface exists.

17 Click on the Multicast CAC tab button to add a multicast CAC policy, if required. The General tab is displayed.

18 Click on the Select button in the Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - PIM Interface form opens.

19 Choose a multicast CAC policy from the list and click on the OK button. The Select Multicast CAC Policy - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form reappears.

20 Configure the parameters:

- Unconstrained Bandwidth
- Mandatory Bandwidth
- Constraint Admin State

21 Click on the IPv6 Specifics tab button.

22 Configure the Administrative State IPv6 parameter.

23 Click on the OK button to close the PIM Interface (Create) form.

24 Click on the OK button to close the IES Site (Edit) form.

25 Click on the OK button to close the IES Service (Edit) form. A dialog box appears.

26 Click on the Yes button to confirm the action. The IES Service (Edit) form closes.

27 Close the Manage Services form.

Procedure 70-6 To create an L2 SDP spoke termination on an IES service

Ensure that a service and site have been created in the IES. To terminate an L2 service on an IES SDP spoke, you must identify the VC and an interface belonging to the VC. The interface must not have an associated port.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the Components tab button.

5 Right-click on Spoke Sdp Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

6 Specify a source interface for the spoke SDP binding.

   i Click on the Select button in the Source Interface panel. The Select Source Interface - Spoke SDP Binding form opens.

   ii Configure the filter criteria. A list of source interfaces appears at the bottom of the Select Source Interface - Spoke SDP Binding form.

   iii Choose a source interface from the list and click on the OK button. The Select Source Interface - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

7 Specify a destination node for the spoke SDP binding:

   a If the destination node is a managed node, choose from a list of managed nodes.

      i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element form opens.

      ii Select a destination node and click on the OK button. The Select Destination Network Element form closes, and the Spoke SDP Binding (Create) form refreshes with the tunnel termination site (the destination node) identifier displayed.

   b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

8 Configure the parameters:

- VC ID
- VC Type
- Auto-Assign ID
- Ingress Label
- Egress Label
- Enable Hash Label

9 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto Select Transport Tunnel parameter.

ii Configure the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

10 Specify an application profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding - IES service form displays only local profiles on the NE.

11 Click on the States tab button.

12 Configure the Administrative State parameter.

13 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes, and the L3 Access Interface (Create) form reappears with the egress ACL filter information displayed.

14 Assign an accounting policy to the spoke SDP binding, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes, and the L3 Access Interface (Create) form reappears with the accounting policy information displayed.

15 Associate a MEP with an SDP binding, if required.

i Click on the MEPs tab button.

ii Click on the Add button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

vi If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step 16.

vii Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

viii Click on the AIS tab button.

ix Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

16 Click on the OK button. The MEP (Create) form closes.

17 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

18 Click on the OK button. The IES Service (Edit) form reappears with the new information displayed in the service components tree.

Procedure 70-7 To add a subscriber interface to an IES

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a subscriber interface in an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Search button. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service Subscriber (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on the Subscriber Interfaces icon below the site to which you want to add the subscriber interface, and choose Create IES Subscriber Interface. The IES Subscriber Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Auto-Assign ID
- Interface ID
- Name
- Description
- Administrative State
- Default Primary DNS Server Address
- Default Secondary DNS Server Address

Note 1 — The Name value for a subscriber interface must be unique in the NE.

Note 2 — You must configure the Default Primary DNS Server Address parameter before you can configure the Default Secondary DNS Server Address parameter.

7 Configure IPv6 forwarding on the subscriber interface, if required.

i Configure the IPv6 Allowed and IPv6 Delegated Prefix Length parameters.

ii Click on the IPv6 Subscriber Prefixes tab button.

iii Select a subscriber prefix from the list and click on the Properties button, or click on the Add button to create a new subscriber prefix.

iv In the Subscriber Prefix [Edit|Create] form, configure the parameters:

- Address ID
- IP Address
- Prefix Length
- WAN Host
- Prefix Delegation

8 Create IP addresses for the subscriber interface that are inherited by the SAPs in the group interfaces that are child objects of the subscriber interface.

i Click on the Address tab button.

ii Click on the Add button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Populate Host Routes
- Gateway IP Address
- Broadcast Address Format

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The IES Subscriber Interface (Create) form reappears with the assigned IP addresses displayed.

vi Repeat steps ii to v for each additional IP address that you want to create.

9 Click on the DHCP tab button.

10 Configure the parameters:

- IP address
- Use as source

11 Click on the OK button. The IES Subscriber Interface (Create) form closes, and a dialog box appears.

12 Click on the OK button. The IES Service (Edit) form reappears with the new subscriber interface displayed in the service components tree.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button. The IES Service (Edit) form closes, and the Manage Services form reappears.

15 Close the Manage Services form.

Procedure 70-8 To add a group interface to an IES

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a group interface in an IES.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on the subscriber interface to which you want to add a group interface, and choose Create IES Subscriber Interface. The IES Subscriber Interface (Create) form opens with the General tab displayed.

6 Click on the Group Interface tab button.

7 Click on the Add button. The IES Group Interface (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Auto-Assign ID
- Interface ID
- Name
- Description
- Administrative State
- MAC Address
- Trusted
- Operational State UP While Empty
- LNS

Note — The LNS parameter defines the type of group interface. This parameter is set at creation time and cannot be modified. Regular group interfaces cannot configure LNS attributes, and an LNS group interface does not allow PPPoE configuration or SAPs.

9 Configure IPv6 router advertisement and DHCPv6 on the group interface, if required.

i Configure the IPv6 Allowed parameter.

ii Click on the IPv6 Advertisement tab button and configure the parameters:

- Administrative State
- Current Hop Limit
- Managed Address Config
- Max Interval (seconds)
- Min Interval (seconds)
- Link MTU
- Other Stateful Config
- Reachable Time (milliseconds)
- Retransmit Time (milliseconds)
- Router Lifetime (seconds)
- Autonomous Address Configuration
- Preferred Lifetime
- Valid Lifetime

iii Click on the DHCPv6 tab button.

iv Click on the Select button and select a local user database from the Select Local User Database form.

v Click on the Proxy Server tab button and configure the parameters:

- Administrative State
- Renew Timer
- Rebind Timer
- Valid Lifetime
- Preferred Lifetime
- Client Applications

10 Click on the Anti-Spoofing tab button.

11 Configure the ARP Populate parameter.

12 Click on the Subscriber Management tab button.

13 Configure the parameters:

- SHCV Enabled
- SHCV Interval (minutes)
- SHCV Source
- SHCV Action

Note — The SHCV Interval (minutes), SHCV Source, and SHCV Action parameters are configurable only when the SHCV Enabled parameter is set to enabled.

14 Configure ICMP for the group interface, if required.

i Click on the ICMP tab button.

ii Configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

15 Configure ARP for the group interface, if required.

i Click on the ARP tab button. The General tab is displayed.

ii Configure the Timeout (seconds) parameter.

iii Click on the Proxy ARP tab button.

iv Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1 through Proxy ARP Policy 5

16 Configure DHCP relay for the group interface, if required.

i Click on the DHCP tab button. The General tab is displayed.

ii Configure the parameters:

- Enable DHCP Relay
- Description
- Match Circuit ID
- Trusted
- Lease Populate
- L2 Header
- Anti-Spoof Mac Address

iii Depending on the type and version of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Select Subscriber Authentication Policy, if required. Otherwise, go to step xiii.

iv Click on the Select button in the Subscriber Authentication Policy panel. The Select Subscriber Authentication Policy - GrpItfDhcpRelayCfg form opens.

v Configure the filter criteria.

vi Click the Search button. A list of subscribers is listed.

vii Select a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - GrpItfDchpRelayCfg form closes, and the IES Group Interface (Create) form refreshes with the subscriber authentication policy name.

viii Configure the parameters:

- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP Address
- Use as source

Note — The Remote ID String parameter is configurable when the Remote ID is set to Remote IDString.

ix Click on the Select button in the Local User Database panel to choose a local user database. The Select localUserDbPointer - GrpItfDhcpRelayCfg form opens.

x Configure the filter criteria.

xi Click the Search button. A list of available databases appears.

xii Select a database and click on the OK button. The Select localUserDbPointer - GrpItfDhcpRelayCfg form closes, and the IES Group Interface (Create) form reappears with the database name information displayed.

xiii Click on the Server tab button.

xiv Configure the parameters:

- Server 1 to Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

Note — The following parameters are configurable when the Lease Time parameter is set to Specified Time Period.

- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

17 Click on the Client Applications tab button. Configure the Client Applications parameter.

18 Click on the PPPoE tab button to configure PPPoE for the group interface.

19 Configure the parameters:

- Description
- Administrative State

20 Click on the Select button in the PPPoE Policy panel. A Select PPPoE Policy form opens with a list of available PPPoE policies.

21 Choose a policy from the list.

22 Click on the OK button. The Select PPPoE Policy form closes and the IES Group Interface (Create) form refreshes with new PPPoE policy values.

23 Click on the Select button in the Local User DB panel. A Select Local User DB form opens with a list of available local user databases.

24 Choose a local user database from the list.

25 Click on the OK button. The Select Local User DB form closes and the IES Group Interface (Create) form refreshes with new Local User DB values.

26 Configure the parameters:

- Session Limit
- Session Limit per SAP

27 Configure the ARP host for the group interface, if required.

i Click on the ARP Host Configuration tab button.

ii Configure the parameters:

- Administrative State
- ARP Host Limit
- Minimum Authentication Interval
- SAP ARP Host Limit

28 If you set the parameter LNS to TRUE in step 8, perform the following steps to configure LNS for the group interface.

Note — After you create an LNS group interface, you must configure the L2TP tunnel group profile or L2TP tunnel profile to terminate sessions for the LNS group interface; see Procedure 28-29 for more information. You can also configure the termination of sessions on a group interface using a RADIUS server.

i Click on the LNS tab button.

ii Configure the Description parameter.

iii Click on the Select button in the Default Subscriber Profile panel. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form opens.

iv Select a subscriber profile from the list and click on the OK button. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the Subscriber Profile displayed.

v Click on the Select button in the Default SLA Profile panel. The Select Default SLA Profile (Terminate LNS PPP Sessions) form opens.

vi Select an SLA profile from the list and click on the OK button. The Select Default SLA Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the SLA Profile displayed.

vii Click on the Select button in the Subscriber Identification Policy panel. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form opens.

viii Select a subscriber identification policy from the list and click on the OK button. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the subscriber identification policy displayed.

ix Click on the Select button in the Default Application Profile panel. The Select Default Application Profile (Terminate LNS PPP Sessions) form opens.

x Select a default application profile from the list and click on the OK button. The Select Default Application Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the default application profile displayed.

29 Configure the Default Subscriber Identification String parameter.

30 Click on the Service Access Points tab button to configure SAPs for the group interface.

31 Click on the Add button. The IES Service Access Point (Create) form opens with the General tab displayed.

32 Configure the parameters:

- Name
- Description
- Administrative State
- Calling Station ID

33 Click on the Port tab button.

34 Click on the Select button to choose a port for the SAP. The Select Terminating Port - IES Service Access Point form opens.

Caution — The creation of a SAP that uses the same port and encapsulation values as an existing inactive MSAP fails under the following conditions:

- If you try to use the 5620 SAM to create a SAP, the configuration fails and the 5620 SAM displays an error message.
- If you use a CLI to create a SAP in a service other than the service that contains the MSAP, the configuration succeeds but the MSAP is inactivate until the regular SAP is deleted. Although the 5620 SAM displays the SAP and MSAP, the MSAP remains inactive and consumes resources.
- If you use a CLI to create a SAP in the service that contains the MSAP, the SAP creation fails.

Alcatel-Lucent recommends that you delete an inactive MSAP from the 5620 SAM if you need to create a regular SAP on the same port using the same encapsulation values. See Procedure 64-14 for more information about deleting MSAPs.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

35 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - IES Service Access Point form closes, and the IES Service Access Point (Create) form displays the port information.

36 Configure the parameters:

- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

If the port uses Dot1 Q encapsulation, you can enable the Auto-Assign ID parameter to have the Outer Encapsulation Value parameter automatically assigned. The system assigns the lowest unused encapsulation value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

37 Assign ingress and egress QoS policies to the SAP, if required.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once. Choose and right-click the components in the service components tree, choose Properties, and configure the parameters on the appropriate tab.

i Click on the QoS tab button.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use Shared Queue

iii Click on the Select button in the Ingress Policy panel. The Select Ingress Policy - IES Service Access Point form opens.

iv Configure the filter criteria and click on the Search button. A list of available ingress policies appear.

v Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - IES Service Access Point form closes, and the IES L3 Service Access Point (Create) form reappears with the ingress QoS policy information displayed.

Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you selected in step 35 has the access ingress queue group with the same name created on it.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

vi Click on the Select button in the Egress Policy panel. The Select Egress Policy - IES L3 Service Access Interface form opens.

vii Configure the filter criteria and click on the Search button. A list of available egress policies is displayed.

viii Select an egress QoS policy and click on the OK button. The Select Egress Policy - IES Service Access Point form closes, and the IES Service Access Point (Create) form reappears with the egress QoS policy information displayed.

Note — If you select an egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you selected in step 35 has the access egress queue group with the same name created on it.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

ix Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

x Select a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the IES Service Access Point (Create) form reappears with the ingress policer control policy information displayed.

xi Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

xii Select a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the IES Service Access Point (Create) form reappears with the egress policer control policy information displayed.

38 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 40.

Note — The Schedulers tab is displayed only if a port is assigned to the SAP earlier in the procedure.

39 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the SAP.

i Set the Aggregation parameter to off.

ii Configure the parameters:

- Egress Aggregate Rate Limit (kbps)
- Frame Base Accounting

Note 1 — The Egress Aggregate Rate Limit (kbps) and Frame Base Accounting parameters are displayed only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — You cannot specify an egress scheduler when the Egress Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - IES Service Access Point form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - IES Service Access Point form closes, and the IES Service Access Point (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Select Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - IES Service Access Point form opens.

vi Select an egress scheduler and click on the OK button. The Select Egress Scheduler - IES Service Access Point form closes, and the IES Service Access Point (Create) form refreshes with the egress scheduler information displayed.

vii Go to step 40.

b Specify that an aggregation scheduler policy is applied to the SAP.

i Set the Aggregation parameter to on.

ii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - IES Service Access Point form opens.

iii Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - IES Service Access Point form closes, and the IES Service Access Point (Create) form refreshes with the aggregation scheduler information displayed.

40 Assign ingress and egress ACL filters to the SAP, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter from the Select Ingress Filter - IES Service Access Point form.

iii Click on the Select button in the Egress Filter panel to choose an egress ACL filter from the Select Egress Filter - IES Service Access Point form.

41 Click on the Accounting tab button to assign an accounting policy to the SAP.

i Click on the Select button to choose an accounting policy. The Select Accounting Policy - IES Service Access Point form opens.

ii Select an accounting policy and click on the OK button. The Select Accounting Policy - IES Service Access Point form closes, and the IES Service Access Point (Create) form reappears with the accounting policy information displayed.

iii Configure the Collect Accounting Statistics parameter.

42 Click on the Anti-Spoofing tab button to configure anti-spoofing for the SAP. The Anti-Spoofing tab opens with the General tab displayed.

i Configure the Anti-Spoofing parameter.

ii Click on the Static Hosts tab button to configure a static subscriber host entry for each subscriber host that is not managed by DHCP.

iii Click on the Add button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

iv Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification
- Use SAP ID as Subscriber ID
- ANCP String
- Intermediate Destination ID

v Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with the list of available subscriber profiles displayed.

vi Select a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

vii Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host. The Select SLA Profile - AntiSpoofingStaticHosts form opens with the list of available SLA profiles displayed.

viii Select an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

ix Click on the Select button in the Application Profile panel to choose an application profile for the static host. The Select Application Profile - AntiSpoofingStaticHosts form opens with the list of application profiles on the NE displayed.

x Select an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes.

43 Assign a DoS protection policy to the SAP, if required.

Note — A default DoS protection policy is automatically assigned to the SAP.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - IES Service Access Point form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - IES Service Access Point form closes and the Policy ID is displayed on the IES Service Access Point (Create) form.

iv Configure the MAC Monitoring parameter.

44 Associate a MEP to a SAP, if required.

i Click on the MEPs tab button.

ii Click on the Add button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

45 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step 49.

46 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

47 Click on the AIS tab button.

48 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

49 Click on the OK button. The MEP (Create) form displays the SAP information.

50 Click on the OK button. The MEP (Create) form closes.

51 Click on the Subscriber Management tab button to configure residential subscriber management on the SAP. The IGMP Host Tracking tab is displayed.

i Click on the Select button to choose the import policy used to filter IGMP packets. The Select SapIgmpHostTracking form opens.

ii Configure the filter parameters and click on the Search button. A list of import policies appears.

iii Choose a policy and click on the OK button. The selected import policy name appears.

iv Configure the parameters:

- Expiry Time
- Max Number of Groups
- Max Number of Sources per Group

v You can click on the Host Tracking Info tab button to view a list of hosts that are being tracked on this service access point.

vi Click on the Profiles tab button.

vii Configure the parameters:

- Admin Status
- Service Model
- Subscriber Limit
- Default Subscriber Identification Type
- Default Subscriber Id
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id
- Profiled Traffic only
- Non-Subscriber Traffic Identification

viii Click on the Select button in the Default Subscriber Profile panel to choose a default subscriber profile for the SAP, if required. The Select Default Subscriber Profile form opens with the list of available subscriber profiles displayed.

ix Select a subscriber profile and click on the OK button. The Select Default Subscriber Profile form closes, and the subscriber profile name appears in the Default Subscriber Profile panel.

x Click on the Select button in the Default SLA Profile panel to choose a Default SLA profile for the SAP, if required. The Select Default SLA Profile form opens with the list of available SLA profiles displayed.

xi Select an SLA profile and click on the OK button. The Select Default SLA Profile form closes, and the SLA profile name appears in the Default SLA Profile panel.

xii Click on the Select button in the Subscriber Identification Policy panel to choose a subscriber identification policy for the SAP, if required. The Select Subscriber Identification Policy form opens with the list of available subscriber identification policies displayed.

xiii Select a subscriber identification policy and click on the OK button. The Select Subscriber Identification Policy form closes, and the subscriber identification policy name appears in the Subscriber Identification Policy panel.

xiv Click on the Select button in the Default Application Profile panel to choose a default application profile for the SAP, if required. The Select Default Application Profile form opens with the list of application profiles on the NE displayed.

xv Select an application profile and click on the OK button. The Select Default Application Profile form closes, and the application profile name appears in the Default Application Profile panel.

xvi Click on the Select button in the Non-Subscriber Traffic Subscriber Profile panel to choose a non-subscriber subscriber profile for the SAP, if required. The Select Non-Subscriber Traffic Subscriber Profile form opens with the list of available subscriber profiles displayed.

xvii Select a subscriber profile and click on the OK button. The Select Non-Subscriber Traffic Subscriber Profile form closes, and the subscriber profile name appears in the Non-Subscriber Traffic Subscriber Profile panel.

xviii Click on the Select button in the Non-Subscriber Traffic SLA Profile panel to choose a Non-Subscriber Traffic SLA profile for the SAP, if required. The Select Non-Subscriber Traffic SLA Profile form opens with the list of available SLA profiles displayed.

xix Select an SLA profile and click on the OK button. The Select Non-Subscriber Traffic SLA Profile form closes, and the SLA profile name appears in the Non-Subscriber Traffic SLA Profile panel.

xx Click on the Select button in the Non-Subscriber Traffic Application Profile panel to choose a non-subscriber traffic application profile for the SAP, if required. The Select Non-Subscriber Traffic Application Profile form opens with the list of application profiles on the NE displayed.

xxi Select an application profile and click on the OK button. The Select Non-Subscriber Traffic Application Profile form closes, and the application profile name appears in the Non-Subscriber Traffic Application Profile panel.

52 Assign an ANCP policy to the interface, if required.

- **i** Click on the ANCP Static Map tab button.
- **ii** Click on the Add button. The ANCP Static Map (Create) form opens.
- **iii** Configure the ANCP String parameter.
- **iv** Click on the Select button to choose an ANCP Policy. The Select ANCP Policy - ANCP Static Map form opens.
- **v** Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.
- **vi** Click on the OK button. The ANCP Static Map form closes.

53 Modify PPPoE Sessions that have been generated by the NE, for the group interface, if required. See chapter 64 for more information about viewing and configuring a PPPoE session.

54 Click on the OK button. The IES Service Access Point (Create) form closes, and a dialog box appears.

55 Click on the OK button. The IES Group Interface (Create) form refreshes to display the SAP.

56 To configure additional SAPs in the group interface, go to step 31.

57 Click on the OK button. The IES Group Interface (Create) form closes, and a dialog box appears.

58 Click on the OK button. The IES Service (Edit) form refreshes to display the SAP below the group interface.

59 Click on the OK button. A dialog box appears.

60 Click on the Yes button. The IES Service (Edit) form closes.

61 Close the Manage Services form.

Procedure 70-9 To implement dual homing using SRRP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES service and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the Components tab button.

5 Specify the pair of sites that are to participate in dual homing.

Note — The sites can be from different services.

6 Ensure that the pair of sites each contains a properly configured subscriber interface and SAPs underneath the group interface that will be participating in the redundant configuration.

7 Ensure that all subscriber interface IP addresses have a gateway address configured on them.

8 Create the Redundant Interface (used for SRRP out-of-band messaging) between the two routers.

i Right-click on the Redundant Interfaces item for one site of the redundant pair, and choose Create Redundant Interface. The Redundant Interface (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State

iii Click on the Address tab button.

iv Click on the Add button. The IP Address (Create) form opens.

v Specify IP addresses for the redundant interface on the current and remote sites. Configure the parameters:

- Address ID
- IP Address (in the form d.d.d.d, where d is a value from 0 to 255)
- Prefix Length
- Remote IP Address

  This must be on the same subnet as the current site's redundant interface IP Address. For example, if the current site's IP Address is 7.7.7.7, with a Prefix Length of 24, then the remote site's redundant interface address must be 7.7.7.d, where d is a value from 0 to 255, excluding 7.
- Broadcast Address Format

vi Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

vii Click on the OK button. The Redundant Interface (Create) form reappears with the assigned redundant interface IP addresses displayed.

viii Click on the OK button. A dialog box appears.

ix Click on the OK button. The Redundant Interface (Create) form for the current site closes.

9 Create an SDP spoke binding between the current and remote sites. The Source Interface is the Redundant Interface you created in step 8 and the Tunnel Termination SIte is the remote site. The Return Tunnel must come from the remote site.

10 Assign the Redundant Interface to the Group Interface for the current site.

i Right-click on the group interface you want to use (under the Subscriber Interface in the Component view) and choose Properties. The IES Group Interface (Edit) form opens with the General tab displayed.

ii Click on the Select button in the Redundant Interface panel. The Select Redundant Interface - IES Group Interface form opens.

iii Configure the list filter parameters if required and click on the Search button. A list of redundant interfaces on the site appears at the bottom of the form.

iv Select the Redundant Interface you created in step 8 and click on the OK button. The Select Redundant Interface - IES Group Interface form closes and the interface you selected appears in the Redundant Interface field.

v Click on the OK button. The IES Group Interface (Edit) form closes.

11 Create an SRRP Instance for the current site.

i Right-click on the SRRP Instances item (under the group interfaces in the Component view) for the current site, and choose Create SRRP Instance. The SRRP Instance (Create) form opens with the General tab displayed.

ii Configure the parameters:

- SRRP ID
  The SRRP ID must be the same value for both the current and remote sites.
- Description
- Administrative State

iii Click on the Behavior tab button.

iv Configure the parameters:

- Gateway MAC address.
- Keep Alive Interval
- Priority

v Configure the message path by clicking the Select button in the Message Path panel. The Select Message Path Pointer - SRRP Instance form opens, displaying the SAPs available on the site.

vi Select the SAP you want to use for the in-band messaging between the sites.

vii Click on the OK button. The Select Message Path Pointer - SRRP Instance form closes.

viii Configure policy pointer 1, if required, by clicking the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 1 - SRRP Instance form opens, displaying the pointers available on the site.

ix Select the pointer you want to use.

x Click on the OK button. The Select Policy Pointer 1 - SRRP Instance form closes.

xi Configure policy pointer 2, if required, by clicking the Select button in the Policy Pointer 2 panel. The Select Policy Pointer 2 - SRRP Instance form opens, displaying the pointers available on the site.

xii Select the pointer you want to use.

xiii Click on the OK button. The Select Policy Pointer 2 - SRRP Instance form closes.

xiv Click on the OK button. The SRRP Instance (Create) form closes, and a dialog box appears.

xv Click on the OK button. The IES (Edit) form reappears with the SRRP Instance displayed.

12 Click on the Turn Up button to activate the SRRP instance.

13 Repeat steps 8 to 12 for the remote site.

Note 1 — When you repeat steps 8 to 12 for the remote site, that site becomes the current site and the previously configured site is the remote site.

Note 2 — After the two sites have been properly set up, you can examine the SRRP peer associations at any time by right-clicking an SRRP Instance in the service's Component view. This opens the SRRP Instance - Edit form, which contains a read-only field called SRRP Peer. The Site ID, Service ID, and Operational State of the associated peer appear in this field.

You can also examine the state of an SRRP Instance by checking the Operational Flags field. The flags indicate specific problems that might occur with the SRRP Instance, as follows:

- Duplicate Subscriber IF Address: one of the local subscriber IP addresses is the same as a subscriber IP address on the remote node.
- Redundant Interface Mismatch: the local SRRP instance and remote SRRP instance have mismatched redundant interfaces.
- SAP Mismatch: the local SRRP instance is backing a different set of SAPs than the peer.
- Subnet Mismatch: one of the subnets that SRRP is backing up does not have a match with the peer.
- Dual Master: both SRRP instances are master at the same time.
- SAP Tag Mismatch: the local SRRP instance is backing a set of SAPs with different remote and local tags.
- SRRP ID Mismatch: the peer has a different SRRP instance ID backing the same subnet.

14 Click on the OK button. A dialog box appears.

15 Click on the OK button. The IES (Edit) form closes.

Procedure 70-10 To modify an IES

Caution — Modifying parameters can be service-affecting.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Properties button. The IES Service (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs list the service elements that can be individually or collectively selected and configured:

- General tab — displays general customer and service information
- Components tab — displays the various service components in a tree format
- Sites tab — lists the sites that are included in the service
- L3 Access Interfaces tab — lists the L3 access interfaces that are included in the service
- Spoke SDP Bindings tab — displays the spoke SDP bindings that are associated with the service
- Address tab — lists the IP addresses that are associated with the service

Note — You cannot remove an IP address from an interface when the IP address of a static host is defined in the subnet of the interface IP address and the ARP Populate parameter is enabled on the Anti-Spoofing tab.

- Subscriber Interfaces tab — allows the creation and configuration of subscriber and group interfaces for L3 aggregation
- Redundant Interfaces tab — allows the creation and configuration of redundant interfaces
- Template tab — displays the template used to create the service, if applicable.
- Faults tab — displays the faults associated with the service

Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Modify the parameters for the service, as required.

Note 1 — To configure items on the Components tab, select and right-click on the items and choose Properties from the contextual menu.

Note 2 — To configure items on the tabs that contain lists of service elements, select the items and click on the Properties button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The IES Service (Edit) form closes, and the Manage Services form reappears.

7 Click on the Close button to close the Manage Services form.

Procedure 70-11 To view the service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The IES Service (Edit) form opens.

4 View the Aggregated Service Site Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab button to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab button to view the aggregated alarms for the object. The Aggregated Alarms tab is displayed.

8 Close the IES Service (Edit) form.

9 Close the Manage Services form.

Procedure 70-12 To view the service topology

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - map opens.

See chapter 4 for more information about service topology views.

Procedure 70-13 To modify an IES using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the component tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select an IES and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains two sub-procedures describing the components that can be created and modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating spoke SDP bindings. Go to step 9.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the Create IES Site option.

The Select Network Elements form appears.

5 Select one or more sites to add to the service and click OK. The IES Site (Create) form for the new site is displayed. If you selected more than one site, the IES Site (Multiple Instances) (Create) form for the new sites is displayed.

6 Click on OK. The IES Site (Create) (or IES Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

7 If you want to perform detailed configuration of site properties for the new site, right-click the site icon and select Properties from the contextual menu. The Site (Edit) form opens. Refer to Procedure 70-1 for detailed site configuration information.

8 Go to step 9 if you want to create spoke SDP bindings or go to step 16 to finish.

Creating spoke SDP bindings

9 Select the sites you want to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.

Note — When you create a spoke binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

10 Select Connect from the contextual menu and choose the Create Spoke SDP Binding option.

The Spoke SDP Binding (Create) form is displayed.

Note — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

11 Enable the Auto Select Transport Tunnel parameter.

12 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedure 70-6 for more detailed information on creating and configuring spoke SDP bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 30 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

13 Assuming that the spoke SDP binding was successfully created in step 12, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a spoke binding for the return tunnel.

14 Right-click on the second site you selected and choose the Create Spoke SDP Binding ... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

15 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 30 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

16 Close the Service Topology form.

17 Close the Manage Services form.

Procedure 70-14 To delete an IES

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose an IES from the list.

4 Click on the Delete button. A dialog box appears and prompts you to confirm that you understand the implications of deleting the service.

5 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

6 Close the Manage Services form.

71 — VPRN service management

71.1 VPRN service management overview

The 5620 SAM supports the creation of VPRN services using the 7450 ESS in mixed mode, 7750 SR and 7710 SR as a PE and provider core (P) router. VPRNs, also called IP VPNs or BGP/MPLS VPNs, are defined in RFC 2547bis. This standard describes a method of forwarding data and distributing routing information across an IP/MPLS service provider core network.

The 5620 SAM does not support the configuration of CE routers or devices.

VPRN services use BGP to exchange the VPRN routes among the PE routers that participate in the VPRN. This is done in a way that ensures that routes from different VPRNs remain distinct and separate, even if two VPRNs have an overlapping address space. PE routers distribute routes to CE routers in the VPRN. Since the CE routers do not peer with each other, there is no overlay visible to the VPRN's routing algorithm. The PE routers use BGP, RIP, or OSPFv2 as the IGP to distribute internal routes to the CE routers.

Each route in a VPRN service is assigned an MPLS label. When BGP distributes a VPRN route, it also distributes an MPLS label for that route. Before a customer data packet travels across the backbone network, it is encapsulated with the MPLS label that corresponds, in the customer VPRN, to the route that best matches the destination address of the packet.

The MPLS packet is further encapsulated with either another MPLS label or with an IP or GRE tunnel header, so that it gets tunneled across the backbone to the proper PE router. Each route exchanged by the MP-BGP protocol includes an RD that identifies the VPRN association. Thus the backbone core routers do not need to know the VPRN routes.

The 5620 SAM supports end-to-end VPRN configuration using the following methods:

- Tabbed configuration forms with an embedded navigation tree. The navigation tree provides a logical view of the service and acts as a configuration interface.
- Pre-configured template. A user that is assigned the template management role can create a service template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with service templates.

The 5620 SAM supports the configuration in a VPRN of an L3 aggregation mechanism called routed CO. Routed CO uses DHCP relay to manage dynamic subscriber hosts; the network resources for static subscriber hosts are explicitly provisioned. Routed CO supports all residential subscriber management functions of the 5620 SAM. See chapter 64 for more information about residential subscriber management and routed CO.

Routed CO uses a subscriber interface that defines up to 16 subnets on an NE at a release earlier than 7.0, or up to 256 subnets on an NE at Release 7.0 or later. A subscriber interface has child objects called group interfaces. A group interface supports the configuration of multiple SAPs as child objects. A SAP in a group interface supports all residential subscriber management functions. A group interface does not allow the specification of IP subnets or addresses, but inherits the addressing scheme of the parent subscriber interface. The 5620 SAM service topology map displays VPRN subscriber interfaces, group interfaces, and the associated SAPs.

You can configure Network Address Translation, or NAT, for dynamic subscriber hosts in a routed CO deployment. NAT implementation in a VPRN service requires a NAT configuration on the VPRN routing instance and a NAT policy that is associated with a subscriber profile. See chapter 27 for general information about configuring and deploying NAT. See chapter 43 for information about configuring a NAT policy. See chapter 64 for information about associating a NAT policy with a subscriber profile. See Procedure 71-1 for information about configuring NAT on a VPRN routing instance.

A VPRN routed CO allows a service provider to resell wholesale carrier services while providing direct DSLAM connectivity. You can create a VPRN service for the retailer and also define subscriber access and configuration information for the retailer network. See Procedure 71-11 for more information on how to define a wholesale and retail VPRN configuration.

IPCP extensions allow you to configure IP addresses and DNS names of remote devices to enable inter-operability with other networks. Specifically setting an IPCP extension is necessary to connect to a mobile service provider network. Routers for mobile services rely on other network routers to provide IP addresses and DNS names (primary and secondary) for a PPP link.

When an IPCP extension is configured, an edge device configured with PPP/MLPPP can signal a far end device.

The General tab of the 5620 SAM service management form displays useful information about the operational state of the service and its sites through the Aggregated Operational State and State Cause indicators.

The 5620 SAM provides OAM tools for service validation and for troubleshooting service and network transport issues. You can run an OAM Validation test suite for the service by clicking on the Validate button. If a check mark appears beside the OAM Validation Failed state cause indicator, the test has failed. The Validation Result tab on the Tests tab displays detailed information about the OAM test result. See chapter 35 for general information about fault management using OAM tools. See chapter 75 for more information about how to configure OAM validation test suites.

The Aggregated Operational State indicator has four possible values: Up, Down, Partially Down, and Unknown. The value is derived from the operational states of the sites that are part of the service, as follows:

- Up—all sites are operationally up
- Partially Down—at least one site is operationally down
- Down—all sites are operationally down
- Unknown—the service has no provisioned sites

When the Aggregated Service Site Operational State is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator. You can view alarms on the Faults page.

When the Aggregated Operational State is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM operator.

When you use the 5620 SAM to create or discover a service, the 5620 SAM assigns a default Service Tier value to the service. The Service Tier parameter value is relevant only in the context of composite service topology views. See chapter 72 for more information about the hierarchical organization of composite services.

Common to all device services, such as VPRN, are policies that are assigned to the service. Policies are defined at a global level and can then be applied to components of the service, such as interfaces or circuits, when the service is configured or modified. The following policies are common to all device services:

- QoS policies define ingress classification, policing, shaping, and marking on the ingress side of the interface. QoS policies are configured using the Access Ingress Policy form, the Access Egress Policy form, and the ATM QoS Policy form.
- Policer control policies to control access ingress policers and access egress policers under a common hierarchy. Policer control policies are configured using the Policer Control Policy Manager.
- Scheduling policies define hierarchical rate limiting and scheduling to govern the scheduling of queues. Scheduler policies are configured using the Scheduler Policy and HSMDA Scheduler Policy forms.
- Port scheduler policies define hierarchical bandwidth allocation and scheduling at the egress port level. Port scheduler policies are configured using the Port Scheduler Policy form.
- Filter policies control network traffic into or out of an interface or circuit based on IP or MAC matching criteria. Filter policies are configured using the ACL IP Filter form and the ACL MAC Filter form.
- Accounting policies measure the traffic on a service to ensure proper billing and enforcement of SLAs. Accounting policies are configured using the Accounting Policy form.
- ANCP policies provide status and control information based on port-up and port-down messages and current line rate changes between the edge device and the access node. ANCP policies are configured using the Manage Subscriber Policies form.
- Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination. Routing policies are configured using the Routing Policy Manager.

See chapter 43 for more information about policies.

VPRN service routers

A VPRN service consists of CE routers or devices connected to PE routers. PE routers connected to P routers transport data across the IP/MPLS provider core network in service tunnels.

Packets that arrive at an edge 7450 ESS, 7710 SR or 7750 SR are associated with a VPRN service based on the access interface on which they arrive. An access interface is uniquely identified by the following parameters:

- physical Ethernet port or POS port and channel
- encapsulation type
- encapsulation identifier (if required)

Table 71-1 describes the general functions performed by PE, P, and CE routers in a VPRN. See Figure 71-4 in this chapter for a sample VPRN. See the appropriate hardware services guide for more detailed information about VPRN functionality on the supported managed devices.

Table 71-1 VPRN router functionality

Router type	Functionality
PE	• Are directly connected to PE, CE, and P routers • Learn VPRN routes from CE devices using e-BGP, RIP, OSPFv2, or static routes • Maintain a separate routing table, called a VRF, for each service • Exchange multicast VPRN route information with PE routers in other autonomous systems using MP-BGP • Distribute MPLS inner labels using MP-BGP. Before data traverses the IP/MPLS backbone, it is encapsulated with the MPLS label that corresponds, within the VPRN, to the route that best matches the packet's destination address. • Distribute MPLS outer labels using RSVP-TE or LDP. Before the MPLS packet traverses the IP/MPLS backbone, it is further encapsulated with either another MPLS label or with a GRE or MPLS LSP service tunnel header, so that it is tunneled across the backbone to the appropriate PE router. • Use RDs to identify the VPRN associations • Use RTs to determine when a received route is destined for a VPRN • Terminate RFC 2684-encapsulated IPv4 traffic from ATM access network on SAPs
P	• Are directly connected to PE and P routers • Act as transit LSRs • Maintain routes to PE routers and are unaware of specific VPRN routing information
CE	• Are directly connected to PE routers • Provide customer access to the VPRN

Inter-AS connections

You can connect VPRN service sites (or VRFs) on multiple ASs using EGBP. ASs set up mutual connections by exchanging routing information, such as routes and labels. Labeled VPN-IPv4 routes are distributed within an AS on a PE router using IGBP and between ASs using EGBP on an ASBR. The ASBR redistributes VPN-IPv4 routes to an ASBR in another AS, which in turn distributes the routes to PE routers in its own AS or to an ASBR.

When a VPRN inter-AS connection is between two service providers, the ASs must be on private peering points. For an LSP to operate between ASBRs on the AS borders, EBGP peering must be set up between the ASBRs and MPLS label exchange must be supported. Furthermore, an LSP must run from a packet's ingress PE router to its egress PE router.

You can enable inter-AS connections from the BGP settings in Procedure 71-3.

MP-BGP Multicast IPv4

The MP-BGP multicast extension allows for a network topology that supports both multicast and unicast routing. Routes from the unicast routing table can be imported into the multicast routing table, and routes from the multicast routing table can be imported into the unicast routing table. An ASBR can be configured to advertise VPRN routes to peers in other ASs, redistributing unicast routes learned by BGP into MP-BGP routes, and MP-BGP routes into unicast routes. This configuration enables the support of the two sets of routing information.

The MP-BGP multicast extension specifies that BGP can exchange routing information for the multicast IPv4 address family within and between BGP ASs. All configurations entered in a multicast IPv4 address family for a BGP instance affect multicast services and are applied to the multicast routing table. See chapter 28 for more information about the configuration of BGP and the MP-BGP multicast extension.

IPv6 support

The 5620 SAM supports IPv6 configuration of the following functions in VPRN services on the 7710 SR and 7750 SR, and on the 7450 ESS in mixed mode:

- addressing for static routes, L3 access interfaces, and BGP peerings
- router advertisement, ICMP, DHCP, neighbor discovery, and ACL filtering

To configure IPv6 in a VPRN, you must first enable VPN IPv6 for BGP on the base routing instance of each device that acts as a site in the VPRN.

A customer can use an SNMP utility to manage the IPv6 objects in a VPRN service. SNMP mediation of VPRN objects requires the configuration of a community string on each site in the VPRN, regardless of the IP or SNMP version. SNMPv3 mediation of VPRN IPv6 objects, however, requires the additional configuration of an SNMP context for the VPRN using a CLI. See chapter 13 for information about configuring an SNMPv3 context for a VPRN.

Note — Release 6.0 R1 of the 7710 SR and 7750 SR does not include an SNMP context or community string in an SNMP trap PDU; an SNMP manager cannot differentiate between VPRN and non-VPRN traps from these devices.

PIM for VPRN

The PIM protocol can be applied to a VPRN service to create a private multicast distribution network. PIM uses an MDT group address to identify multicast traffic for the VPRN instance to prevent flooding of multicast packets to PE devices in the VPRN. VRFs with the same MDT address are members of that group and receive multicast traffic from each other. The MDT address cannot be in the SSM range.

By default, the PIM protocol only uses the information in the unicast routing table to determine the RPF interface. PIM can be configured to use the separate multicast and unicast routing tables built by MP-BGP to perform RPF lookups for multicast-capable sources to build and maintain distribution trees for multicast traffic forwarding. See chapter 28 for more information about configuring PIM to use multicast or unicast routing tables in RPF lookups.

Data-MDT

A data-MDT is a tunnel for high-bandwidth source traffic through the P-network to interested PE routers. Data-MDTs do not broadcast customer multicast traffic to all PE routers in a multicast domain.

Note — Data-MDTs are only supported for VPRN services.

Multicast data transmission from a CE router is typically delivered to all CE routers in the same multicast group. Some CE routers do not require the delivery of a specific multicast stream because there no downstream receivers for the multicast group. You can prune a PE router from the MDT if the router does not deliver multicast traffic to the attached CE routers. This task is beneficial for high-traffic multicast applications.

A data-MDT allows you to configure a traffic threshold in Kb/s. The 5620 SAM signals the data-MDTs when the bandwidth for the SSM group exceeds the configured threshold. The PE router sends an MDT join TLV, at 60 s intervals, over the default MDT to all PE routers. The routers respond with the following actions:

- PE routers that require the SSM group specified in the MDT join TLV; join the data-MDT used by the PE router to transmit the SSM group
- PE routers that do not require the SSM group specified in the MDT join TLV; do not join the data-MDT, pruning the PEs from the MDT

The transmitting PE router switches the multicast stream to the data-MDT after allowing the PE routers to join the data MDT. You can configure the data-MDT delay interval using the 5620 SAM.

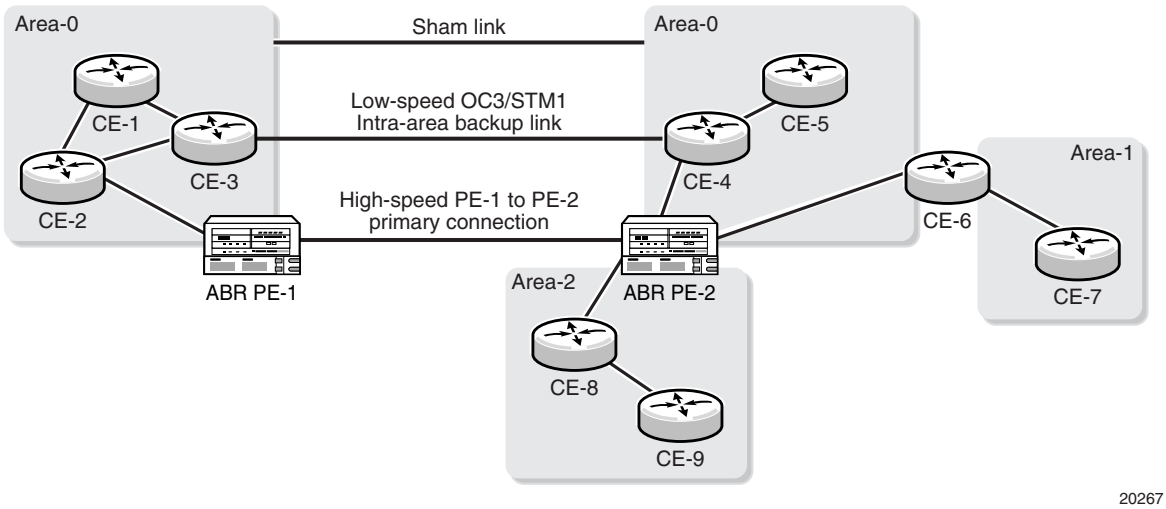
The PE router stops sending the MDT join TLV when the transmission bandwidth no longer exceeds the configured threshold. The PE routers using the data-MDT leave the group and transmission resumes over the default MDT.

OSPF sham link support

You can use the OSPF protocol to connect CE routers to PE routers over an MPLS VPN backbone. This can be useful for customers who subscribe to a VPN service and want to use OSPF as their intra-site routing protocol to exchange routing information between their sites. However, there is a potential configuration issue associated with this approach.

OSPF PE-CE connections assume that the only path between two client sites is across the MPLS VPN backbone. OSPF treats a link through a Layer 3 VPN as an inter-area link. However, other paths between VPN sites may also exist. For example, in Figure 71-1, the link between CE-3 and CE-4 (two CE routers in the same OSPF area) might be a low-speed OC3/STM1 intra-area backup link. OSPF preferentially utilizes intra-area links over inter-area links, and since it establishes an intra-area route connection between CE-3 and CE-4, the potentially high-speed PE-1 to PE-2 primary connection is not utilized.

Figure 71-1 Sham link configuration example



OSPF sham links can be created to resolve this problem. By creating and configuring a sham link as an intra-area link between PE-1 and PE-2, a normal OSPF adjacency is formed, and the link-state database is exchanged across the MPLS VPN. As a result, the desired intra-area connectivity is created between PE-1 and PE-2. In addition, the cost of the CE-3/CE-4 and PE-1/PE-2 links can be managed by the use of a numerical metric. You could then configure the service so that the CE-3/CE-4 link becomes a standby link only in event that the VPN fails.

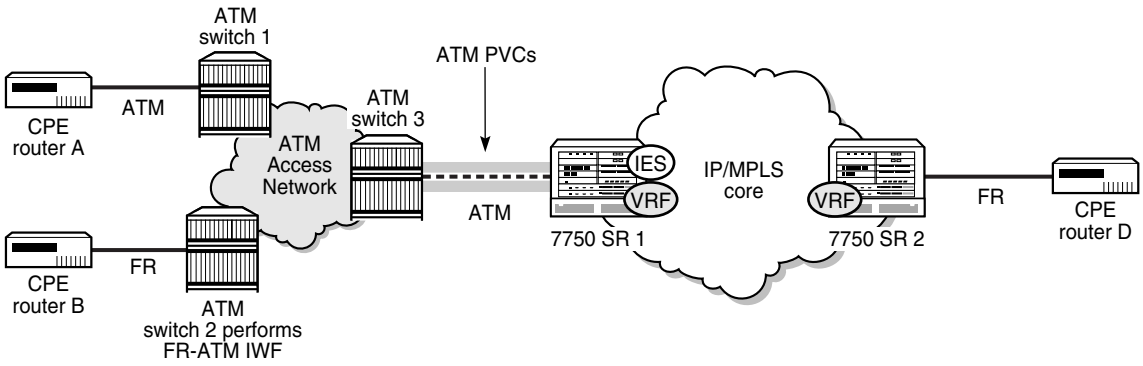
The use of OSPF sham links in the VPRN context is only applicable to 7450 ESS, 7710 SR and 7750 SR nodes.

ATM SAP terminations for VPRN

CE routers that have access to an ATM network can connect with a VPRN using ATM SAP terminations on a 7750 SR or 7710 SR. The interconnection between ATM point-to-point and L3 services uses RFC 2684-encapsulated IPv4 traffic over an ATM PVC that terminates on a specially configured SAP. All RFC 2684-encapsulated traffic can be routed over ATM networks, frame relay, or directly through ATM connections.

Figure 71-2 shows how CPE Router A in an ATM network can access L3 IP services, such as a VPRN, using a statically configured ATM PVC on a 7750 SR (SR#1). A SAP is configured on SR #1 to serve a specific VPRN as identified by the VRF. Destination CPE router D can receive RFC 2684-encapsulated traffic over an IP network through a Frame Relay over 7750 SR 2.

Figure 71-2 ATM SAP network connection to a VPRN



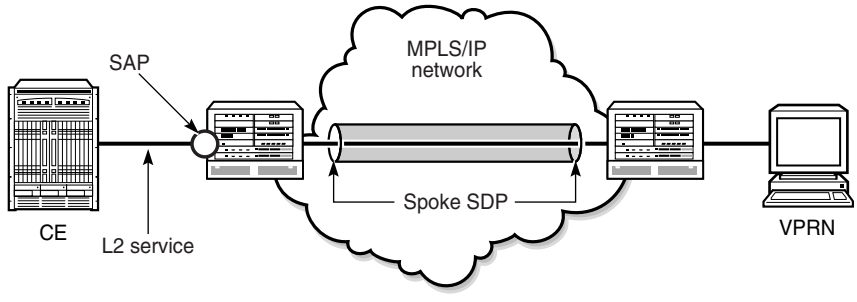
The two connection methods used between ATM and VPRN, which appear in 5620 SAM as AAL5 Encapsulation parameters: LLC/SNAP encapsulation and VC-multiplexing.

Epipe SDP spoke termination on VPRN services

A VLL Epipe service can terminate directly on a VPRN service using an SDP spoke on the 7750 SR, 7450 ESS, or 7710 SR. Traffic that terminates on a VPRN service is identified by the interface ID of the SDP on the L2 access router and the VC ID label in the service packet. All routing protocols supported by VPRN are also supported for spoke SDP termination.

Figure 71-3 shows a spoke SDP terminating directly on a VPRN. The spoke SDP could be tied to an Epipe or VPLS. No configuration is required for the CE-to-PE connection on the SAP.

Figure 71-3 SDP spoke termination on an L2 service



Routed CO dual homing using SRRP

Subscriber Router Redundancy Protocol (SRRP) allows two separate connections to an access NE such as DSLAM to operate in an active/standby configuration similar to the way in which VRRP interfaces operate. SRRP is a collection of functions and messaging protocols that allows a system to create a set of redundant gateway IP addresses that are shared by a local and remote NE.

Each SRRP instance is created within the context of a subscriber group IP interface and is identified by a unique SRRP instance ID. This SRRP instance ID only needs to be unique in the context of a specific NE. This SRRP instance controls the redundant routing for all subscriber subnets configured or associated with the group interface. One SRRP instance is supported for each group interface and the SRRP ID must be the same as the SRRP instance ID on the group IP interface on the redundant NE.

A subscriber subnet redundant gateway IP host address is assigned at the subscriber IP interface level and is used for all SRRP instances associated with the subscriber subnet. The redundant IP host address must be configured for a subscriber subnet before it can be associated with an SRRP instance.

When SRRP is active on a group interface, the SRRP instance advertises to a remote NE using in-band messaging on the group-interface SAPs and out-of-band messaging on the group-interface redundant interface. If the remote NE uses the same SRRP instance ID, one NE enters a master state, while the other NE enters a backup state. Since the NEs share a common SRRP gateway MAC address (used for the SRRP gateway IP address and for proxy ARP functions), either NE can act as the default gateway for the attached subscriber hosts. This functionality helps to preserve subscriber QoS enforcement. The master state allows routing to and from the subscriber hosts associated with the group IP interface. The backup state stops ingress forwarding for packets destined to the SRRP gateway MAC and causes all packets destined to subscriber hosts on the group IP interface to be forwarded to a redundant IP interface associated with the group IP interface.

Normally, when anti-spoofing is enabled on a group-interface SAP, the SAP drops SRRP packets because they do not contain a subscriber MAC or IP address. However, you can use a configuration option to enable anti-spoofing for subscriber hosts on a group-interface SAP that participates in SRRP advertisements.

The underlying mechanism to control master/backup state transitions is based on a dynamic priority level maintained by the SRRP instance. The SRRP instance with the highest priority level assumes the master operating state. An SRRP instance with a higher current priority level always preempts an SRRP instance with a lower priority level. If the priority levels are equal, the SRRP instance with the lowest source SRRP host IP address assumes the master state. The local SRRP instance priority may also be controlled by associating the instance with an existing VRRP policy.

The redundant IP interface is a special interface that connects two systems with one or more common SRRP instances. The interface is configured with a /31 address and a spoke SDP binding, creating an Ethernet pseudowire shortcut between the redundant NEs. When the SRRP instance is in backup state, the group interface associated with this instance is not allowed to forward or route traffic downstream towards the subscriber. As a result of this, the packets are shunted across the redundant interface so that the active group interface does the forwarding or routing.

If the redundant IP interface goes down, the system allows the group IP interfaces associated with the down interface to forward locally downstream, when they are in the backup SRRP state. While forwarding downstream in the backup state, the system uses the MAC address associated with the group IP interface, not the SRRP redundant gateway MAC address.

SRRP is supported on the 7450 ESS in mixed mode, 7710 SR and 7750 SR.

DoS protection

The 7450 ESS-7, 7450 ESS-12, 7750 SR-7, and 7750 SR-12 support DoS protection policies.

To protect a VPRN from a high incoming packet rate that characterizes a DoS attack, you can use the 5620 SAM to create DoS protection policies for the VPRN L3 access interfaces. A DoS protection policy limits the number of control-plane packets that an interface receives each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

You can configure a DoS protection policy to control the following on a VPRN L3 access interface:

- the control-plane packet arrival rate per subscriber host on the interface
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

Each VPRN L3 access interface on an NE that supports DoS protection is automatically assigned a default DoS protection policy. This default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified. See Procedure 18-3 for information about creating a DoS protection policy.

Local DHCP servers

The 5620 SAM supports configuring local DHCP servers on the 7710 SR and 7750 SR, and on the 7450 ESS. The local DHCP server leases IP addresses to clients in the network. Options are configured to define the IP address properties, such as, the length of time an IP address is active and which DNS server must be used. A local user database is used to authenticate and authorize clients requesting IP addresses from the local DHCP server. If the local DHCP server does not use the local user database, the server can use the GI address to assign free IP addresses, however it is not possible to configure match or authentication parameters.

Three applications are targeted for the Local DHCP server.

- Subscriber aggregation in a single node or TPSDA.
- Business services running VPRN and locally attached to the host can request and obtain IP addresses directly from the server.
- The DHCP server identifies an IP request from a PPPoE client and provides an IP address and options.

DHCP servers can be integrated with Enhanced Subscriber Management for DHCP and PPPoE clients. A local DHCP server can be created in the routing instance window or VPRN service site window. A local DHCP server created in the VPRN service site can be associated with the L3 access interface on a VPRN service only. A local DHCP server created in the routing instance window can be associated with a network interface or L3 access interface on IES.

Local user database

The 5620 SAM supports the configuration of a local user database on the 7710 SR and 7750 SR, and on the 7450 ESS. The local database is configured and associated with the local DHCP server to provide local authentication. The local DHCP server must have a pool of IP addresses configured, otherwise it is not able to lease IP addresses.

A create local user database configuration form is available from the Manage Residential Subscribers form. After a local user database is configured, it can be associated with a local DHCP server and PPPoE configurations on group interfaces.

When a local user database is not configured, you can use GI addresses to access free IP addresses, however the clients requesting the IP address are not authenticated.

PPPoE protocol on VPRN services

A VPRN service can be configured to run PPPoE protocol. PPPoE is used in subscriber networks to encapsulate PPP frames inside Ethernet frames. PPPoE combines the point-to-point protocol used with DSL sessions with the Ethernet protocol used to support multiple subscribers in a local area network. From the group interface configuration form you can assign a PPPoE policy and a local user database to authenticate PPPoE subscribers.

PPPoE termination in a business VPRN environment is also supported. This ability targets applications such as PPPoE VPRN with IP overlap, where there are two participants in the service:

- The “Wholesale VPRN”, which is a VPRN that provides access to the SAP.
- The “Retail VPRN”, which is a business VPRN that routes the packets belonging to the PPPoE sessions terminating in it. The Retail VPRNs may have overlapping IP addresses.

In this configuration, the PPPoE subscriber host terminates in a Retail VPRN and provides a routed path to the customer site. The VPRN service-id that carries it is determined by the service configuration, specifically:

- If a local user database is used, the Retail Service ID property that you specify in the PPPoE host configuration provides a reference to the VPRN service-id that should be used.
- If RADIUS is used for authentication, the retailer service-id is provided by an Alcatel-Lucent VSA.
- If MSAP is used, the SAP is created in the wholesale VPRN using the information from RADIUS.

The PPPoE session is negotiated with the parameters defined by the Wholesale VPRN interface. Since the IP address space of the subscriber management host may overlap between VPRN services, the node anti-spoofs the packets at access ingress with the session-id.

L2TP on VPRN services

The 5620 SAM supports the configuration of L2TP on a Release 8.0 or later 7750 SR, and on the 7450 ESS in mixed mode. L2TP is a session-layer protocol that extends the PPP model by allowing L2 and PPP endpoints to reside on different devices that are interconnected by a PSN. L2TP extends the PPP sessions between the CPE and PPP/L2TP termination points on the L2TP network server (LNS), via an intermediate L2TP access concentrator (LAC). The LAC is the initiator of session-generated L2TP tunnels; the LNS is the server that waits for new tunnels. Manually configured and initiated L2TP tunnels can be initiated or stopped from either the LNS or LAC.

At least one ISA-LNS group must be configured for the LNS NE.

On an LNS NE, L2TP destinations configured for L2TP tunnel profiles can include the following:

- loopback L3 access interfaces for a VPRN or IES service
- loopback interfaces configured for a base routing instance

Note — On a Release 7.0 7750 SR that acts as an LAC NE, each L2TP tunnel must have the local IP address set to the system interface IP address.

See chapter 15 for more information about ISA-LNS groups. See Procedure 17-19 for information about how to create and configure an ISA-LNS group. See chapter 28 for more information about L2TP.

See Procedure 71-1 for information about enabling L2TP on a VPRN router instance site. See Procedure 71-11 for information about configuring a VPRN group interface to terminate LNS PPP sessions.

IPsec

You can configure a VPRN with an IPsec interface for secure and encrypted tunneling between sites. An IPsec VPRN allows you to share secure and encrypted VPN traffic among multiple sites.

IPsec VPRN services include:

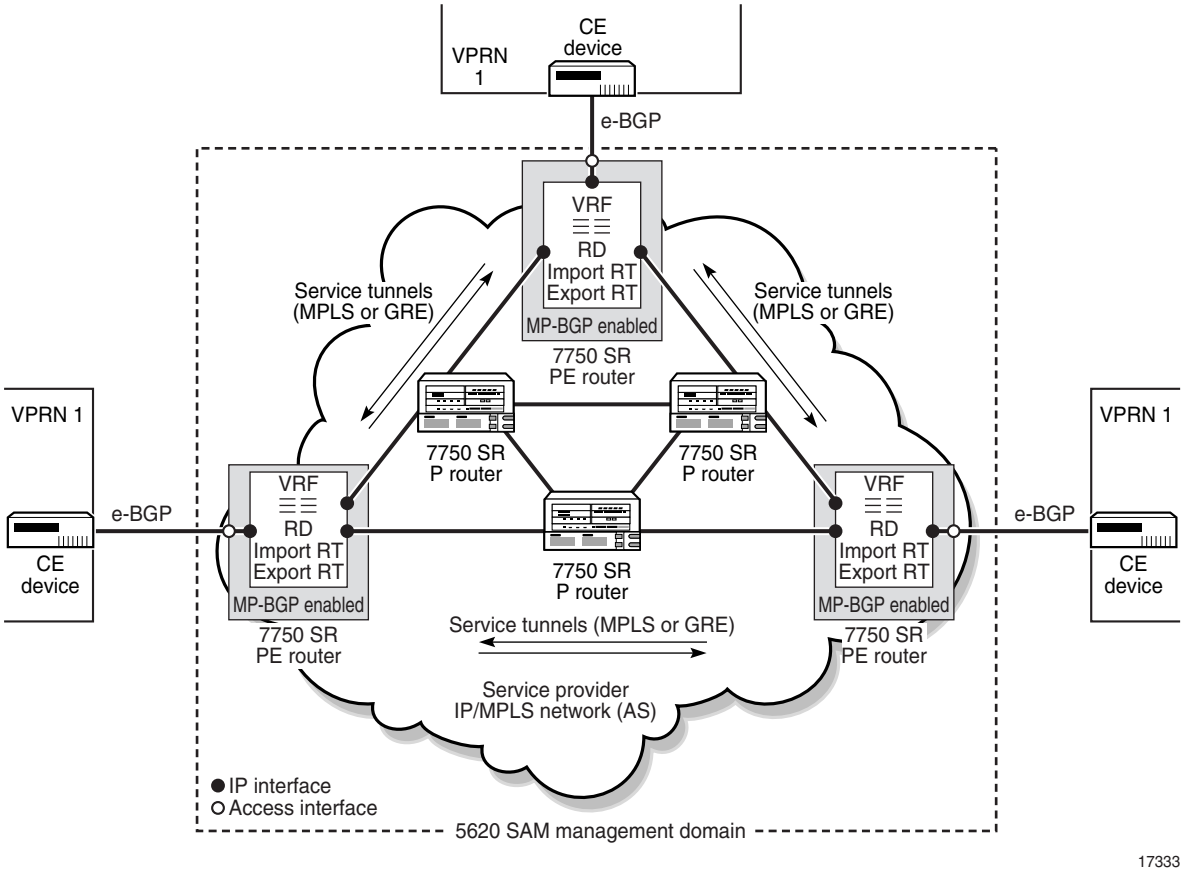
- NAT traversal
- DES, 3DES, AES-128, AES-192 and AES-256 encryption methods
- HMAC-MD5 and HMAC-SHA1 authentication and hashing methods
- Diffie-Hellman key generation algorithms
- Pre-shared keys and IKE shared secret with PFS key management authentication methods

See chapter 32 for more information about IPsec configuration.

71.2 Sample VPRN service configuration

Figure 71-4 shows a sample VPRN service configuration.

Figure 71-4 Sample VPRN Configuration



Assuming the core IP/MPLS or GRE network is already configured, Table 71-2 lists the high-level tasks that are required to configure the sample VPRN service.

Table 71-2 Sample VPRN service configuration

Task	Description

1. Configure policies as required	Policies should be configured before you create a service. Participation in policies is defined when you configure or modify resources, such as access interfaces or circuits, during service creation or modification. The following key policies can be applied to resources that are part of a VPRN.
	• Routing policies.
	  • Choose Policies→Routing→Statement to open the routing policy-statements form.
	  • Choose Policies→Routing→Prefix List to open the routing policy-prefix lists form.
	  • Choose Policies→Routing→Community to open the routing policy-communities form.
	  • Choose Policies→Routing→Damping to open the routing policy-dampings form.
	  • Choose Policies→Routing→AS Path to open the routing policy-AS paths form.
	• Access ingress and egress interface policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress to open these forms.
	• Scheduler policies. Choose Policies→QoS→SROS QoS→Scheduler to open the scheduler policy form.
	• ACL IP filter policies. Choose Policies→Filter→ACL IP Filter to open the ACL form.
	• Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form.
	• ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form.

2. Configure ports as access ports for use in the service	Right-click on a port from the equipment navigation tree and choose Properties. Specify the port as an access port and optionally specify an encapsulation type.
3. Configure service tunnels as required	Choose Manage→Service Tunnels to create service tunnels. Service tunnels carry service traffic between edge-managed routers by circuits aggregated in unidirectional service tunnels. Circuits can be associated with service tunnels during service configuration.
4. Configure MP-BGP for PE-to-PE routing.	Perform the following steps. See chapter 28 for more information about protocol configuration. • Right-click on a router instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the Protocols tab and select the BGP check mark box. • Right-click on the BGP instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the VPN tab and enable VPN IPv4 or VPN IPv6 as required. Enable Multicast IPv4 or Multicast IPv6 to apply a multicast definition to this BGP routing instance. Click on the Behavior tab and set the Enable Inter AS VPRN parameter to true. • Right-click on the BGP Peer Group instance in the Routing view of the network navigation tree and choose Create Peer. In the Peer form that opens, configure the Peer Address and other parameters.
5. Create and configure customers	Choose Manage→Service→Customers to open the customer manager form and create a customer.

(1 of 2)

Task	Description

6. Create and configure VPRN 1.	Ensure that the operator creating the service has Service Mgmt and Interface Mgmt user group privileges. See chapter 8 for more information about user and user group privileges.
	Choose Create→Service→VPRN. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure VPRN 1.
	• Specify the newly created customer as the customer for the VPRN 1.
	• Specify and configure the VPRN service sites. Perform the following for each VRF:
	  • Configure autobinding to specify that the service is automatically bound to service tunnels.
	  • Configure routing properties.
	  • Configure the route distinguisher.
	  • Configure VRF targets.
	  • Configure import and export route targets.
	  • Configure import and export routing policies.
	  • Configure BGP on the PE VPRN sites for PE-to-CE routing. See chapter 28 for information about routing protocol configuration.
	  • If required, configure a GSMP group and a GSMP group neighbor
	  • If required, configure PIM to create a multicast domain within the VPRN.
	  • If required, configure the RPF Lookup Sequence parameter to specify which routing tables PIM uses for standard multicast and unicast RPF lookups.
	  • If required, configure an override source IP address or L3 interface used by IP applications to communicate with the site.
	• Create and configure an access interface on each VPRN service site.
	  • Configure general parameters such as a name, ID, and MAC address.
	  • Specify a port that is in access or hybrid mode.
	  • Assign ingress and egress QoS policies as required.
	  • Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
	  • Assign ACL filter policies as required.
	  • Assign an accounting policy, if required.
	  • Specify a local DHCP server, if required.
	  • Specify a ToD suite, if required.
	  • Configure subscriber management parameters, if required.
	  • Specify a DoS protection policy, if required.
	  • Configure a local IP address.
	  • Configure the ARP timeout and proxy ARP settings, if required.
	  • Configure ICMP parameters, if required.
	  • Configure IPCP parameters, if required.
	  • Configure DHCP parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure anti-spoofing parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure router advertisement parameters.
	  • Configure ANCP parameters, if required.

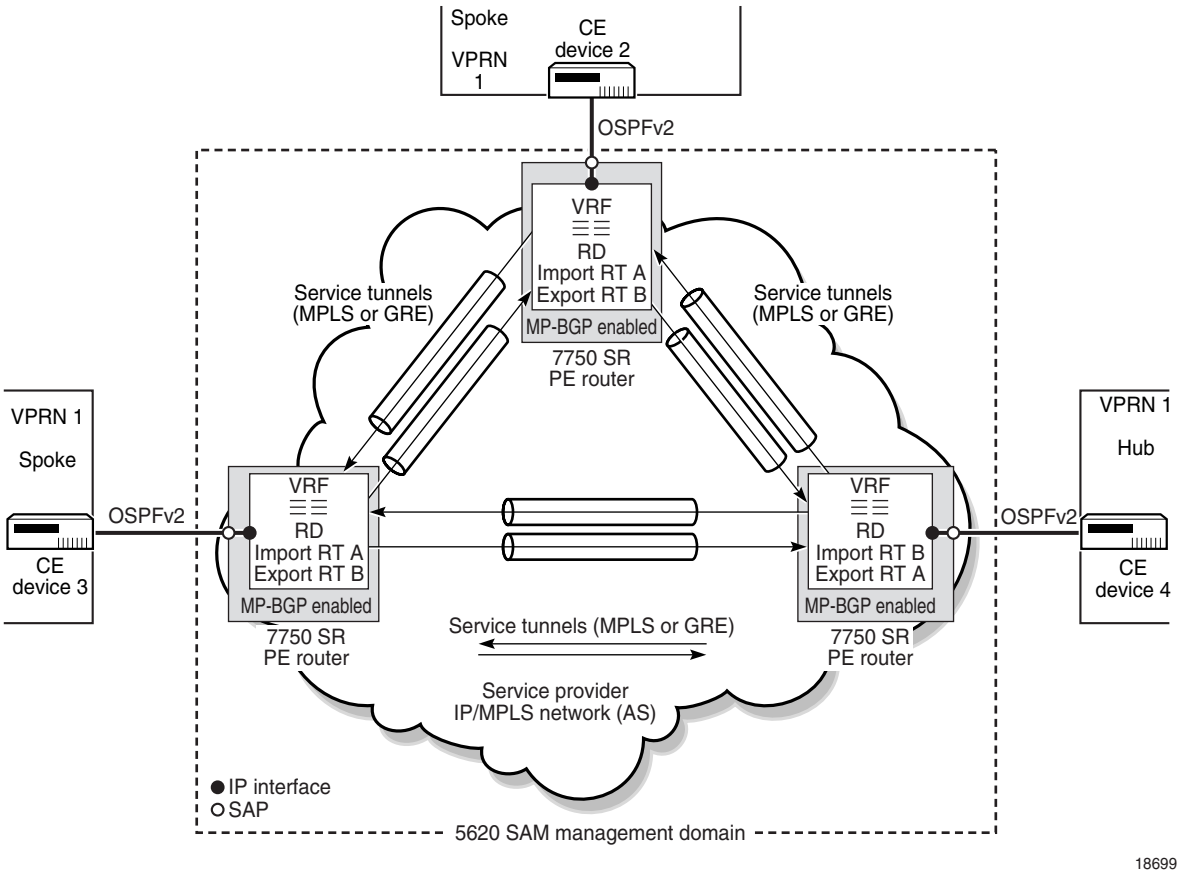
(2 of 2)

71.3 Sample hub-and-spoke VPRN configuration

In a hub-and-spoke VPRN, the majority of the traffic is exchanged between the hub (for example, headquarters) and spoke sites (for example, branches). Traffic between spoke sites passes through the hub site. Spoke sites advertise their routes to the hub site, which in turn advertises these routes to the other spoke sites.

Figure 71-5 shows a sample hub-and-spoke VPRN service configuration. Your configuration will vary depending on your network requirements.

Figure 71-5 Sample hub-and-spoke VPRN Configuration



Assuming the core IP/MPLS or GRE network is already configured, Table 71-3 lists the high-level tasks that are required to configure this sample hub-and-spoke VPRN service.

Table 71-3 Sample hub-and-spoke VPRN service configuration

Task	Description

1. Configure policies as required	Policies should be configured before you create a service. Participation in policies is defined when you configure or modify resources, such as access interfaces or circuits, during service creation or modification. The following key policies can be applied to resources that are part of a VPRN.
	• Routing policies.
	  • Choose Policies→Routing→Statement to open the routing policy-statements form.
	  • Choose Policies→Routing→Prefix List to open the routing policy-prefix lists form.
	  • Choose Policies→Routing→Community to open the routing policy-communities form.
	  • Choose Policies→Routing→Damping to open the routing policy-dampings form.
	  • Choose Policies→Routing→AS Path to open the routing policy-AS paths form.
	• Access ingress and egress interface policies. Choose Policies→QoS→SROS QoS→Access Ingress or Access Egress to open these forms.
	• Scheduler policies. Choose Policies→QoS→SROS QoS→Scheduler to open the scheduler policy form.
	• ACL IP filter policies. Choose Policies→Filter→ACL IP Filter to open the ACL form.
	• Accounting policy. Choose Tools→Statistics→Accounting Policies to open the accounting policy form.
	• ANCP policy. Choose Policies→Residential Subscriber to open the Manage Subscriber Policies form.
	• DoS protection policy. Choose Administration→Security→NE DoS Protection to open the NE DoS protection form.

2. Configure ports as access ports for use in the service	Right-click on a port in the equipment navigation tree and choose Properties. Specify the port as an access port and specify an encapsulation type, if required.
3. Configure service tunnels as required	Choose Manage→Service Tunnels to create service tunnels. Service tunnels carry service traffic between edge-managed routers by circuits aggregated in unidirectional service tunnels. Circuits can be associated with service tunnels during service configuration.
4. Configure MP-BGP for PE-to-PE routing.	Perform the following steps. See chapter 28 for more information about protocol configuration. • Right-click on a router instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the Protocols tab and select the BGP check mark box. • Right-click on the BGP instance in the Routing view of the network navigation tree and choose Properties. In the Properties form that opens, click on the VPN tab and enable VPN IPv4 or VPN IPv6 as required. Enable Multicast IPv4 or Multicast IPv6 to apply a multicast definition to this BGP routing instance. Click on the Behavior tab and set the Enable Inter AS VPRN parameter to true. • Right-click on the BGP Peer Group instance in the Routing view of the network navigation tree and choose Create Peer. In the Peer form that opens, configure the Peer Address and other parameters.
5. Create and configure customers	Choose Manage→Service→Customers to open the customer manager form and create a customer.

(1 of 2)

Task	Description

6. Create and configure VPRN 1	Ensure that the operator creating the service has Service Mgmt and Interface Mgmt user group privileges. See chapter 8 for more information about user and user group privileges.
	Choose Create→Service→VPRN. Use the tabbed form and embedded navigation tree to configure the service. You configure the following key elements when you configure VPRN 1.
	• Specify the newly created customer as the customer for the VPRN 1.
	• Specify and configure the sites for VPRN 1. For each VRF:
	  • Configure autobinding to specify that the service is automatically bound to service tunnels.
	  • Configure routing properties.
	  • Configure the route distinguisher.
	  • Configure VRF targets.
	  • Configure import and export route targets.
	  • Configure import and export routing policies.
	  • Configure BGP on the PE VPRN sites for PE-to-CE routing. See chapter 28 for information about routing protocol configuration.
	  • Configure other routing protocols on the sites, as required.
	  • If required, configure a GSMP group and a GSMP group neighbor
	  • If required, configure PIM to create a multicast domain within the VPRN.
	  • If required, configure the RPF Lookup Sequence parameter to specify which routing tables PIM uses for standard multicast and unicast RPF lookups. See chapter 28 for more information about protocol configuration.
	  • If required, configure an override source IP address or L3 interface used by IP applications to communicate with the site.
	• Create and configure one or more access interface on each VPRN service site.
	  • Configure general parameters such as a name, ID, and MAC address.
	  • Specify a port that is in access or hybrid mode.
	  • Assign ingress and egress QoS policies as required.
	  • Assign an aggregation scheduler for traffic rate limiting across the card or port, if required. Otherwise, assign ingress and egress scheduler policies.
	  • Assign ACL filter policies as required.
	  • Assign an accounting policy, if required.
	  • Specify a local DHCP server, if required.
	  • Specify a ToD suite, if required.
	  • Configure subscriber management parameters, if required.
	  • Specify a DoS protection policy, if required.
	  • Configure a local IP address.
	  • Configure the ARP timeout and proxy ARP settings, if required.
	  • Configure ICMP parameters, if required.
	  • Configure IPCP parameters, if required.
	  • Configure DHCP parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure anti-spoofing parameters, if required.
	  • Configure VRRP parameters, if required.
	  • Configure router advertisement parameters.
	  • Configure ANCP parameters, if required.

(2 of 2)

71.4 Workflow to create a VPRN service

1 Set up group and user access privileges.

2 Configure equipment and the network.

   i Build the IP or IP/MPLS core network.

   ii Create service tunnels, if required.

   iii Configure ports for the service as access ports.

3 Configure pre-defined routing, QoS, scheduling, filter, accounting, and time of day suite policies. You do not have to create pre-defined policies if policies are created on a per-service basis.

4 Provision the service.

   i Create and configure the VPRN for a customer.

   ii Apply protocols, such as BGP, OSPFv2, PIM, RIP or L2TP, and apply PIM and IGMP interfaces to the VPRN service, if required.

5 Turn up the service.

71.5 VPRN service management procedures

Use the following procedures to perform VPRN creation and management tasks.

Procedure 71-1 To create a VPRN service using configuration forms

1 Choose Create→Service→VPRN from the 5620 SAM main menu. The VPRN (Create) form opens with the General tab displayed.

2 Click on the Select button to choose a customer to associate with the VPRN. The Select Customer - VPRN (Create) form opens.

3 Select a customer for the VPRN and click on the OK button. The Select Customer - VPRN (Create) form closes and the VPRN (Create) form refreshes with the customer information.

4 Configure the parameters:

- Auto-Assign ID
- Service ID
- Service Name
- Description
- Service Tier
- Administrative State
- Automatic Mesh SDP Binding Creation
- Profile Name
- OLC State

The Profile Name parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled.

The OLC State parameter is configurable after you click on the Apply button.

5 Perform one of the following:

a Create a site for the VPRN. Go to step 6.

b Complete service creation, if sites and access interfaces for the VPRN are to be created later. Go to step 80.

6 Click on the Components tab button.

7 Select and then right-click on VPRN and choose Create Site. The Select Network Elements - VPRN form opens with a list of available sites displayed.

8 Select a site and click on the OK button. The Site (Create) form opens with the General tab displayed.

9 Configure the parameters:

- Name
- Description
- Administrative State
- Monitor Access Interface Operational State
- Enable Hash Label
- GSMP Administrative State

10 To configure NAT on the VPRN Site, click on the NAT Configuration tab button. Otherwise, go to step 22.

Note — NAT configuration is supported only on a Release 8.0 or later 7750 SR-7 or 7750 SR-12 in chassis mode B or higher.

11 Click on the Add button. The NAT Configuration (Create) form opens with the General tab displayed.

12 Click on the Select button to choose a NAT policy. The Select NAT policy form opens.

13 Select a policy in the list and click on the OK button. The Select NAT policy form closes, and the policy name is displayed on the NAT Configuration (Create) form.

14 Click on the Apply button. A dialog box appears.

15 Click on the Yes button.

16 Perform the following steps to configure static port forwarding, if required.

Note — You can configure NAT static port forwarding only for large-scale NAT.

i Click on the Static Port Forwarding tab button.

ii Click on the Add button. The NAT Static Port Forwarding Display (Create) form opens.

iii Configure the IP Address parameter.

iv Click on the Port Configuration tab button.

v Click on the Add button. The NAT Static Port Forwarding Port Display (Create) form opens.

vi Configure the parameters:

- Port
- Protocol
- Outside Port

Note — You cannot specify the same set of Port and Protocol values in more than one static port mapping to an IP Address.

You can specify the same Outside Port value in multiple mappings to an IP Address.

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The NAT Static Port Forwarding Port Display (Create) form closes, and the new entry is listed on the NAT Static Port Forwarding Display (Create) form.

ix Repeat steps v to viii to assign an additional static address, if required.

x Click on the General tab button.

xi Configure the Administrative State parameter.

xii Click on the OK button. A dialog box appears.

xiii Click on the OK button. The NAT Static Port Forwarding Display (Create) form closes, and the new static port forwarding entry is displayed on the NAT Configuration (Create) form.

17 Perform the following steps to configure a NAT pool.

i Click on the NAT Pools tab button.

ii Click on the Add button. The NAT Pool (Create) form opens.

iii Configure the parameters:

- Displayed Name
- Description
- NAT Pool Type
- Administrative State
- Port Reservation Type
- Port Reservation Value
- High Watermark
- Low Watermark

iv Click on the Select button to choose an ISA-NAT group. The Select ISA-NAT group form opens.

v Select an ISA-NAT group in the list and click on the OK button. The Select ISA-NAT group form closes, and the ISA-NAT group name is displayed on the NAT Pool (Create) form.

vi Click on the NAT Pool Ranges tab button.

vii Click on the Add button. The NAT Pool Range (Create) form opens.

viii Configure the parameters:

- Description
- Range Start
- Range End

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The NAT Pool Range (Create) form closes, and the NAT Pool (Create) form lists the pool range.

xi Click on the OK button. A dialog box appears.

xii Click on the OK button. The NAT Pool (Create) form closes, and the NAT Configuration (Create) form lists the NAT pool.

xiii Repeat steps vii to xii to add another pool, if required.

18 Perform the following steps to add an IP address for L2-aware NAT forwarding, if required.

i Click on the L2 Aware IP Addresses tab button.

ii Click on the Add button. The L2 Aware IP (Create) form opens.

iii Configure the parameters:

- IP Address
- Prefix Length

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The L2 Aware IP (Create) form closes, and the NAT Configuration (Create) form lists the IP address.

vi Repeat steps ii to v to add another IP address, if required.

19 Perform the following steps to add a NAT destination address.

i Click on the NAT Destinations tab button.

ii Click on the Add button. The NAT Destination (Create) form opens.

iii Configure the parameters:

- IP Address
- Prefix Length

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The NAT Destination (Create) form closes, and the NAT Configuration (Create) form lists the destination.

vi Repeat steps ii to v to add another destination, if required.

20 Click on the OK button. A dialog box appears.

21 Click on the Yes button. The NAT Configuration (Create) form closes, and the NAT configuration is listed on the VPRN Site form.

22 If the VPRN site is to support multicasting, click on the MVPN tab button and perform steps 23 to 33; otherwise go to step 34.

23 Click on the Routing sub-tab to configure an MVPN VRF instance.

24 Configure the MVPN VRF Target Type parameter:

a Specify None if you do not want to specify a VRF target for the site. Go to step 28.

b Specify Define Default if you want to specify a default VRF target for the site. Go to step 25.

c Specify Define Import and Export if you want to specify import and export VRF targets for the service site. Go to step 26.

Route targets are used to identify the VRFs of a VPRN. A PE router that is not a route reflector or an AS border router installs a VPRN route only when its import target matches the target of the route.

A fully-meshed VPRN requires one target for all participating VRFs. A hub-and-spoke VPRN requires VRF import and export targets. The export target of the hub VRF must be the same as the import target of the spoke VRFs. The import target of the hub VRF must be the same as the export target of the spoke VRF. VPRN VRF targets must not overlap.

25 Configure the Target Format parameter by performing one of the following steps:

a To specify a two-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value
- Target Extended Community Value

The Target AS Value is the Autonomous System number of the PE node. For the Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 44.

b To specify an IP Address for the default target, if required:

i Configure the parameters:

- Target IP Address
- Target Community Value

ii Go to step 44.

c To specify a four-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value (4Byte)
- Target Community Value

The Target AS Value (4Byte) is the Autonomous System number of the PE node. For the Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 44.

26 Configure the Import Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF import target format for the site, then go to step 27.

b Choose AS as the two-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value
- Import Target Extended Community Value

The Import Target AS Value is the two-byte Autonomous System number of the PE node. For the Import Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When

all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 27.

c Choose IP Address as the import target format for the site.

i Configure the parameters:

- Import Target IP Address
- Import Target Community Value

ii Go to step 27.

d Choose AS-4Byte as the four-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value (4Byte)
- Import Target Community Value

The Import Target AS Value (4Byte) is the four-byte Autonomous System number of the PE node. For the Import Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 27.

27 Configure the Export Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF export target format for the site, then go to step 28.

b Choose AS as the two-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value
- Export Target Extended Community Value

The Export Target AS Value parameter is the two-byte Autonomous System number of the PE node. For the Export Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 28.

c Choose IP Address as the export target format for the site.

i Configure the parameters:

- Export Target IP Address
- Export Target Community Value

ii Go to step 28.

d Choose AS-4Byte as the four-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value (4Byte)
- Export Target Community Value

The Export Target AS Value (4Byte) parameter is the four-byte Autonomous System number of the PE node. For the Export Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 28.

28 Click on the Import Policies sub-tab.

29 Configure the Import Unicast parameter. If you set the parameter to True, go to step 31.

30 Specify up to five Unicast import policies by using the Select button to choose a policy from the filtered list.

31 Click on the Export Policies sub-tab.

32 Configure the Export Unicast parameter. If you set the parameter to True, go to step 34.

33 Specify up to five VRF export policies by using the Select button to choose a policy from the filtered list.

34 If the VPRN site is to support IPv6 addressing (for router advertisement or neighbor discovery) or VRRP objects, perform the following substeps to configure an SNMP community for mediating the IPv6 objects.

i Click on the SNMP Community tab button.

ii Click on the Add button. The SNMP Community (Create) form opens.

iii Configure the SNMP Community String parameter.

iv Click on the OK button. The SNMP community string entry is displayed on the Site (Create) form and a dialog box appears.

v Click on the OK button. The SNMP Community (Create) form closes.

Note — When the 5620 SAM uses SNMPv2 for device mediation, you must configure one and only one SNMP community string for the VPRN site. Otherwise, there is no mediation of the VPRN IPv6 objects on the site, and the 5620 SAM raises an alarm. The alarm is cleared and mediation resumes after the configuration is modified so that exactly one SNMP community string is associated with the VPRN site.

35 Perform the following substeps to enable one or more routing protocols on the site.

i Click on the Protocols tab button.

ii Configure the parameters:

- BGP Enabled
- OSPFv2 Enabled
- OSPFv3 Enabled
- RIP Enabled
- L2TP Enabled

When you choose a protocol, the site and the protocols that are enabled on the site appear in the list panel.

iii If both the OSPFv2 Enabled parameter and the OSPFv3 Enabled parameter are disabled, navigate to the Components view of the VPRN, right-click on Protocols, then select Create OSPF. The OSPF Routing Instance (Create) form opens. In the OSPF Instance panel, configure the Version parameter.

iv Configure multicast for the site, if required. Click on the Multicast tab button.

v Configure the parameters:

- PIM Enabled
- IGMP Enabled

When you choose a protocol, the site and the protocols that are enabled on the site appear in the list panel.

36 Click on the Routing tab button to configure a routing instance. The General tab is displayed.

37 Configure the parameters:

- Router ID
- Maximum Number of Equal Cost Routes
- Autonomous System
- Type
- Enforce Maximum Number of Routes
- Route Distinguisher Type
- Enforce Maximum Number of Multicast Routes
- Maximum Number Of IPv6 Routes
- Log Only
- Threshold (%)

When you set the Route Distinguisher Type parameter to Type 0, the following configurable parameters appear:

- Type 0 Administrative Value
- Type 0 Assigned Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique RD from the drop-down menu.

The Type 0 Administrative Value is the Autonomous System (AS) number of the PE node. For the Type 0 Assigned Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

When you set the Route Distinguisher Type parameter to Type 1, the following configurable parameters appear:

- Type 1 IP Address
- Type 1 Assigned Value

When you set the Route Distinguisher Type parameter to Type 2, the following configurable parameters appear:

- Type 2 Administrative Value
- Type 2 Assigned Value

When you select the Enforce Maximum Number of Routes parameter, the following configurable parameters appear:

- Maximum Number of Routes
- Log Only
- Threshold (%)

When you select the Enforce Maximum Number of Multicast Routes parameter, the following configurable parameters appear:

- Maximum Number of Multicast Routes
- Log Only
- Threshold (%)

38 Configure the parameters:

- Single SFM Overload Admin State
- Hold-Off Time (seconds)

The Hold-Off Time (seconds) parameter and read-only attributes Overload State, Overload Start, and Overload Duration are only displayed when the Single SFM Overload Admin State parameter is set to Up.

39 Click on the VRF Target tab button to configure a VRF instance.

40 Configure the VRF Target Type parameter:

a Specify None if you do not want to specify a VRF target for the site. Go to step 44.

b Specify Define Default if you want to specify a default VRF target for the site. Go to step 41.

c Specify Define Import and Export if you want to specify import and export VRF targets for the service site. Go to step 42.

Route targets are used to identify the VRFs of a VPRN. A PE router that is not a route reflector or an AS border router installs a VPRN route only when its import target matches the target of the route.

A fully-meshed VPRN requires one target for all participating VRFs. A hub-and-spoke VPRN requires VRF import and export targets. The export target of the hub VRF must be the same as the import target of the spoke VRFs. The import target of the hub VRF must be the same as the export target of the spoke VRF. VPRN VRF targets must not overlap.

41 Configure the Target Format parameter by performing one of the following steps:

a To specify a two-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value
- Target Extended Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Target AS Value is the Autonomous System number of the PE node. For the Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 44.

b To specify an IP Address for the default target, if required:

i Configure the parameters:

- Target IP Address
- Target Community Value

ii Go to step 44.

c To specify a four-byte AS number for the default target, if required:

i Configure the parameters:

- Target AS Value (4Byte)
- Target Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Target AS Value (4Byte) is the Autonomous System number of the PE node. For the Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 44.

42 Configure the Import Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF import target format for the site, then go to step 43.

b Choose AS as the two-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value
- Import Target Extended Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Import Target AS Value is the two-byte Autonomous System number of the PE node. For the Import Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 43.

c Choose IP Address as the import target format for the site.

i Configure the parameters:

- Import Target IP Address
- Import Target Community Value

ii Go to step 43.

d Choose AS-4Byte as the four-byte import target format for the site.

i Configure the parameters:

- Import Target AS Value (4Byte)
- Import Target Community Value

You can click on the Suggest Value button to let the 5620 SAM assign these values. Choose Generate Unique VRF Target from the drop-down menu.

The Import Target AS Value (4Byte) is the four-byte Autonomous System number of the PE node. For the Import Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 43.

43 Configure the Export Target Format parameter by performing one of the following steps:

a Choose None to specify no VRF export target format for the site, then go to step 44.

b Choose AS as the two-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value
- Export Target Extended Community Value

The Export Target AS Value parameter is the two-byte Autonomous System number of the PE node. For the Export Target Extended Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 44.

c Choose IP Address as the export target format for the site.

i Configure the parameters:

- Export Target IP Address
- Export Target Community Value

ii Go to step 44.

d Choose AS-4Byte as the four-byte export target format for the site.

i Configure the parameters:

- Export Target AS Value (4Byte)
- Export Target Community Value

The Export Target AS Value (4Byte) parameter is the four-byte Autonomous System number of the PE node. For the Export Target Community Value, the 5620 SAM assigns the next unused number within the valid range. When all of the numbers within the valid range have been used once, the system starts at the beginning of the range and assigns the next available number.

ii Go to step 44.

44 Configure ingress multicast forwarding, if required.

i Click on the Mcast Path Mgmt tab button.

ii Click on the Select button beside the Name parameter. The Select Ingress Info Policy - Service L3 Routing list form opens.

iii Choose an ingress info policy and click on the OK button. The Select Ingress Info Policy - Service L3 Routing list form closes.

Note — The Mcast Path Mgmt Channels tab displays data on the operational channels after actual traffic from a specific multicast source for a specific multicast group passes through the virtual router. You must click on the Search button to refresh the data. See chapter 43 for a listing of the displayed operational channel parameters.

45 Click on the Auto-Bind tab button to configure the binding of the site to service tunnels.

46 Configure the Transport parameter.

a Choose None to explicitly specify service tunnels and circuits for the service.

b Choose LDP for the service to be automatically bound to MPLS service tunnels utilizing LDP.

Note — To use MPLS as the transport type, you must bind LSPs to service tunnels during service tunnel configuration. See Procedure 30-1 for more information.

c Choose RSVP-LSP for the service to be automatically bound to MPLS service tunnels utilizing RSVP-LSP.

Note — The RSVP-LSP option is available only for a Release 7.0 or later 7710 SR or 7750 SR, or a 7450 ESS in mixed mode.

d Choose RSVP or LDP for the service to be bound to MPLS service tunnels utilizing either RSVP or LDP.

This choice provides the ability to simultaneously support both tunnel options, in networks that have a mixture of LDP and RSVP-TE in place. 5620 SAM always tries to resolve the VPN route by using RSVP-LSP tunnels first (lowest metric). If no RSVP-LSP service tunnels are available, then tunnels configured for LDP are used. If RSVP-LSP tunnels subsequently become available again, then the route resolution automatically returns to RSVP-LSP.

Note — The RSVP or LDP option is available only for a Release 7.0 R3 or later 7710 SR or 7750 SR, or a 7450 ESS in mixed mode.

e Choose GRE for the service to be automatically bound to GRE service tunnels.

47 Click on the VRF Import Policies tab button.

48 Specify up to five VRF import policies by using the Select button to choose a policy from the filtered list.

49 Click on the VRF Export Policies tab button.

50 Specify up to five VRF export policies by using the Select button to choose a policy from the filtered list.

51 Configure static routes, if required.

i Click on the Static Routes tab button.

ii Click on the Add button to define a static route that the PE VRF is to exchange with the CE. The Static Route (Create) form opens.

iii Configure the parameters:

- Auto-Assign ID
- Static Route ID
- BFD Enabled
- Multicast Capable Peers
- Destination
- Prefix Length
- Type
- IP Address
- Preference
- Metric
- Administrative State
- Tag
- Enable CPE Check
- Target IP Address
- Interval (seconds)
- Drop Count
- Log
- Prefix List Name
- Prefix List Flag

The IP Address parameter is configurable when the Type parameter is set to an option other than Black Hole.

The Target IP Address, Interval (seconds), Drop Count, and Log parameters are only displayed when Enable CPE Check is enabled.

You cannot specify a Prefix List if either BFD Enabled or Enable CPE Check parameters are enabled for the static route.

The Prefix List Flag parameter is only displayed once the Prefix List Name parameter is configured.

iv Click on the OK button. The Static Route (Create) form closes and the Site (Create) form reappears.

52 Configure a GSMP group on the site, if required.

i Click on the GSMP tab button.

ii Click on the Add button. The GSMP Group (Create) form opens with the General tab displayed.

iii Configure the following parameters:

- Displayed Name
- Description
- Administrative State
- Keep-Alive (seconds)
- Hold Multiplier
- OAM Administrative State
- Dynamic Topology Discovery

iv Click on the GSMP Group Neighbor tab button.

v Click on the Add button. The GSMP (Create) form opens with the General tab displayed.

vi Configure the following parameters:

- IP Address
- Description
- Administrative State
- Local Address
- Priority Type
- Priority Precedence
- Priority Dscp

vii Click on OK button. The GSMP (Create) form closes.

viii Click on OK button. The GSMP Group (Create) form closes.

53 Perform the following steps to configure a local DHCP server on the VPRN routing instance, if required.

i Click on the Local DHCP Servers tab button.

ii Click on the Add button. The Local DHCP Server (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Server Name
- Description
- Administrative State
- Use GI Address

iv Click on the Select button. The Select Local User Database form opens.

v Select a local user database in the list and click on the OK button. The Select Local User Database form closes and the local user database information is displayed on the Local DHCP Servers (Create) form.

vi Configure the following parameters:

- Allow Send Force Renews
- Use Pool From Client

vii Click on the IP Address Pools tab button to assign one or more IP addresses to the local DHCP server.

viii Click on the Add button. The IP Address Pool (Create) form opens with the General tab displayed.

ix Configure the following parameters:

- Pool Name
- Description

x Configure the parameters in the Minimum Lease Time panel:

- Days
- Hours
- Minutes
- Seconds

xi Configure the parameters in the Maximum Lease Time panel:

- Days
- Hours
- Minutes
- Seconds

xii Configure the parameters in the Offer Time panel:

- Minutes
- Seconds

xiii Click on the Subnets tab button to add subnets to the DHCP server pool.

xiv Click on the Add button. The Subnet (Create) form opens with the General tab displayed.

xv Configure the parameters:

- IP Address
- Prefix Length
- Free Addresses Minimum Threshold
- Maximum Declined Addresses Stored

xvi Click on the Address Ranges tab button.

xvii Click on the Add button. The Subnet Address Range (Create) form opens.

xviii Configure the parameters:

- Action
- Start Address
- End Address

Note — You must exclude static IP addresses from the subnet address range because static IP addresses are dedicated.

xix Click on the OK button. The Subnet Address Range (Create) form closes and a dialog box appears.

xx Click on the OK button. The Subnet (Create) form reappears.

xxi Click on the Options tab button.

xxii Click on the Add button. The Subnet Option (Create) form opens.

xxiii Configure the parameters:

- Option
- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Number parameter is configurable when the Option parameter is set to Custom Option.

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xxiv Click on the OK button. The Subnet Option (Create) form closes and a dialog box appears.

xxv Click on the OK button. The Subnet (Create) form reappears.

xxvi Click on the OK button. The Subnet (Create) form closes and a dialog box appears.

xxvii Click on the OK button. The IP Address Pool (Create) form reappears.

xxviii Click on the Options tab button.

xxix Click on the Add button. The IP Address Pool Option (Create) form opens.

xxx Configure the Option parameter.

xxxi If you set the Option parameter to Custom Option, configure the following parameters:

- Number
- Type
- Value
- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

The Value parameter is configurable when the Type parameter is set to ASCII String or Hex String.

The IP Address 1, IP Address 2, IP Address 3, and IP Address 4 parameters are configurable when the Type parameter is set to IP Address.

xxxii If you set the Option parameter to DNS Name Servers or Netbios Name Server, configure the following parameters:

- IP Address 1
- IP Address 2
- IP Address 3
- IP Address 4

xxxiii If you set the Option parameter to Domain Name, configure the Value parameter.

xxxiv If you set the Option parameter to Lease Time, Lease Renew Time, or Lease Rebind Time, configure the following parameters:

- Days
- Hours
- Minutes
- Seconds

xxxv If you set the Option parameter to Netbios Node Type, configure the Netbios Node Type parameter.

xxxvi Click on the OK button. The IP Address Pool Option (Create) form closes and a dialog box appears.

xxxvii Click on the OK button. The IP Address Pool (Create) form reappears.

xxxviii Click on the OK button. The IP Address Pool (Create) form closes and a dialog box appears.

xxxix Click on the OK button. The Local DHCP Server (Create) form reappears.

xl Click on the OK button. The Local DHCP Server (Create) form closes and a dialog box appears.

xli Click on the OK button. The VPRN Site (Create) form reappears.

54 Click on the Self Generated Traffic tab button. The DSCP Marking tab is displayed with a list of all the applications for which the DSCP can be set.

55 Choose an application to view or edit the DSCP setting.

56 Click on the Properties button. An Application DCSP Marking form opens.

57 Configure the DSCP parameter.

58 Click on the Apply button. A dialog box appears. Click on the OK button.

59 Click on the DSCP Mapping tab. A list of DSCP types and corresponding forwarding classes is displayed.

60 Choose a DSCP to view or edit the forwarding class.

61 Click on the Properties button. An Application DCSP Marking form opens.

62 Configure the Forwarding Class parameter.

63 Click on the Apply button. A dialog box appears. Click on the OK button.

64 Click on the Dot1p Marking tab button. A list of applications for which the Dot1p can be set is displayed.

65 Choose a Dot1p to view or edit the setting.

66 Click on the Properties button. An Application Dot1p Marking form opens.

67 Configure the dot1p parameter.

68 Click on the OK button. A dialog box appears. Click on the OK button.

69 Configure an override source IP address or L3 interface for use by a selected IP application, if required.

i Click on the Source Addresses tab button.

ii Click on the Add button. The Source Address (Create) form opens.

70 Choose an IP application from the Source IP Application drop-down menu.

71 Specify the source address for the IP application server by performing one of the following steps:

Note — If you choose the interface index option, the router used for this VPRN must already have an access interface created for its routing instance.

a Choose IP Address in Source Address Termination to specify the source IP address of the IP application server.

i Enter a valid IP address that the VPRN virtual routing instance will identify in the Source IP Address field.

ii Go to step 72.

Note 1 — An IPv6 address option for the Source IP Address parameter is available when the IPv6 Allowed parameter is set during network interface creation. See chapter 27 for more information about creating a network interface.

Note 2 — You must select an IPv6 Source IP Address before you can select IPv6 Source IP Applications.

b Choose Interface Index in Source Address Termination to use the primary address of the L3 network interface as the source address of the IP application server.

i Click on the Select button to choose an interface. The Select Source Address VPRN Interface - Source Address form opens. Choose an interface from the list and click on the OK button. The IP address and Interface ID of the L3 interface appear on the form.

ii Go to step 72.

72 Click on the OK button. The Source Address (Create) form closes and the Site (Create) form reappears. The IP application source address and parameters appear on the form.

73 Click on the IGMP Host Tracking tab button.

74 Configure the parameters:

- Expiry Time
- Administrative State

75 Click on the Route Aggregation tab button to configure route aggregates for the VPRN service.

Route aggregation allows you to group a number of routes with common IP prefixes into a single entry in the routing table. This reduces the number of routes that need to be advertised by the hosting router and reduces the number of routes in the routing tables of downstream routers.

Note — Route aggregation for VPRN sites is supported on 7450 ESS in mixed mode, 7750 SR and 7710 SR nodes.

i Click on the Add button. The Aggregation (Create) form opens.

ii Configure the parameters:

- IP Address Prefix
- Mask
- Summary Only
- As Set
- Aggregator
- Aggregator AS
- Aggregator IP Address

The IP Address Prefix you enter must be an IPv4 address in the form x.x.x.0, where the last integer is the host bits and must have a value of 0.

The Aggregator AS and Aggregator IP Address parameters are configurable when the Aggregator parameter value is set to True.

76 Click on the OK button. A dialog box appears.

77 Click on the OK button. The Site (Create) form closes, and the VPRN (Create) form reappears with the new site information displayed in the service components tree.

78 Perform one of the following:

a Create an additional site for the VPRN. Go to step 6.

b Go to step 79.

79 Perform one or more of the following.

a Create an L3 access interface for the VPRN site. Perform Procedure 71-2.

b Configure BGP, OSPFv2, OSPFv3, PIM, IGMP, RIP or L2TP in the VPRN routing instance. Perform Procedure 71-3.

c Add a PIM interface to the VPRN. Perform Procedure 71-6.

d Add an IGMP interface to the VPRN. Perform Procedure 71-7.

e Create a VPRN spoke SDP binding. Perform Procedure 71-8.

f Add an IPsec interface on a VPRN. See Procedure 32-6 in chapter 32.

g Add a Video interface to a VPRN site. See Procedure 33-1 in chapter 33.

h Add a subscriber interface to the VPRN. Perform Procedure 71-10.

i Add a group interface to the VPRN. Perform Procedure 71-11.

j Add an IP mirror interface to the VPRN. Perform Procedure 71-12.

k Go to step 80 to complete service creation.

80 Click on the OK button. A dialog box appears.

81 Click on the Yes button to confirm the action. The VPRN (Create) form closes.

Procedure 71-2 To create a VPRN L3 access interface

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Components tab button.

6 Right-click on Access Interfaces in the site components tree and choose Create L3 Access Interface. The L3 Access Interface (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- MAC Address
- Allow Directed Broadcasts
- Loopback Enabled
- Cflowd Type
- Trusted
- Class
- IPv6 Allowed
- Admin Link Local Address
- Admin Link Local Address Preferred
- Calling Station ID
- Configured IP MTU (Octets)
- Unnumbered Type
- IP Address
- Interface Name

The Unnumbered Type parameter is configurable when the Class parameter is set to Unnumbered.

The IP Address parameter is configurable when the Unnumbered Type parameter is set to IP Address.

The Interface Name parameter is configurable when the Unnumbered Type parameter is set to Name.

The Admin Link Local Address and Admin Link Local Address Preferred parameters are only configurable when the IPv6 Allowed parameter is enabled.

8 If the Loopback Enabled parameter in step 7 is enabled, you cannot associate a port with the L3 interface. Go to step 16.

9 Click on the Select button beside the Application Profile parameter. The Application Profile String: - VPRN L3 Access Interface list form opens.

10 Select a profile from the list and click on the OK button. The Application Profile String - VPRN L3 Access Interface list form closes and the L3 Access Interface (Create) form is refreshed with the Application Profile information.

Note — The Application Profile String: - VPRN L3 Access Interface list form only displays local profiles that already exist on the NE.

11 Click on the Port tab button.

12 Click on the Select button to choose a port for the L3 access interface. The Select Terminating Port - VPRN L3 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

13 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPRN L3 Access Interface form closes, and the VPRN L3 Access Interface (Create) form displays the port information.

14 Configure the parameters:

- Auto-Assign ID
- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

The Auto-Assign ID parameter is configurable if the port uses Dot1 Q encapsulation. When the parameter is enabled, the 5620 SAM automatically configures the Outer Encapsulation Value parameter using the lowest unassigned value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

15 If the selected port uses FR encapsulation, configure Frame Relay for the interface.

i Click on the Frame Relay tab button.

ii Set the FRF-12 Mode parameter to Enabled.

iii Configure the parameters:

- FRF-12 End-To-End Fragment Threshold
- Scheduling Class
- Fragment Interleave

Note — If a bundle is selected in step 13, only the Scheduling Class parameter is configurable.

16 Assign ingress and egress QoS policies to the interface, if required.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once by selecting and right-clicking the components in the service components tree, choosing Properties, and configuring the parameters on the appropriate tab.

i Click on the QoS tab button.

Note — The QoS tab is configurable only if a port is assigned to the interface.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use Shared Queue
- Use Multipoint Shared Queue
- HSMDA Packet Byte Offset (bytes)

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is BCP Dot1 Q, Dot1 Q, or QinQ.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - L3 Access Interface form opens.

iv Use the configurable filter and Search button to choose a policy, and click on the OK button. The Select Ingress Policy - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the ingress QoS policy information displayed.

Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you selected in step 13 has the access ingress queue group with the same name created on it.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - L3 Access Interface form opens.

vi Use the configurable filter and Search button to choose a QoS policy, and click on the OK button. The Select Egress Policy - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the egress QoS policy information displayed.

Note — If you select an egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you selected in step 13 has the access egress queue group with the same name created on it.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

vii Click on the Select button in the HSMDA Egress Secondary Shaper panel to choose an HSMDA egress secondary shaper policy. The Select HSMDA Egress Secondary Shaper form opens.

viii Select a secondary shaper and click on the OK button. The Select HSMDA Egress Secondary Shaper form closes and the L2 Access Interface (Create) form reappears with the egress secondary shaper information displayed.

ix Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

x Select a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the L2 Access Interface (Create) form reappears with the ingress policer control policy information displayed.

xi Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

xii Select a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the L2 Access Interface (Create) form reappears with the egress policer control policy information displayed.

17 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 19.

Note — The Schedulers tab is configurable only if a port is assigned to the SAP earlier in the procedure.

18 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the interface.

i Set the Aggregation parameter to off.

ii Configure the parameters:

- Egress Aggregate Rate Limit (kbps)
- Frame Base Accounting

Note 1 — The Egress Aggregate Rate Limit (kbps) and Frame Base Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — You cannot specify an egress scheduler when the Egress Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - L3 Access Interface form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - L3 Access Interface form closes, and the L3 Access Interface (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - L3 Access Interface form opens.

vi Select an egress scheduler and click on the OK button. The Select Egress Scheduler - L3 Access Interface form closes, and the L3 Access Interface (Create) form refreshes with the egress scheduler information displayed.

vii Go to step 19.

b Specify that an aggregation scheduler policy is applied to the interface.

i Set the Aggregation parameter to on.

ii Configure the Frame Base Accounting parameter.

iii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - L3 Access Interface form opens.

iv Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - L3 Access Interface form closes, and the L3 Access Interface (Create) form refreshes with the aggregation scheduler information displayed.

19 Assign ingress and egress ACL filters to the interface, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress IPv4 ACL filter. The Select Ingress Filter - L3 Access Interface form opens.

iii Select an ingress ACL filter and click on the OK button. The Select Ingress Filter - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the ingress IPv4 ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress IPv4 ACL filter. The Select Egress Filter - L3 Access Interface form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the egress IPv4 ACL filter information displayed.

vi If the L3 Access Interface supports IPv6 addressing, perform the following substeps. Otherwise, go to step 21.

vii Click on the Select button in the IPv6 Ingress Filter panel to choose an ingress IPv6 ACL filter. The Select IPv6 Ingress Filter - L3 Access Interface form opens.

viii Select an ingress ACL filter and click on the OK button. The Select IPv6 Ingress Filter - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the ingress IPv6 ACL filter information displayed.

ix Click on the Select button in the IPv6 Egress Filter panel to choose an egress IPv6 ACL filter. The Select IPv6 Egress Filter - L3 Access Interface form opens.

x Select an egress ACL filter and click on the OK button. The Select IPv6 Egress Filter - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the egress IPv6 ACL filter information displayed.

20 Bind a VPRN L3 access interface to a VPLS site, if required.

Note 1 — The operational state of the IP interface binding will not be turned up until the Enable IP Interface Binding parameter is set to true.

Note 2 — You can create and manage a routed VPLS connector from the Components tab on the Composite Service (Edit) form.

i Click on the Routed VPLS tab button.

ii Enter a VPLS site name or click on the Select button next to the VPLS Name parameter to choose a VPLS site. The Routed VPLS String - VPRN L3 Access Interface form opens.

iii Select a VPLS site and click on the OK button. The VPLS site is displayed.

iv In the Ingress - IPv4 Filter panel, click on the Select button. The Select IPv4 Filter - VPRN L3 Access Interface form opens.

v Select an IPv4 filter and click on the OK button. The IPv4 filter information is displayed.

vi In the Ingress - IPv6 Filter panel, click on the Select button. The Select IPv6 Filter - VPRN L3 Access Interface form opens.

vii Select an IPv6 filter and click on the OK button. The IPv6 filter information is displayed.

viii In the Egress - QoS Policy panel, click on the Select button. The Select QoS Policy - VPRN L3 Access Interface form opens.

ix Select a QoS Policy and click on the the OK button. The QoS Policy information is displayed.

21 Assign an accounting policy to the interface, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - L3 Access Interface form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - L3 Access Interface form closes and the L3 Access Interface (Create) form reappears with the accounting policy information displayed.

22 Associate a local DHCP server to the L3 interface, if required.

i Click on the Local DHCP Servers tab button

ii Click on the Select button in the Local DHCP Server panel to choose a local DHCP server. The Select Local DHCP Server - L3 Access Interface form opens.

iii Select a local DHCP server and click on the OK button. The Select Local DHCP Server - L3 Access Interface form closes, and the L3 Access Interface (Create) form reappears with the local DHCP server information displayed.

Note — You cannot associate a local DHCP server to the L3 group Interface if the Administrative State parameter in the Local Proxy Service panel is up. Go to step 7 to set the Administrative State.

23 Assign a time of day suite to the interface, if required.

i Click on the TOD Suite tab button.

ii Click on the Select button beside the Name parameter. The Select Time Of Day Suite - L3 Access Interface list form opens.

iii Select a time of day suite and click on the OK button. The Select Time Of Day Suite - L3 Access Interface list form closes, and the L3 Access Interface (Create) form refreshes with the time of day suite name.

Note 1 — You cannot assign a ToD suite to a L3 access interface if accounting statistics collection is enabled on the interface. You must first disable the Collect Accounting Statistics parameter in step 21.

Note 2 — SapEgrQosPlcyStats and SapIngQosPlcyStats statistics will only be collected if a Time Of Day Suite is applied on the SAP.

24 Configure residential subscriber management for the interface, if required. Residential subscriber management is supported on the 7450 ESS in mixed mode, 7750 SR, and 7710 SR.

i Click on the Subscriber Management tab button. The Host Connectivity tab is displayed.

ii Select the SHCV Enabled parameter to enable SHCV, if required. Otherwise, go to step 26.

iii Configure the parameters:

- SHCV Interval (minutes)
- SHCV Source
- SHCV Action

25 Assign a DoS protection policy to the interface, if required.

Note — A default DoS protection policy is automatically assigned to the interface.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - L3 Access Interface form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - L3 Access Interface form closes and the policy ID is displayed on the L3 Access Interface (Create) form.

26 Assign an IP address to the interface.

i Click on the Address tab button.

ii Click on the Add button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Broadcast Address Format
- EUI-64
- IP Address Preferred

The Broadcast Address Format parameter only appears if the IP Address parameter is set to an IPv4 address.

The EUI-64 and IP Address Preferred parameters only appear if the IP Address parameter is set to an IPv6 address.

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The L3 Access Interface (Create) form reappears with the assigned IP addresses displayed.

27 Configure IPv4 ICMP for the interface, if required.

i Click on the ICMP tab button.

ii Configure the parameters:

- Mask Reply
- Redirects
- Number of Redirects
- Redirects Time (seconds)
- Unreachables
- Number of Unreachables
- Unreachables Time (seconds)
- TTL Expired
- Number of TTL Expired
- TTL Expired Time (seconds)

28 If the IPv6 Allowed parameter in step 7 is enabled, the ICMPv6 tab is configurable. Configure IPv6 ICMP, if required. Otherwise, go to step 29.

Configure the parameters:

- Redirects
- Number of Redirects
- Redirects Time (seconds)
- Unreachables
- Number of Unreachables
- Unreachables Time (seconds)
- Packet Too Big
- Number of Packet Too Big
- Packet Too Big Time (seconds)
- Param Problem
- Number of Param Problem
- Param Problem Time (seconds)
- Time Exceeded
- Number of Time Exceeded
- Time Exceeded Time (seconds)

29 Configure IPCP for the interface, if required. IPCP is available only on the ASAP MDA on the 7750 SR and 7710 SR.

i Click on the IPCP tab button.

ii Configure the parameters:

- Peer Address
- Primary DNS Address
- Secondary DNS Address

Note — Primary and secondary DNS addresses have similar functionality however they are assigned independently. When both are present, the primary DNS address is used to resolve address names. If the primary DNS address cannot be used the secondary DNS address is used.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button to confirm the action.

The IPCP tab is available when the SAP and port is configured with Null or IPCP encapsulation.

30 Configure Bi-directional Forwarding Detection for the interface, if required.

i Click on the BFD tab button.

ii Click on the Configuration tab button.

iii Configure the parameters:

- Administrative Status
- Transmit Interval
- Receive interval
- Echo Interval
- Multiplier

The Transmit Interval, Receive interval, Receive interval, Echo Interval, and Multiplier parameters are configurable only when the Administrative Status is set to Up.

iv To view local and remote session peers that are managed by the 5620 SAM. Click on the BFD Session tab button. A list of BFD current sessions on a router interface or an L3 interface appears.

v Click on a session. The properties form for the session opens. View the following:

- BFD status
- protocol used
- local address
- remote address
- operational status and statistics

vi Close the form.

Note — You cannot configure BFD for an interface if BFD is disabled. See chapter 28 for information about enabling and disabling BFD for routing protocols.

31 Configure ARP for the interface, if required.

i Click on the ARP tab button. The General tab is displayed.

ii Configure the Timeout (seconds) parameter.

iii Click on the Proxy ARP tab button.

iv Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1
- Proxy ARP Policy 2
- Proxy ARP Policy 3
- Proxy ARP Policy 4
- Proxy ARP Policy 5

32 If the IPv6 Allowed parameter in step 7 is enabled, the Neighbor Discovery tab is configurable. Configure neighbor discovery, if required. Otherwise, go to step 33.

i Click on the Neighbor Discovery tab button.

ii Click on the Add button. The Neighbor Discovery (Create) form opens.

iii Configure the parameters:

- IP Address
- Physical Address

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The Neighbor Discovery (Create) form closes, and the L3 Access Interface (Create) form refreshes with the neighbor entry.

vi Click on the Proxy ND tab button.

vii Configure the parameters:

- Enable Local Proxy
- Policy 1
- Policy 2
- Policy 3
- Policy 4
- Policy 5

Note — Do not leave an empty policy parameter between two configured policy parameters. For example, do not configure the Policy 1 and Policy 3 parameters and leave the Policy 2 parameter unconfigured, or the 5620 SAM reorders the policies and move the policy specified for the Policy 3 parameter to the Policy 2 parameter.

viii Repeat steps i to vii for each neighbor entry you want to create.

33 Configure IPv4 DHCP for the interface, if required.

i Click on the DHCP tab button. The General tab is displayed.

ii Configure the parameters:

- Enable DHCP Relay
- Description
- Trusted
- Lease Populate
- Enable
- Relay Plain BOOTP
- Use ARP

The Lease Populate parameter is configurable when the Enable parameter is enabled.

iii Depending on the type and version of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step viii.

iv Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form opens.

v Click on the Search button.

vi Select a subscriber authentication policy and click on the OK button. The Select Subscriber Authentication Policy - DhcpRelayConfiguration form closes, and the L3 Access Interface (Create) form refreshes with the subscriber authentication policy name.

vii Configure the parameters:

- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP Address
- Use as source

The Remote ID String parameter is configurable when the Remote ID is set to Remote ID String.

viii Click on the Server tab button.

ix Configure the parameters:

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time RADIUS Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

34 The ATM tab is configurable when the interface port is an ATM port. Specify OAM functionality and assign ingress and egress ATM policies to the interface, if required.

i Click on the ATM tab button.

ii Configure the parameters:

- AAL5 Encapsulation
- ATM OAM Alarm Cell Handling
- Periodic ATM OAM Loopback

iii Click on the Select button in the Ingress ATM Policy panel to choose an ingress ATM policy. The Select Ingress ATM Policy - ATM Configuration form opens.

iv Select an ingress ATM policy and click on the OK button. The Select Ingress ATM Policy - ATM Configuration form closes and the L3 Access Interface form reappears with the ingress ATM policy information displayed.

v Click on the Select button in the Egress ATM Policy panel to choose an egress ATM policy. The Select Egress ATM Policy - ATM Configuration form opens.

vi Select an egress ATM policy and click on the OK button. The Select Egress ATM Policy - ATM Configuration form closes and the L3 Access Interface (Create) form reappears with the egress ATM policy information displayed.

35 Click on the VRRP tab button to create a VRRP instance on the current L3 interface for a virtual router. You must know the VRID for an existing virtual router and ensure that the interface is a member of the same subnet as the virtual router.

Note — The following configurations are required for the operation of the IPv6 VRRP instance:

- Two sub-tabs are available under the VRRP tab, one for IPv4 instances and the other for IPv6 instances. You can only create an IPv6 VRRP Instance if you enable the IPv6 Allowed parameter in step 7.
- The Link Local Address on the parent interface has to be set to preferred and configured as one of the backup addresses (or same subnet) for the IPv6 VRRP instance. To do this, the Admin Link Local Address and Admin Link Local Address Preferred parameters in step 7 must be set accordingly.
- The IPv6 address on the parent interface must be set to preferred to be used as a backup address (on same subnet) for the IPv6 VRRP instance. The IP Address and IP Address Preferred parameters in step 26 must be set accordingly.
- The Send Advertisement and Use Virtual MAC Address parameters must be enabled in step 37 for the router advertisement on the parent interface.

See chapter 36 for configuration information about VRRP instances and virtual routers.

i Click on the Add button. The VRRP Instance (Create) form opens with the General tab displayed.

ii Configure the Virtual Router Id parameter.

iii Perform steps 8 to 14 of Procedure 36-2.

Note — You can use the VR Instances tab to create, modify, and view VR instances.

iv Click on the OK button. The VRRP Instance (Create) closes and the L3 Access Interface (Create) form reappears.

36 Configure anti-spoofing filters for the interface, if required.

i Click on the Anti-Spoofing tab button.

ii Configure the parameters:

- Anti-Spoofing
- ARP Populate

The ARP Populate parameter is configurable when all of the IP addresses of the defined static hosts on the interface are in one of the subnets configured for the interface.

iii Click on the Static Hosts tab button to configure static subscriber host entries, if subscriber entries are not available through DHCP lease management. Otherwise, go to step 42.

iv Click on the Add button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

v Configure the parameters:

- IP Address
- MAC Address

Specify at least one IP address or MAC address for each static host. The values specified for the Anti-Spoofing and ARP Populate parameters determine the type of address entry that is required for the static host. For example, when you set the Anti-Spoofing parameter to Source Ip Addr, you must specify at least the IP address for the static host.

Note — You can configure a static host on a SAP only when no static ARP entries exist on the IP interface.

When the ARP Populate parameter is enabled, the IP address of the new static host must be in one of the subnets that is configured for the interface in step 26.

vi Click on the Apply button if you want to create additional entries. A dialog box appears. Otherwise, go to step ix.

vii Click on the OK button.

viii Repeat steps v to vii to create additional entries, if required.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes and the Static Hosts tab refreshes with the configured static hosts displayed.

37 Configure router advertisement, if required.

i Click on the Advertisement tab button.

ii Click on the Add button to add a router advertisement entry. The Router Advertisement (Create) form opens.

iii Configure the parameters:

- Send Advertisement
- Min Interval (seconds)
- Reachable Time (milliseconds)
- Managed Address Config
- MTU
- Use Virtual MAC Address
- Max Interval (seconds)
- Retransmit Time (milliseconds)
- Other Stateful Config
- Current Hop Limit
- Lifetime (seconds)

If you are configuring the L3 interface for an IPv6 VRRP instance, then the Send Advertisement and Use Virtual MAC Address parameters must both be enabled.

iv Click on the Prefix tab button.

v Click on the Add button. The Router Advertisement Prefix (Create) form opens.

vi Configure the parameters:

- IPv6 Prefix
- On-Link Determination
- Prefix Length
- Autonomous Address Configuration
- Lifetime (seconds) in Preferred Lifetime panel
- No Expiry in Preferred Lifetime panel
- Lifetime (seconds) in Valid Lifetime panel
- No Expiry in Valid Lifetime panel

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Router Advertisement (Create) form reappears.

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Router Advertisement (Create) form closes and the L3 Access Interface (Create) form refreshes with the router advertisement entry.

38 Assign an ANCP policy to the interface, if required.

i Click on the ANCP Static Map tab button.

ii Click on the Add button. The ANCP Static Map (Create) form opens with the General tab displayed.

iii Configure the ANCP String parameter.

iv Click on the Select button in the ANCP Policy panel to choose an ANCP policy. The Select ANCP Policy - ANCP Static Map list form opens.

v Select an ANCP policy and click on the OK button. The Select ANCP Policy - ANCP Static Map form closes and the ANCP Static Map form reappears with the ANCP policy information displayed.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The ANCP Static Map (Create) form closes.

39 Specify queue overrides by clicking on the Override tab button. See Procedure 44-40 for information about how to set queue overrides.

Note — The Override tab contains four sub-tabs: Access Ingress Queue, Access Egress Queue, Access Ingress HSMDA Queue, and Access Egress HSMDA Queue. However, only two of the four are active, depending on the port type you have chosen for this interface.

If you have configured an HSMDA port, then the Access Ingress HSMDA Queue and Access Egress HSMDA Queue sub-tabs are active. If you have configured a non-HSMDA port, then the Access Ingress Queue and Access Egress Queue sub-tabs are active.

40 If the IPv6 Allowed parameter in step 7 is enabled, the DHCPv6 tab is configurable. Configure IPv6 DHCP, if required. Otherwise, go to step 41.

i Click on the DHCPv6 tab button. The General tab is displayed.

ii Configure the parameters:

- Enable DHCPv6 Relay
- Description
- Lease Populate
- Maximum Number of Leases
- Interface Id Option
- Interface Id String
- Remote ID
- Source IP Address
- Neighbor Resolution
- Prefix Option

iii Click on the Server tab button.

iv Configure the Server 1 through Server 8 parameters.

v Configure the interface name for each DHCPv6 server that you configured in step iv by clicking on the Select button in the Zone Index panel. The Select Zone Index - DhcpRelayV6Configuration form opens with a list of configured interfaces.

vi Select an interface from the list and click on the OK button. The Select Zone Index - DhcpRelayV6Configuration list form closes and the L3 Access Interface form refreshes with the interface information.

vii Click on the DHCPv6-Prefix tab button.

viii Click on the Add button. The DhcpRelayV6PrefixDelegation (Create) form opens.

ix Configure the parameters:

- Prefix Address
- Prefix Length
- Prefix DUID
- Prefix IAID
- Prefix Life Time (seconds)
- Prefix Valid Life Time (seconds)

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The L3 Access Interface (Create) form reappears.

41 Configure Unicast RPF if required.

i Click on the Unicast RPF tab button.

ii Configure the parameters:

- URPF Check State
- URPF Check Mode

42 Click on the OK button. A dialog box appears.

43 Click on the OK button. The L3 Access Interface (Create) form closes, and the Site (Create) form reappears with the new interface information displayed in the service components tree.

Repeat steps 6 to 43 to create another L3 access interface for the site in the VPRN service.

Note — If you are creating the L3 access interface during service creation, return to Procedure 71-1.

Procedure 71-3 To configure BGP, OSPFv2, OSPFv3, PIM, RIP, or L2TP on a VPRN routing instance

Note — To configure IGMP on a VPRN routing instance, see Procedure 71-4.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Components tab button.

6 Expand the Routing Instance icon.

7 Right-click on the Protocols icon and perform one of the following from the contextual menu:

a Choose Create BGP Site to configure BGP on the VPRN routing instance, and then perform steps 4 to 30 of Procedure 28-2.

b Choose Create OSPF Site to configure OSPFv2 on the VPRN routing instance, and then perform steps 5 to 19 of Procedure 28-11.

c Choose Create OSPF Site to configure OSPFv3 on the VPRN routing instance, and then perform steps 5 to 11 and steps 13 to 19 in Procedure 28-11.

d Choose Create PIM Site to configure PIM on the VPRN routing instance, and then perform steps 4 to 77 in Procedure 28-32.

e Choose Create RIP Site to configure RIP on the VPRN routing instance, and then perform steps 4 to 15 in Procedure 28-7.

f Choose Create L2TP Site to configure L2TP on the VPRN routing instance, and then perform steps 3 to 18 in Procedure 28-29.

8 Click on the OK button. The protocol configuration form closes, and a dialog box appears.

9 Click on the OK button. The VPRN (Edit) form reappears.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button to confirm the action. The VPRN (Edit) form closes.

12 Close the Manage Services form.

Procedure 71-4 To configure IGMP on a VPRN routing instance

Note — PIM-SSM for IPv6 is currently not supported in VPRN services.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Components tab button.

6 Expand the Routing Instance icon.

7 Right-click on the Protocols icon and choose Create IGMP Site from the contextual menu. The IGMP Site (Edit) form opens with the General tab displayed.

8 Configure the parameters:

- Administrative State
- Query Interval (seconds)
- Last Member Query Interval (seconds)
- Query Response Interval (seconds)
- Robust Count

9 Click on the SSM Translation tab button to configure SSM, if required.

i Click on the Add button to create a new entry. The SSM Translation (Create) form opens.

ii Configure the parameters:

- Start Mcast Address
- End Mcast Address
- Configured Source

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The new SSM entry appears on the form.

10 Click on the Interfaces tab button to add an interface, if required.

i Click on the Add button.

ii Perform steps 4 to 14 of Procedure 28-38.

iii Click on the OK button. The new interface entry appears on the form.

11 Click on the Group Interfaces tab button to identify an IGMP group interface for a VPRN service, if required.

12 Click on the Add button and configure the parameters in the IGMP Group Interface - Routing Instance (Create) form:

- Description
- Administrative State
- Forwarding Service ID
- Name

13 Click on the OK button. The Group Interfaces tab reappears.

14 Click on the Select button next to the Interface ID field to select a group interface from the Select IGMP Group Interface - IGMP Group Interface - Routing Instance form.

15 Click on the following tab buttons to view and edit information.

- Multicast Group/Source
- Statistics
- Faults

16 Click on the OK button. The protocol configuration form closes, and a dialog box appears.

17 Click on the OK button. The VPRN (Edit) form reappears.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button to confirm the action. The VPRN (Edit) form closes.

20 Close the Manage Services form.

Procedure 71-5 To add a Global Route Table to a VPRN site

Packets within a VRF are able to perform a parallel lookup against a Global Route Table (GRT), as well as within the local VRF table. A successful routing table match found in the local VRF is typically preferred over any match found in the GRT. However, a static route can be used to allow for specific prefixes covered by the static route to fail the lookup in the local VRF table, thus resulting in the guaranteed use of a route from the GRT.

The GRT is populated by defining export policies for each participating VPRN service, and the maximum number of routes that are exported from a specific VRF can be limited.

Note — Only Release 8.0 or later of the 7710 SR and 7750 SR, and the 7450 ESS in mixed mode, support the addition of a GRT to a VPRN service.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose the required VPRN service and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on the routing instance to which you want to add the GRT and select Properties. The VPRN Site (Edit) form opens, with the General tab displayed.

6 Click on the Routing tab.

7 Configure the Enable GRT Lookup parameter in the General sub-tab.

8 Click on the GRT Export Policies sub-tab.

9 Configure the Max Number of Exported Policies parameter.

10 Specify up to five export policies by using the Select button to choose policies from the filtered list and then clicking on the OK button.

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The VPRN Site (Edit) form closes and a dialog box appears.

13 Click on the OK button. The VPRN Service (Edit) form closes.

14 Close the Manage Services form.

Procedure 71-6 To add a PIM interface to a VPRN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Components tab button.

6 Expand the Routing Instance icon.

7 Expand the Protocols icon.

8 Right-click on a PIM instance in the service components tree and choose Create PIM Interface. The PIM Interface, Routing Instance (Create) form opens.

9 Assign an L3 access interface to the PIM interface by clicking on the Select button in the Interface panel. The Select Interface - PIM Interface form opens.

10 Configure the filter criteria. A list of available L3 access interfaces appears at the bottom of the Select Interface - PIM Interface form.

11 Select an interface and click on the OK button. The Select Interface - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the L3 access interface information.

12 Configure the parameters:

- Description
- Administrative State
- BFD Enabled

13 Click on the Behavior tab button.

14 Configure the parameters:

- Hello Interval (seconds)
- Tracking Support
- BSM Check Router Alert
- Improved assert
- Max Groups
- Three Way Hello
- Multicast Senders
- Hello Multiplier
- Assert Period
- DR Priority
- Sticky DR
- Operational DR Priority

The Operational DR Priority parameter is configurable when the Sticky DR parameter is enabled.

15 Click on the Multicast CAC tab button to add a multicast CAC policy, if required. The General tab is displayed.

16 Click on the Select button in the Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - PIM Interface form opens.

17 Choose a multicast CAC policy from the list and click on the OK button. The Select Multicast CAC Policy - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the multicast CAC policy information.

18 Configure the parameters:

- Unconstrained Bandwidth
- Mandatory Bandwidth
- Constraint Admin State

19 Click on the OK button. A dialog box appears.

20 Click on the OK button.

21 Click on the OK button to close the VPRN (Edit) form. A dialog box appears.

22 Click on the Yes button to confirm the action. The VPRN (Edit) form closes.

23 Click on the Close button to close the Manage Services form.

Procedure 71-7 To add an IGMP interface to a VPRN

Note — IGMP must be enabled at the routing instance level before you can create an IGMP interface.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on an IGMP instance in the service components tree and choose Create IGMP Interface. The IGMP interface, Routing Instance (Create) form opens with the General tab displayed.

6 Assign an L3 access interface to the PIM interface by clicking on the Select button in the Interface panel. The Select Interface - PIM Interface form opens.

7 Configure the filter criteria. A list of available L3 access interfaces appears at the bottom of the Select Interface - PIM Interface form.

8 Select an interface and click on the OK button. The Select Interface - PIM Interface form closes and the PIM Interface, Routing Instance (Create) form refreshes with the L3 access interface information.

9 Configure the parameters:

- Description
- Administrative State
- Administrative Version
- Maximum Number of Groups
- Subnet Check

10 Click on the Behavior tab button to add an import policy, if required.

11 Click on the Select button in the Properties panel to choose an import policy. The Select - IGMP Interface form opens.

12 Configure the filter criteria. A list of import policies appears at the bottom of the Select - IGMP Interface form.

13 Choose an import policy from the list and click on the OK button. The Select - IGMP Interface form closes and the IGMP Interface, Routing Instance (Create) form reappears.

14 Click on the Multicast CAC tab button to add a multicast CAC policy, if required.

15 Click on the Select button in the Multicast CAC Policy panel to choose a multicast CAC policy. The Select Multicast CAC Policy - IGMP Interface form opens.

16 Choose a multicast CAC policy from the list and click on the OK button. The Select Multicast CAC Policy - IGMP Interface form closes and the IGMP Interface, Routing Instance (Create) form refreshes with the multicast CAC policy information.

17 Configure the parameters:

- Unconstrained Bandwidth
- Mandatory Bandwidth
- Constraint Admin State

18 Click on the Static Group/Source tab button to add a static multicast group or source, if required.

19 Click on the Add button to add a new entry. The StaticGrpSrc, Routing Instance (Create) form opens.

20 Configure the parameters:

- Static Multicast Group
- Static Source

21 Click on the OK button. The StaticGrpSrc, Routing Instance (Create) form closes and a dialog box appears.

22 Click on the OK button to confirm the action.

23 Click on the OK button to close the IGMP Interface, Routing Instance (Create) form. A dialogue box opens.

24 Click on the OK button to confirm the action. The VPRN (Edit) form reappears.

25 Click on the OK button to close the VPRN (Edit) form. A dialog box appears.

26 Click on the Yes button to confirm the action. The VPRN (Edit) form closes and the Manage Services form reappears.

27 Close the Manage Services form.

Procedure 71-8 To create a VPRN spoke SDP binding

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN (Edit) form opens.

4 Click on the Components tab button.

5 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding from the contextual menu. The Spoke SDP Binding (Create) form opens with the General tab displayed.

6 Specify a source interface for the SDP binding:

i Click on the Select button in the Source Interface panel. The Select Source Interface - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of interfaces appears at the bottom of the form.

iii Select an entry and click on the OK button. The Select Source Interface - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the source interface information.

iv Configure the parameters:

- VC ID
- Auto-Assign ID
- VC Type
- Enable Hash Label

The Enable Hash Label parameter can only be configured for spoke-SDP bindings that are access interface terminated.

7 Specify a destination node for the spoke SDP binding:

a If the destination node is a managed node, choose from a list of managed nodes.

i Click on the Select button beside the Tunnel Termination Site parameter. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Select a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify its system ID in the Tunnel Termination Site parameter.

8 Configure the Description parameter.

9 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

10 Specify an application profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of application profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding - VPRN service form displays only local profiles on the NE.

11 Perform one of the following to specify a transport tunnel for the Return SDP binding, if required.

Note — You can create a return tunnel only between sites that are within the same service. If the sites are not in the same service, the Return tab does not appear.

a Let the 5620 SAM configure the transport tunnel automatically.

i Click on the Return tab.

ii Enable the Auto Select Return Transport Tunnel parameter.

iii Configure either the Profile Name or the Return Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Return tab.

ii Click on the Select button in the Return Tunnel panel. The Select Return Tunnel - Spoke SDP Binding form opens.

iii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Return Tunnel - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the service Tunnel ID, Name, and Underlying Transport displayed in the Tunnel panel.

12 Click on the States tab button.

13 Configure the Administrative State parameter.

14 Associate a MEP to the spoke SDP binding, if required.

i Click on the MEPs tab button.

ii Click on the Add button. The MEP (Create) form opens with the General tab displayed.

iii Click on the Select button to choose a MEG. The Select Maintenance Entity Group form opens.

iv Select an entry and click on the OK button. The Select Maintenance Entity Group form closes.

v Configure the parameters:

- Auto-Assign ID
- ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- MAC Address
- Fault Propagation
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

15 If the MD for the MEP has a Name Type of none and the associated MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable; click on the Y.1731 Tests tab button. Otherwise, go to step 19.

16 Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

17 Click on the AIS tab button.

18 Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

19 Click on the OK button. A dialog box appears.

20 Click on the OK button. The MEP (Create) form closes.

21 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

22 Click on the OK button.

Procedure 71-9 To create an L2 SDP spoke termination on a VPRN service

Ensure that a service and site have been created in the VPRN. To terminate an L2 service on a VPRN SDP spoke, you must identify the VC and an interface belonging to the VC. The interface must not have an associated port.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN (Edit) form opens.

4 Click on the Components tab button.

5 Right-click on Spoke SDP Bindings and choose Create Spoke SDP Binding. The Spoke SDP Binding (Create) form opens with the General tab displayed.

6 Click on the Select button in the Source Interface panel to select an interface with no port assigned.

If you are creating this spoke SDP binding for use with an IP mirror interface, select the required IP mirror interface as the source interface.

7 Click on the OK button. The Select Interface - Spoke SDP Bindings form closes and the Spoke SDP Bindings (Create) form reappears with the interface information displayed.

8 Specify a destination node for the spoke SDP binding by performing one of the following tasks.

a If the destination node is a managed node, choose from the list of managed nodes.

i Click on the Select button in the Tunnel Termination Site panel. The Select Destination Network Element - Spoke SDP Binding form opens.

ii Choose a destination node and click on the OK button. The Select Destination Network Element - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form refreshes with the tunnel termination site (the destination node) identifier displayed.

b If the destination node is an unmanaged node, specify the system ID for the Tunnel Termination Site parameter.

c If you are configuring IP mirroring, select a mirror source site as the tunnel termination site.

9 Configure the parameters:

- Auto-Assign ID
- VC ID
- VC Type
- Ingress Label
- Egress Label
- Enable Hash Label

If you are configuring IP mirroring, set the VC ID parameter to the mirror service ID.

10 Perform one of the following to specify a transport tunnel for the spoke SDP binding.

a Let the 5620 SAM configure the transport tunnel automatically.

i Enable the Auto Select Transport Tunnel parameter.

ii Configure either the Profile Name or the Tunnel Auto-Selection Transport Preference parameter.

b Configure the transport tunnel manually.

i Click on the Select button in the Tunnel panel. The Select Tunnel - Spoke SDP Binding form opens.

ii Select a service tunnel for the spoke SDP binding and click on the OK button. The Select Tunnel - Spoke SDP Binding form closes, and the Spoke SDP Binding (Create) form refreshes with the service tunnel identifier.

11 Select an Application Profile for the spoke SDP binding.

i Click on the Select button next to the Application Profile parameter. The Application Profile String: - Spoke SDP Binding form opens.

ii Configure the filter criteria. A list of Application Profiles appears.

iii Choose an application profile from the list and click on the OK button. The Application Profile String: - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form appears.

Note — The Application Profile String: - Spoke SDP Binding - VPRN service form displays only local profiles on the NE.

12 Click on the States tab button.

13 Configure the Administrative State parameter.

14 Assign ingress and egress ACL filters to the spoke SDP binding, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter. The Select Ingress Filter - Spoke SDP Binding form opens.

iii Select an ingress ACL filter. If you are configuring IP mirroring, you can optionally select an ingress IP filter. This is a packet mirroring option which specifies that packets matching the IP filter are mirrored to the mirror destination. Click on the OK button. The Select Ingress Filter - Spoke SDP Binding form closes and the Spoke SDP Binding (Create) form reappears with the ingress ACL filter information displayed.

iv Click on the Select button in the Egress Filter panel to choose an egress ACL filter. The Select Egress Filter - Spoke SDP Binding form opens.

v Select an egress ACL filter and click on the OK button. The Select Egress Filter - Spoke SDP Binding form closes and the L3 Access Interface (Create) form reappears with the egress ACL filter information displayed.

15 If you are configuring IP mirroring, go to step 17.

16 Assign an accounting policy to the spoke SDP binding, if required.

i Click on the Accounting tab button.

ii Configure the Collect Accounting Statistics parameter.

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy - Spoke SDP Binding form opens.

iv Select an accounting policy and click on the OK button. The Select Accounting Policy - Spoke SDP Binding form closes and the L3 Access Interface (Create) form reappears with the accounting policy information displayed.

17 Click on the OK button. The Spoke SDP Binding (Create) form closes and a dialog box appears.

18 Click on the OK button. The VPRN (Edit) form reappears with the new information displayed in the service components tree.

Procedure 71-10 To add a subscriber interface to a VPRN

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a subscriber interface in a VPRN.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and click on the Sreach button. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN Service Subscriber (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on the Subscriber Interfaces icon below the site to which you want to add the subscriber interface, and choose Create VPRN Subscriber Interface. The VPRN Subscriber Interface (Create) form opens with the General tab displayed.

6 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Default Primary DNS Server Address
- Default Secondary DNS Server Address

Note 1 — The Name value for a subscriber interface must be unique in the context on the VPRN Service Site. That is, there cannot be another L3 access interface, subscriber interface, or group interface with the same name on the same VPRN site.

Note 2 — You must configure the Default Primary DNS Server Address parameter before you can configure the Default Secondary DNS Server Address parameter.

7 Configure IPv6 forwarding on the subscriber interface, if required.

i Configure the IPv6 Allowed and IPv6 Delegated Prefix Length parameters.

ii Click on the IPv6 Subscriber Prefixes tab button.

iii Select a subscriber prefix from the list and click on the Properties button, or click on the Add button to create a new subscriber prefix.

iv In the Subscriber Prefix [Edit|Create] form, configure the parameters:

- Address ID
- IP Address
- Prefix Length
- WAN Host
- Prefix Delegation

8 Perform one of the following:

a Create a subscriber interface for a wholesale and retail VPRN.

When you configure the routing instance for the VPRN, you can set the Type parameter to Subscriber Split Horizon to enable the forwarding service and forwarding subscriber information. The subscriber split horizon VPRN controls the flow of traffic for wholesale subscriber applications. See Procedure 71-1 for more information on how to configure this parameter.

Note — You cannot create a group interface under a forwarding subscriber interface.

Go to step 9.

b Create a subscriber interface for a traditional VPRN. Go to step 11.

9 Assign a forwarding service to the subscriber interface if you are configuring a wholesale and retail configuration for the VPRN.

i Click on the Select button in the Forwarding Service panel to choose a service. The Select Forwarding Service - VPRN Subscriber Interface form opens.

ii Select a service and click on the OK button. The Select Forwarding Service - VPRN Subscriber Interface form closes, and the VPRN Subscriber Interface (Create) form reappears with the service information displayed.

iii Configure the Private Retail Subnets parameter that appears after you have assigned a forwarding service.

10 Assign a forwarding subscriber interface to the VPRN subscriber interface.

i Click on the Select button in the Forwarding Subscriber Interface panel to choose a subscriber. The Select Forwarding Subscriber Interface - VPRN Subscriber Interface form opens.

ii Select a subscriber and click on the OK button. The Select Forwarding Subscriber Interface - VPRN Subscriber Interface form closes, and the VPRN Subscriber Interface (Create) form reappears with the subscriber information displayed.

11 Create IP addresses for the subscriber interface that are inherited by the SAPs in the group interfaces that are child objects of the subscriber interface.

i Click on the Address tab button.

ii Click on the Add button. The IP Address (Create) form opens.

iii Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Populate Host Routes
- Broadcast Address Format

iv Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

v Click on the OK button. The Subscriber Interface (Create) form reappears with the assigned IP addresses displayed.

vi Repeat steps ii to v for each additional IP address that you want to create.

12 Configure IPv4 DHCP for the interface, if required.

i Click on the DHCP tab button.

ii If you specified a forwarding service in step 9, the General tab is configurable. Configure the parameters that define the forwarding service information. Otherwise go to step vii.

- Enable DHCP Relay
- Description
- Lease Populate

iii If you specified a forwarding service in step 9 and depending on the type and version of the device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step vii.

iv Click on the Select button in the Subscriber Authentication Policy panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - SubItfDhcpRelayCfg form opens.

v Configure the filter criteria. A list of available policies appears.

vi Select a policy and click on the OK button. The Select Subscriber Authentication Policy - SubItfDhcpRelayCfg form closes, and the VPRN Subscriber Interface (Create) form refreshes with the subscriber authentication policy name.

vii Configure the parameters:

- IP address
- Use as source

viii Click on the Server tab button.

ix Configure the parameters.

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time RADIUS Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

x Click on the Client Applications tab button.

xi Configure the Client Applications parameter. You can enable either or both of the PPPoE or DHCP choices.

13 Configure PPPoE for the interface, if required.

Note — PPPoE is only configurable on a VPRN subscriber interface if the interface is a retailer interface.

i Click on the PPPoE tab button.

ii Configure the parameters:

- Description
- Session Limit

14 Configure the ARP host for the interface, if required.

Note — The ARP host is only configurable on a VPRN subscriber interface when the interface is a retailer interface.

i Click on the ARP Host Configuration tab button.

ii Configure the parameters:

- Administrative State
- ARP Host Limit

15 Click on the OK button. The VPRN Subscriber Interface (Create) form closes, and a dialog box appears.

16 Click on the OK button. The VPRN (Edit) form reappears with the new subscriber interface displayed in the service components tree.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The VPRN (Edit) form closes, and the Manage Services form reappears.

19 Close the Manage Services form.

Procedure 71-11 To add a group interface to a VPRN

The 7450 ESS in mixed mode, 7710 SR and 7750 SR support the configuration of a group interface in a VPRN.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on the subscriber interface to which you want to add a group interface, and choose Create VPRN Subscriber Interface. The VPRN Subscriber Interface (Create) form opens with the General tab displayed.

6 Click on the Group Interfaces tab button.

7 Click on the Add button and the VPRN Group Interface (Create) form opens with the General tab displayed.

8 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- MAC Address
- Trusted
- LNS

Note — The LNS parameter defines the type of group interface (regular or LNS). This parameter is set at creation time and cannot be modified. Regular group interfaces cannot configure LNS attributes and an LNS group interface does not allow PPPoE configuration or SAPs.

9 Configure IPv6 router advertisement and DHCPv6 on the group interface, if required.

i Configure the IPv6 Allowed parameter.

ii Click on the IPv6 Advertisement tab button and configure the parameters:

- Administrative State
- Current Hop Limit
- Managed Address Config
- Max Interval (seconds)
- Min Interval (seconds)
- Link MTU
- Other Stateful Config
- Reachable Time (milliseconds)
- Retransmit Time (milliseconds)
- Router Lifetime (seconds)
- Autonomous Address Configuration
- Preferred Lifetime
- Valid Lifetime

iii Click on the DHCPv6 tab button.

iv Click on the Select button and select a local user database from the Select Local User Database form.

v Click on the Proxy Server tab button and configure the parameters:

- Administrative State
- Renew Timer
- Rebind Timer
- Valid Lifetime
- Preferred Lifetime
- Client Applications

10 Click on the Anti-Spoofing tab button.

11 Configure the ARP Populate parameter.

12 Click on the Subscriber Management tab button.

13 Configure the parameters:

- SHCV Enabled
- SHCV Interval (minutes)
- SHCV Source
- SHCV Action

14 Configure ICMP for the group interface, if required.

i Click on the ICMP tab button.

ii Configure the parameters:

- Mask Reply
- Redirects
- Unreachables
- TTL Expired
- Number of Redirects
- Redirects Time (seconds)
- Number of Unreachables
- Unreachables Time (seconds)
- Number of TTL Expired
- TTL Expired Time (seconds)

15 Configure ARP for the group interface, if required.

i Click on the ARP tab button. The General tab is displayed.

ii Configure the Timeout (seconds) parameter.

iii Click on the Proxy ARP tab button.

iv Configure the parameters:

- Remote Proxy ARP
- Enable Local Proxy ARP
- Proxy ARP Policy 1 through Proxy ARP Policy 5

16 Configure IPv4 DHCP relay for the group interface, if required.

i Click on the DHCP tab button. The DHCP form opens with the General tab displayed.

ii Configure the parameters:

- Enable DHCP Relay
- Description
- Match Circuit ID
- Trusted
- Lease Populate
- L2 Header
- Anti-Spoof MAC Address
- Action
- Circuit ID
- Remote ID
- Remote ID String
- Vendor Specific Options
- Vendor String
- IP address
- Use as source

iii Depending on the type and version of device that you are configuring, the Subscriber Authentication Policy panel is present. Choose a Subscriber Authentication policy, if required. Otherwise, go to step x.

iv Click on the Select button in the Subscriber Authentication panel to choose a subscriber authentication policy. The Select Subscriber Authentication Policy - GrpItfDhcpRelayCfg form opens.

v Configure the filter criteria. A list of available policies appears.

vi Select a policy and click on the OK button. The Select Subscriber Authentication Policy - GrpItfDhcpRelayCfg form closes, and the VPRN Group Interface (Create) form reappears with the policy name information displayed.

vii Click on the Select button in the Local User Database panel to choose a local user database. The Select localUserDbPointer - GrpItfDhcpRelayCfg form opens.

viii Configure the filter criteria. A list of available databases appears.

ix Select a database and click on the OK button. The Select localUserDbPointer - GrpItfDhcpRelayCfg form closes, and the VPRN Group Interface (Create) form reappears with the database name information displayed.

x Click on the Server tab button.

xi Configure the parameters:

- Server 1 through Server 8
- Administrative State
- Emulated Server IP Address
- Lease Time
- Number of Days
- Number of Hours
- Number of Minutes
- Number of Seconds
- Lease Time RADIUS Override

The Number of Days, Number of Hours, Number of Minutes, Number of Seconds, and Lease Time RADIUS Override parameters are configurable only when the Lease Time parameter is set to Specified Time Period.

xii Click on the Client Applications tab button.

xiii Configure the Client Applications parameter.

17 Click on the PPPoE tab button to configure PPPoE for the group interface.

18 Configure the parameters:

- Description
- Administrative State

19 Click on the Select button beside the Name parameter. The Select PPPoE Policy form opens with a list of available PPPoE policies.

20 Choose a policy from the list.

21 Click on the OK button. The Select PPPoE Policy form closes and the VPRN Group Interface (Create) form refreshes with the new PPPoE policy.

22 Click on the Select button beside the Name parameter in the Local User DB panel. The Select Local User DB form opens with a list of available local user databases.

23 Choose a database from the list.

24 Click on the OK button. The Select Local User DB form closes and the VPRN Group Interface (Create) form refreshes with the selected local user DB.

25 Configure the remaining parameters:

- Session Limit
- Session Limit per SAP

26 Configure the ARP host for the group interface, if required.

i Click on the ARP Host Configuration tab button.

ii Configure the parameters:

- Administrative State
- ARP Host Limit
- Minimum Authentication Interval
- SAP ARP Host Limit

27 If you set the LNS parameter to TRUE in step 8, perform the following steps to configure LNS for the group interface.

Note — After you create an LNS group interface, you must configure the L2TP tunnel group profile or tunnel profile to terminate sessions for the LNS group interface that you just created; see Procedure 28-29. You can also configure the termination of sessions on a group interface using a RADIUS server.

i Click on the LNS tab button.

ii Configure the Description parameter.

iii Click on the Select button in the Default Subscriber Profile panel. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form opens with a list of available profiles.

iv Choose a subscriber profile from the list and click on the OK button. The Select Default Subscriber Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the Subscriber Profile displayed.

v Click on the Select button in the Default SLA Profile panel. The Select Default SLA Profile (Terminate LNS PPP Sessions) form opens with a list of available SLA profiles.

vi Choose an SLA profile from the list and click on the OK button. The Select Default SLA Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the SLA Profile displayed.

vii Click on the Select button in the Subscriber Identification Policy panel. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form opens with a list of available subscriber identification policies.

viii Choose a subscriber identification policy from the list and click on the OK button. The Select Subscriber Identification Policy (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the subscriber identification policy displayed.

ix Click on the Select button in the Default Application Profile panel. The Select Default Application Profile (Terminate LNS PPP Sessions) form opens with a list of available default application profiles.

x Choose a default application profile from the list and click on the OK button. The Select Default Application Profile (Terminate LNS PPP Sessions) form closes and the IES Group Interface (Create) form reappears with the default application profile displayed.

28 Configure the Default Subscriber Identification String parameter.

29 Click on the Service Access Points tab button to configure SAPs for the group interface.

30 Click on the Add button. The VPRN Service Access Point (Create) form opens with the General tab displayed.

31 Configure the parameters:

- Name
- Description
- Administrative State
- Calling Station ID

32 Click on the Port tab button.

33 Click on the Select button to choose a port for the L3 access interface. The Select Terminating Port - VPRN L3 Access Interface form opens.

Note — The form lists only ports in access or hybrid mode. To choose a port that is not listed, you must set the Mode parameter for the port to Access or Hybrid. After you do this, the port is listed when you click on the Search button.

34 Use the configurable filter and Search button to choose a port, and click on the OK button. The Select Terminating Port - VPRN L3 Access Interface form closes, and the VPRN L3 Access Interface (Create) form displays the port information.

35 Configure the parameters:

- Auto-Assign ID
- Outer Encapsulation Value
- Inner Encapsulation Value
- Outer Encapsulation Value (VPI)
- Inner Encapsulation Value (VCI)
- SAP Description
- SAP Administrative State

The Auto-Assign ID parameter is configurable if the port uses Dot1 Q encapsulation. When the parameter is enabled, the 5620 SAM automatically configures the Outer Encapsulation Value parameter using the lowest unassigned value.

Note — You can set the Auto-Assign ID parameter to be the default parameter for dot1q encapsulation by enabling the Access Interface Encap Value (Dot1q only) parameter on the User Preferences form.

The Inner Encapsulation Value is configurable only when the port is an Ethernet or frame relay port with Q in Q encapsulation.

The Outer Encapsulation Value (VPI) and Inner Encapsulation Value (VCI) parameters are configurable only for ATM ports.

36 Assign ingress and egress QoS policies to the SAP, if required.

Note — Items such as policies, schedulers, and filters can be applied later to multiple service components at once. Choose and right-click the components in the service components tree, choose Properties, and configure the parameters on the appropriate tab.

i Click on the QoS tab button.

ii Configure the parameters:

- Ingress Match QinQ Dot1P
- Egress Mark QinQ Top Bits Only
- Use Shared Queue

The Ingress Match QinQ Dot1P and Egress Mark QinQ Top Bits Only parameters are configurable only when the encapsulation type of the port is BCP Dot1 Q, Dot1 Q, or Q in Q.

iii Click on the Select button in the Ingress Policy panel to choose an ingress QoS policy. The Select Ingress Policy - VPRN Service Access Point form opens.

iv Select an ingress QoS policy and click on the OK button. The Select Ingress Policy - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form reappears with the ingress QoS policy information displayed.

Note — If you select an ingress policy which has a forwarding class mapped to an ingress queue group, you must ensure that the port you selected in step 34 has the access ingress queue group with the same name created on it.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

v Click on the Select button in the Egress Policy panel to choose an egress QoS policy. The Select Egress Policy - VPRN Service Access Point form opens.

vi Select an egress QoS policy and click on the OK button. The Select Egress Policy - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form reappears with the egress QoS policy information displayed.

Note — If you select an egress policy which has a forwarding class mapped to an egress queue group, you must ensure that the port you selected in step 34 has the access egress queue group with the same name created on it.

See Procedure 17-61 in chapter 17 for more information about how to configure Ethernet ports. See chapter 43 for more information about queue group template policies.

vii Click on the Select button in the Ingress Policer Control Policy panel to choose an ingress policer control policy. The Select Ingress Policer Control Policy form opens.

viii Select a policer control policy and click on the OK button. The Select Ingress Policer Control Policy form closes and the VPRN Service Access Point (Create) form reappears with the ingress policer control policy information displayed.

ix Click on the Select button in the Egress Policer Control Policy panel to choose an egress policer control policy. The Select Egress Policer Control Policy form opens.

x Select a policer control policy and click on the OK button. The Select Egress Policer Control Policy form closes and the VPRN Service Access Point (Create) form reappears with the egress policer control policy information displayed.

37 Click on the Schedulers tab button to configure scheduling; otherwise, go to step 41.

Note — The Schedulers tab is configurable only if a port is assigned to the SAP earlier in the procedure.

38 Perform one of the following.

a Specify that an aggregation scheduler policy is not applied to the SAP.

i Set the Aggregation parameter to off.

ii Configure the parameters:

- Aggregate Rate Limit (kbps)
- Frame Base Accounting

Note 1 — The Egress Aggregate Rate Limit (kbps) and Frame Base Accounting parameters are configurable only when there is no scheduler specified in the Egress Scheduler panel.

Note 2 — You cannot specify an egress scheduler when the Egress Aggregate Rate Limit (kbps) parameter is set to a value greater than zero.

iii Click on the Select button in the Ingress Scheduler panel to choose an ingress scheduler. The Select Ingress Scheduler - VPRN Service Access Point form opens.

iv Select an ingress scheduler and click on the OK button. The Select Ingress Scheduler - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form refreshes with the ingress scheduler information displayed.

v Click on the Select button in the Egress Scheduler panel to choose an egress scheduler. The Select Egress Scheduler - VPRN Service Access Point form opens.

vi Select an egress scheduler and click on the OK button. The Select Egress Scheduler - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form refreshes with the egress scheduler information displayed.

vii Go to step 41.

b Specify that an aggregation scheduler policy is applied to the SAP.

i Set the Aggregation parameter to on.

ii Configure the Frame Base Accounting parameter.

iii Click on the Select button in the Aggregation Scheduler panel to choose an aggregation scheduler. The Select Aggregation Scheduler - VPRN Service Access Point form opens.

iv Select an aggregation scheduler and click on the OK button. The Select Aggregation Scheduler - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form refreshes with the aggregation scheduler information displayed.

39 Click on the Aggregation Rate tab button to configure the aggregation rate; otherwise, go to step 41.

Note — The Aggregation Rate tab is configurable only when a port is assigned to the HSMDA SAP.

40 Configure the Aggregate Rate Limit (kbps) parameter in the Ingress Aggregate Rate Limit and Egress Aggregate Rate Limit panels.

41 Assign ingress and egress ACL filters to the SAP, if required.

i Click on the ACL tab button.

ii Click on the Select button in the Ingress Filter panel to choose an ingress ACL filter from the Select Ingress Filter - VPRN Service Access Point form.

iii Click on the Select button in the Egress Filter panel to choose an egress ACL filter from the Select Egress Filter - VPRN Service Access Point form.

42 Click on the Accounting tab button to assign an accounting policy to the SAP.

i Configure the Collect Accounting Statistics parameter.

ii Click on the Select button to choose an accounting policy. The Select Accounting Policy - VPRN Service Access Point form opens.

iii Select an accounting policy and click on the OK button. The Select Accounting Policy - VPRN Service Access Point form closes, and the VPRN Service Access Point (Create) form reappears with the accounting policy information displayed.

43 Click on the Anti-Spoofing tab button to configure anti-spoofing for the SAP.

i Configure the Anti-Spoofing parameter.

To configure residential subscriber management for static hosts, the Anti-Spoofing parameter must be set to at least IP-address matching, or optionally, to IP- and MAC-address matching.

ii Click on the Static Hosts tab button to add a static host to the SAP.

iii Click on the Static Hosts tab button to configure a static subscriber host entry for each subscriber host that is not managed by DHCP.

iv Click on the Add button. The Access Interface Anti-Spoofing Static Host Display (Create) form opens.

v Configure the parameters:

- IP Address
- MAC Address
- Subscriber Identification

vi Configure residential subscriber management for the static host.

vii Click on the Select button in the Subscriber Profile panel to choose a subscriber profile for the static host, if required. The Select Subscriber Profile - AntiSpoofingStaticHosts form opens with the list of available subscriber profiles displayed. Otherwise, go to step 44.

viii Select a subscriber profile and click on the OK button. The Select Subscriber Profile - AntiSpoofingStaticHosts form closes, and the subscriber profile name appears in the Subscriber Profile panel.

ix Click on the Select button in the SLA Profile panel to choose an SLA profile for the static host. The Select SLA Profile - AntiSpoofingStaticHosts form opens with the list of available SLA profiles displayed.

x Select an SLA profile and click on the OK button. The Select SLA Profile - AntiSpoofingStaticHosts form closes, and the SLA profile name appears in the SLA Profile panel.

xi Click on the Select button in the Application Profile panel to choose an application profile for the static host. The Select Application Profile - AntiSpoofingStaticHosts form opens with the list of application profiles on the NE displayed.

xii Select an application profile and click on the OK button. The Select Application Profile - AntiSpoofingStaticHosts form closes, and the application profile name appears in the Application Profile panel.

44 Click on the OK button. A dialog box appears.

45 Click on the OK button. The Access Interface Anti-Spoofing Static Host Display (Create) form closes.

46 Assign a DoS protection policy to the SAP, if required.

Note — A default DoS protection policy is automatically assigned to the SAP.

i Click on the Security tab button.

ii Click on the Select button. The Select NE DoS Protection - VPRN Service Access Point form opens.

iii Select a DoS protection policy in the list and click on the OK button. The Select NE DoS Protection - VPRN Service Access Point form closes and the policy ID is displayed on the L3 Access Interface (Create) form.

iv Configure the MAC Monitoring parameter.

47 Click on the Subscriber Management tab button to configure residential subscriber management on the SAP. The IGMP Host Tracking tab is displayed.

i Click on the Select button to choose the import policy used to filter IGMP packets. The Select SapIgmpHostTracking form opens.

ii Configure the filter parameters and click on the Search button. A list of import policies appears.

iii Choose a policy and click on the OK button. The selected import policy name appears.

iv Configure the parameters:

- Expiry Time
- Max Number of Groups
- Max Number of Sources per Group

v You can click on the Host Tracking Info tab button to view a list of hosts that are being tracked on this service access point.

vi Click on the Profiles tab button.

vii Configure the parameters:

- Admin Status
- Service Model
- Subscriber Limit
- Profiled Traffic only
- Non-Subscriber Traffic Identification
- Default Subscriber Identification Type
- Default Subscriber Id
- Default Intermediate Destination Id Type
- Default Intermediate Destination Id

viii Click on the Select button in the Default Subscriber Profile panel to choose a default subscriber profile for the SAP, if required. The Select Default Subscriber Profile form opens with the list of available subscriber profiles displayed.

ix Select a subscriber profile and click on the OK button. The Select Default Subscriber Profile form closes, and the subscriber profile name appears in the Default Subscriber Profile panel.

x Click on the Select button in the Default SLA Profile panel to choose a Default SLA profile for the SAP, if required. The Select Default SLA Profile form opens with the list of available SLA profiles displayed.

xi Select an SLA profile and click on the OK button. The Select Default SLA Profile form closes, and the SLA profile name appears in the Default SLA Profile panel.

xii Click on the Select button in the Subscriber Identification Policy panel to choose a subscriber identification policy for the SAP, if required. The Select Subscriber Identification Policy form opens with the list of available subscriber identification policies displayed.

xiii Select a subscriber identification policy and click on the OK button. The Select Subscriber Identification Policy form closes, and the subscriber identification policy name appears in the Subscriber Identification Policy panel.

xiv Click on the Select button in the Default Application Profile panel to choose a default application profile for the SAP, if required. The Select Default Application Profile form opens with the list of application profiles on the NE displayed.

xv Select an application profile and click on the OK button. The Select Default Application Profile form closes, and the application profile name appears in the Default Application Profile panel.

xvi Click on the Select button in the Non-Subscriber Traffic Subscriber Profile panel to choose a non-subscriber subscriber profile for the SAP, if required. The Select Non-Subscriber Traffic Subscriber Profile form opens with the list of available subscriber profiles displayed.

xvii Select a subscriber profile and click on the OK button. The Select Non-Subscriber Traffic Subscriber Profile form closes, and the subscriber profile name appears in the Non-Subscriber Traffic Subscriber Profile panel.

xviii Click on the Select button in the Non-Subscriber Traffic SLA Profile panel to choose a Non-Subscriber Traffic SLA profile for the SAP, if required. The Select Non-Subscriber Traffic SLA Profile form opens with the list of available SLA profiles displayed.

xix Select an SLA profile and click on the OK button. The Select Non-Subscriber Traffic SLA Profile form closes, and the SLA profile name appears in the Non-Subscriber Traffic SLA Profile panel.

xx Click on the Select button in the Non-Subscriber Traffic Application Profile panel to choose a non-subscriber traffic application profile for the SAP, if required. The Select Non-Subscriber Traffic Application Profile form opens with the list of application profiles on the NE displayed.

xxi Select an application profile and click on the OK button. The Select Non-Subscriber Traffic Application Profile form closes, and the application profile name appears in the Non-Subscriber Traffic Application Profile panel.

xxii Click on the Subscriber Hosts tab button to view active hosts for the subscriber instance, if required.

48 Click on the OK button. The VPRN Service Access Point (Create) form closes and a dialog box appears.

49 Click on the OK button. The VPRN Group Interface (Create) form refreshes to display the SAP.

50 To configure an additional SAP in the group interface, go to step 30.

51 Click on the SRRP tab button.

52 Click on the Add button. The SRRP Instance (Create) form opens with the General tab displayed.

53 Configure the parameters:

- SRRP ID
- Description
- Administrative State

54 Click on the Behavior tab button.

55 Configure the General parameters:

- Gateway MAC address.
- Keep Alive Interval
- Priority

56 Click on the Select button in the Message Path panel. The Select Message Path Pointer - SRRP Instance form opens, displaying the SAPs available on the site.

57 Select the SAP you want to use for the in-band messaging between the sites and click on the OK button. The Select Message Path Pointer - SRRP Instance form closes.

58 Click on the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 1 - SRRP Instance form opens.

59 Select an entry and click on the OK button. The Select Policy Pointer 1 - SRRP Instance form closes.

60 Click on the Select button in the Policy Pointer 1 panel. The Select Policy Pointer 2 - SRRP Instance form opens.

61 Select an entry and click on the OK button. The Select Policy Pointer 2 - SRRP Instance form closes.

62 Click on the OK button. The SRRP Instance (Create) form closes and a dialog box appears.

63 Click on the OK button.

64 Click on the OK button. The VPRN Group Interface (Create) form closes and a dialog box appears.

65 Click on the OK button. The VPRN (Edit) form refreshes to display the SAP below the group interface.

66 Click on the OK button. A dialog box appears.

67 Click on the Yes button. The VPRN (Edit) form closes.

68 Close the Manage Services form.

Procedure 71-12 To add an IP mirror interface to a VPRN

Perform this procedure to configure an IP mirror interface in a VPRN service. This is a spoke terminated interface used to receive mirrored packets from a remote source.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN and click on the Properties button. The VPRN (Edit) form opens with the General tab displayed.

4 Click on the Components tab button.

5 Right-click on IP Mirror Interfaces and choose Create IP Mirror Interface. The IP Mirror Interface (Create) form opens.

6 Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State

Note — The Name value for an IP mirror interface must be unique in VPRN site. There cannot be another L3 access interface, subscriber interface, or group interface with the same name on the VPRN site.

7 Click on the OK button. The IP Mirror Interface (Create) form closes and a dialog box appears.

8 Click on the OK button. The VPRN (Edit) form reappears with the IP mirror interface displayed in the service components tree.

9 Create a spoke SDP binding for the interface by performing steps 5 to 18 of Procedure 71-9.

10 Click on the OK button. A dialog box appears.

11 Click on the Yes button. The VPRN (Edit) form closes, and the Manage Services form reappears.

12 Close the Manage Services form.

Procedure 71-13 To implement dual homing using SRRP

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service and click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

4 Click on the Components tab button.

5 Create the redundant interface used for SRRP out-of-band messaging between the two NEs.

Note 1 — The two sites that participate in the dual homing configuration do not have to be part of the same service.

Note 2 — Ensure that the pair of sites each contains a properly configured subscriber interface and SAPs underneath the group interface that are participating in the redundant configuration.

Note 3 — Ensure that all subscriber interface IP addresses have a gateway address configured on them.

i Right-click on Redundant Interfaces for one site of the redundant pair, and choose Create Redundant Interface. The Redundant Interface (Create) form opens with the General tab displayed.

ii Configure the parameters:

- Interface ID
- Auto-Assign ID
- Name
- Description
- Administrative State

iii Click on the Address tab button.

iv Click on the Add button. The IP Address (Create) form opens.

v Specify IP addresses for the redundant interface on the current and remote sites. Configure the parameters:

- Address ID
- IP Address
- Prefix Length
- Remote IP Address

  This must be on the same subnet as the redundant interface IP address of the current site. For example, if the IP address of the current site is 7.7.7.7, with a prefix length of 24, then the redundant interface IP address of the remote site must be 7.7.7.d, where d is a value from 0 to 255, excluding 7.
- Broadcast Address Format

vi Click on the OK button. The IP Address (Create) form closes, and a dialog box appears.

vii Click on the OK button. The Redundant Interface (Create) form reappears with the assigned redundant interface IP addresses listed.

viii Click on the OK button. A dialog box appears.

ix Click on the OK button. The Redundant Interface (Create) form for the current site closes.

6 Create an SDP spoke binding between the current and remote sites. The Source Interface is the Redundant Interface you created in step 5 and the Tunnel Termination SIte is the remote site. The Return Tunnel must come from the remote site. See Procedure 71-8 for more information.

7 Assign the Redundant Interface to the Group Interface for the current site.

i Right-click on the Group Interface you want to use (under the Subscriber Interface in the Component view) and choose Properties. The VPRN Group Interface (Edit) form opens with the General tab displayed.

ii Click on the Select button in the Redundant Interface block. The Select Redundant Interface - VPRN Group Interface form opens.

iii Configure the list filter parameters if required and click on the Search button. A list of Redundant Interfaces on the site appears at the bottom of the form.

iv Select the Redundant Interface you created in step 5. The Select Redundant Interface - VPRN Group Interface form closes and the interface you selected appears in the Redundant Interface field.

v Click on the OK button. The VPRN Group Interface (Edit) form closes.

8 Create an SRRP Instance for the current site.

i Right-click on the SRRP Instances item (under Group Interfaces in the Component view) for the current site, and choose Create SRRP Instance. The SRRP Instance (Create) form opens with the General tab displayed.

ii Configure the parameters:

- SRRP ID
- Description
- Administrative State

Note — The SRRP ID value must be the same for the current and remote sites.

iii Click on the Behavior tab button.

iv Configure the General parameters:

- Gateway MAC address. Default is 00-00-00-00-00-00.
- Keep Alive Interval
- Priority

v Configure the Message Path by clicking the Select button adjacent to the Port field. The Select Message Path Pointer - SRRP Instance form opens, displaying the SAPs available on the site. Select the SAP you want to use for the in-band messaging between the sites.

vi Configure the Policy Pointers for the SRRP Instance, if required.

vii Click on the OK button. The SRRP Instance (Create) form closes, and a dialog box appears.

viii Click on the OK button. The VPRN (Edit) form reappears with the SRRP Instance displayed.

9 Click on the Turn Up button to activate the SRRP instance.

10 Repeat steps 5 to 9 for the remote site.

Note 1 — When you repeat steps 5 to 9 for the remote site, that site becomes the current site and the previously configured site is the remote site.

Note 2 — After the two sites have been properly set up, you can examine the SRRP peer associations at any time by right-clicking an SRRP Instance in the service's Component view. This opens the SRRP Instance - Edit form, which contains a read-only field called SRRP Peer. The Site ID, Service ID, and Operational State of the associated peer appear in this field.

You can also examine the state of an SRRP Instance by checking the Operational Flags field. The flags indicate specific problems that might occur with the SRRP Instance, as follows:

- Duplicate Subscriber IF Address: one of the local subscriber IP addresses is the same as a subscriber IP address on the remote node.
- Redundant Interface Mismatch: the local SRRP instance and remote SRRP instance have mismatched redundant interfaces.
- SAP Mismatch: the local SRRP instance is backing a different set of SAPs than the peer.
- Subnet Mismatch: one of the subnets that SRRP is backing up does not have a match with the peer.
- Dual Master: both SRRP instances are master at the same time.
- SAP Tag Mismatch: the local SRRP instance is backing a set of SAPs with different remote and local tags.
- SRRP ID Mismatch: the peer has a different SRRP instance ID backing the same subnet.

11 Click on the OK button. A dialog box appears.

12 Click on the OK button. The VPRN (Edit) form closes.

Procedure 71-14 To create an OSPF sham link

Perform this procedure to create an intra-area OSPF sham link between two VPRN sites. See "OSPF sham link support" in section 71.1 for more information.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service.

4 Click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

5 Click on the Components tab button.

6 Choose the first site that to participate in the sham link. If you need to create the site, perform steps 7 to 80 of Procedure 71-1.

7 Choose an L3 access interface for the site. If you need to create the L3 access interface, perform steps 5 to 43 of Procedure 71-2.

8 Configure OSPFv2 for the site. Perform to steps 6 to 9 of Procedure 71-3. Ensure that you select sub-step b in step 7.

9 Right-click on the OSPFv2 icon under the Protocols icon and choose Create Sham Link. The ShamLink (Create) form opens with the General tab displayed.

10 Click on the Select button to configure the Remote Neighbor IP Address parameter. This is the IP Address of the other site participating in the sham link.

11 Click on the Select button in the Interface block to configure the Interface Name parameter. The Select Interface - ShamLink form opens.

12 Click on the Search button.

13 Select an interface from the displayed list and click on the OK button. The Select Interface - ShamLink form closes and the ShamLink (Create) form refreshes with the selected Interface Name displayed.

14 Click on the Select button in the Area block to configure the Area ID parameter. The Select Area - ShamLink form opens.

15 Click on the Search button.

16 Select an area from the displayed list and click on the OK button. The Select Area - ShamLink form closes and the ShamLink (Create) form refreshes with the selected Area ID displayed.

17 Configure the Administrative State parameter.

18 Click on the Protocol Properties tab button.

19 Configure the parameters:

- Metric
- Hello Interval (seconds)
- Router Dead Interval (seconds)
- Retransmission Interval (seconds)
- Transit Delay (seconds)

20 The Authentication tab is configurable, depending on the OSPF version. Click on the Authentication tab button to configure authentication for the sham link, if required. Otherwise, go to step 23.

21 Configure the Authentication Type parameter. Perform one of the following:

a Click on the Authentication Type menu button and choose MD5-based Authentication from the drop-down menu.

i Click on the Add button to create an MD5 authentication key. The Md5Key (Create) form opens.

ii Configure the parameters:

- Key Index
- Key
- Re-enter Key

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Md5Key (Create) form closes, and the new authentication key appears in the list.

b Click on the Authentication Type menu button and choose Simple Password from the drop-down menu.

i Click on the Change Password button to enter a password. The Password (Create) form opens.

ii Configure the parameters:

- Password
- Re-enter Password

iii Click on the OK button. A dialog box appears.

iv Click on the Yes button. The Password (Create) form closes.

22 You can click on the Virtual Neighbor tab button to view OSPF configuration information on neighbor sites, if required.

23 Click on the OK button. A dialog box appears.

24 Click on the Yes button. The ShamLink (Create) form closes, and the 5620 SAM displays an icon for the new sham link in the navigation tree.

25 Repeat steps 6 to 24 for the second site participating in the sham link.

26 Click on the OK button. A dialog box appears.

27 Click on the Yes button to confirm the action. The VPRN (Edit) form closes and the Manage Services form reappears.

28 Click on the Close button to close the Manage Services form.

Procedure 71-15 To modify a VPRN service

Caution 1 — Modifying parameters can be service-affecting.

Caution 2 — The behavior of the VPRN service may become unpredictable if modifications to the configuration affect the IPsec portion of the service configuration. For example, if a VPRN service is configured with IPsec tunnels, IPsec SAPS, and policies are deleted, the service is not deleted from the 5620 SAM and the service will be in an inconsistent state. The IPSEC portion of the VPRN configuration must be deleted using CLI scripts or the CLI before the VPRN service can be deleted from the 5620 SAM.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service and click on the Properties button. The VPRN (Edit) form opens with the general properties of the service displayed on the General tab.

The following tabs list the service elements that can be individually or collectively selected and configured:

- Components tab — displays the various service components in a tree format
- Tests tab — allows the creation and execution of service-specific diagnostic tests
- Sites tab — lists the sites that are included in the service
- L3 Access Interfaces tab — lists the L3 access interfaces that are included in the service
- Spoke SDP Bindings tab — displays the spoke SDP bindings that are associated with the service
- Address tab — lists the IP addresses that are associated with the service

Note — You cannot remove an IP address from an interface when the IP address of a static host is defined in the subnet of the interface IP address and the ARP Populate parameter is enabled on the Anti-Spoofing tab.

- Template tab — displays the template used to create the service, if applicable.
- Faults tab — displays the faults associated with the service

Note — Users with the administrator scope of command role can click on the Select button on the Template tab to associate a service template with the service object, if required.

4 Modify the parameters for the service, as required.

To configure items in the Components tab, select and right-click on the items and choose Properties from the contextual menu.

To configure items in the tabs that contain lists of service elements, select the items and click on the Properties button.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The VPRN (Edit) form closes and the Manage Services form reappears.

7 Click on the Close button to close the Manage Services form.

Procedure 71-16 To view the service operational status

The Aggregated Operational State and State Cause indicators on the General tab of the service management form display information about service faults.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VPRN (Edit) form opens.

4 View the Aggregated Operational State and State Cause indicators. When the Aggregated Operational State is Down or Partially Down, a check mark beside the appropriate State Cause indicator identifies the type of associated service fault.

5 Click on the appropriate tab button to view or edit an object that is identified as faulty by a State Cause indicator.

6 Click on the Faults tab button to view the alarms for the object. The Object Alarms tab is displayed.

7 Click on the Aggregated Alarms tab button to view the aggregated alarms for the object. The Aggregated Alarms tab is displayed.

8 Close the VPRN (Edit) form.

9 Click on the Close button to close the Manage Services form.

Procedure 71-17 To run an OAM validation test

An OAM validator test suite must be created for the tested entity. See chapter 75 for more information about how to create an OAM validator test suite.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a service and click on the Properties button. The VPRN (Edit) form opens with the General tab displayed.

4 Click on the Validate button. If an OAM validator test suite is not associated to the service, a dialog box appears. Perform the following steps:

   i Click on the OK button to associate the service with an existing OAM validator test suite. The Choose Validator Test Suite form appears.

   ii Configure the filter criteria. A list of OAM validator test suites appears.

   iii Select an OAM validator test suite and click on the OK button. The Choose Validator Test Suite form closes.

5 View the State Cause indicators. When the validation test fails, a check mark appears beside the OAM Validation Failure indicator.

6 Click on the Tests tab button.

7 Click on the Validation Result tab button.

8 Choose an entry and click on the Properties button. The Tested Entity Result (Edit) form opens with the General tab displayed.

9 Click on the Results tab button to display the validation test results.

10 If you need to compare two test results from the same type of test, choose the two test results and click on the Compare button; the Difference form opens. Otherwise, go to step 13.

11 Compare the test results.

12 Close the Difference form.

13 Close the Tested Entity Result form.

14 Close the VPRN (Edit) form.

15 Close the Manage Services form.

Procedure 71-18 To view the service topology

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service and click on the Topology View button. A Topology View dialog box appears.

4 Click on the Yes button to proceed. The Service Topology - map opens.

See chapter 4 for more information about service topology views.

Procedure 71-19 To modify a VPRN service using the topology view

The topology view for a service provides a graphical representation of the various components and their interconnections. You can also use this view to add, modify, or just navigate to service components. This provides an alternative approach to performing these functions from the component tree view.

Working from the topology view can expedite the creation of the components, since many of the fields you would ordinarily have to set in the configuration forms will be automatically populated using this approach. The configuration forms can also be accessed directly at any time from this view by right-clicking a component. This allows quick access to conduct more detailed component configuration.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Select a VPRN service and click on the Topology View button. The Service Topology map opens.

The remainder of this procedure contains a number of sub-procedures describing the various components that can be viewed, created, or modified from the topology view. These include:

- Creating a new site. Go to step 4.
- Creating site components. Go to step 9.
- Creating spoke SDP bindings. Go to step 36.
- Viewing the route target topology. Go to step 44.

Adding a new site

4 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the Create VPRN Site option.

The Select Network Elements form appears.

5 Select one or more sites to add to the service and click OK. The VPRN Site (Create) form for the new site is displayed. If you selected more than one site, the VPRN Site (Multiple Instances) (Create) form for the new sites is displayed.

6 Click on OK. The VPRN Site (Create) (or VPRN Site (Multiple Instances) (Create)) form closes and the new site (or sites) is displayed on the map.

7 If you want to perform detailed configuration of site properties for the new site, right-click the site icon and select Properties from the contextual menu. The Site (Edit) form opens. Refer to Procedure 71-1 for detailed site configuration information.

8 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

Creating site components

9 Right-click on any site icon in the service topology map. A contextual menu is displayed. You can choose to create one of the following:

- VPRN L3 Access Interface. Go to step 10.
- IPsec Interface. Go to step 15.
- VPRN Subscriber Interface. Go to step 20.
- Redundant Interface. Go to step 24.
- IP Mirror Interface. Go to step 28.
- Video Interface. Go to step 32.

10 If you choose to create a VPRN L3 Access Interface, then the VPRN L3 Access Interface (Create) form is displayed.

11 Configure the Name parameter on the General tab page.

12 Click on the Port tab and assign a port to the interface.

Refer to Procedure 71-2 for detailed information on further configuring the interface, if required.

13 Click OK. The VPRN L3 Access Interface (Create) form closes and the new L3 access interface is displayed in the topology view.

14 Go to step 35.

15 If you choose to create an IPsec Interface, then the IPsec Interface (Create) form is displayed.

16 Configure the Name parameter on the General tab page.

17 Click on the Port tab and assign a port to the interface.

Refer to Procedure 32-6 in Chapter 32 for detailed information on further configuring the interface, if required.

18 Click OK. The IPsec Interface (Create) form closes and the new IPsec interface is displayed in the topology view.

19 Go to step 35.

20 If you choose to create a VPRN Subscriber Interface, then the VPRN Subscriber Interface (Create) form is displayed.

21 Configure the Name parameter for the interface.

Refer to Procedure 71-10 for detailed information on further configuring the interface, if required.

22 Click OK. The VPRN Subscriber Interface (Create) form closes and the new subscriber interface is displayed in the topology view.

23 Go to step 35.

24 If you choose to create a Redundant Interface, then the Redundant Interface (Create) form is displayed.

25 Configure the Name parameter for the interface.

Refer to Procedure 71-13 for detailed information on further configuring the interface, if required.

26 Click OK. The Redundant Interface (Create) form closes and the new redundant interface is displayed in the topology view.

27 Go to step 35.

28 If you choose to create an IP Mirror Interface, then the IP Mirror Interface (Create) form is displayed.

29 Configure the Name parameter for the interface.

Refer to Procedure 71-12 for detailed information on further configuring the interface, if required.

30 Click OK. The IP Mirror Interface (Create) form closes.

31 Go to step 35.

32 If you choose to create a Video Interface, then the Video Interface (Create) form is displayed.

33 Configure the Name parameter for the interface.

Refer to Procedure 33-1 in Chapter 33 for detailed information on further configuring the interface, if required.

34 Click OK. The Video Interface (Create) form closes and the new video interface is displayed in the topology view.

35 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

Creating spoke SDP bindings

36 Select the sites you want to connect in the service topology map and right-click on any one of them. A contextual menu is displayed.

Note — When you create a spoke binding between two sites, the order in which you select them is important. The first site you select will become the source site and the second site will become the destination site. Therefore, it is not recommended that you do a marquee-select in the topology view, since you will not be sure of this hierarchy. Instead, select the sites individually, and hold down the Shift or Ctrl key after your first selection.

37 Select Connect from the contextual menu and choose the Create Spoke SDP Binding option.

The Spoke SDP Binding (Create) form is displayed.

Note — For this function, it is assumed that you clicked on the source site first and then held down the Shift or Ctrl key while right-clicking on the destination site to display the contextual menu.

38 Enable the Auto Select Transport Tunnel parameter.

39 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new binding between the two sites is displayed in the topology view. Refer to Procedure 71-8 for more detailed information on creating and configuring spoke SDP bindings, if required.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 30 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

40 Assuming that the spoke SDP binding was successfully created in step 39, select the same two sites again in the topology view, although this time do so in the opposite order that you originally selected them. This will allow you to create a spoke binding for the return tunnel.

41 Right-click on the second site you selected and choose the Create Spoke SDP Binding ... option from the contextual menu. The Spoke SDP Binding (Create) form is displayed.

42 You can manually configure other parameters here if required, or just click on OK. One of the following will result:

- If an available transport tunnel exists between the two sites, then the Spoke SDP Binding (Create) form closes and the new return binding between the two sites is displayed in the topology view.
- If an available transport tunnel does not exist between the two sites, then an error message is displayed to that affect. Refer to Chapter 30 for information on how to create the required tunnel. Once the tunnel is created, you can repeat this sub-procedure.

43 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

Viewing the route target topology

44 Right-click on any blank space in the service topology map. A contextual menu is displayed. Choose the Highlight Route Target Topology option.

This option essentially draws dotted lines to represent the route target topology between NEs. For example, for two NEs A and B, if the import and export route targets match, then two dotted lines will be drawn on the map. One will represent the route target going from A to B, and the other from B to A.

45 Return to step 3 for a list of other functions you can perform from the topology view or go to step 46 to finish.

46 Close the Service Topology form.

47 Close the Manage Services form.

Procedure 71-20 To delete a VPRN service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria. A list of services appears at the bottom of the Manage Services form.

3 Choose a VPRN service.

Note 1 — You cannot delete a VPRN service when IPsec security policies, interfaces, or tunnels are configured. See the appropriate node documentation for more information about modifying or deleting IPsec configurations.

For example, if a VPRN service is configured with IPsec tunnels, IPsec SAPS, and policies is deleted, the service is not deleted from the 5620 SAM and the service will be in an inconsistent state. The IPSEC portion of the VPRN configuration must be deleted using the CLI scripts or through the CLI before the VPRN service can be deleted from the 5620 SAM.

Note 2 — The L3 interface properties for the IPSEC SAP cannot be configured using the 5620 SAM.

4 Click on the Delete button. A dialog box appears and prompts you to confirm that you understand the implications of deleting the service.

5 Click on the Yes button to confirm the action. The service is deleted and removed from the list.

6 Click on the Close button to close the Manage Services form.

72 — Composite service management

72.1 Composite service management overview

A composite service is a set of linked services. Composite service functionality supports complex applications that require a combination of services, such as VLAN connections to an HVPLS, an IES spoke into a VPLS, or a VPRN-to-VPLS interconnection.

Services that are owned by different customers can be connected to form a composite service. An example is an HVPLS in which the core VPLS belongs to one customer and the satellite VPLS instances belong to other customers. An HVPLS is considered to be a composite service by the 5620 SAM.

Composite services consist of customer services, called SCs in the context of a composite service, and connectors. A connector is a bidirectional logical link between two SCs, such as a pair of PW spokes that carry traffic in opposite directions between VLL and VPLS instances, a dot1Q-encapsulated link between a VLAN and a VPLS, or an internal cross-connect.

The term SCP describes a type of connector endpoint. In the case of the services that are available on the 7450 ESS, 7710 SR, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, or the 7750 SR, an SCP is a service interface or SAP. For L2 switches, such as the 7250 SAS or Telco, an SCP may be a network interface, such as an uplink port.

Composite services exist only in the context of the 5620 SAM and are configured through the 5620 SAM GUI or an OSS application. They are unknown to individual network devices. To simplify composite service configuration and to ensure that non-5620 SAM device configuration does not disrupt the management of composite services, the following rules apply to the creation, deletion, modification, and presentation of composite services.

- A composite service can have zero SCs.
- A composite service can have zero connectors.
- Two connected SCs can belong to only one composite service.
- A connector between two SCs belongs to only one composite service.
- An SC cannot be removed from a composite service until its connector to the composite service is removed.
- A group of connected services can be moved from one composite service to another.

The 5620 SAM supports composite-service configuration using the following methods.

- Tabbed configuration forms with an embedded navigation tree that provides a logical, hierarchical view of the composite service and acts as a configuration interface. When you right-click on an object in the navigation tree, a menu specific to the object appears. When you choose an object in the menu, the related configuration form opens.
- Connector creation and configuration from within the composite service's flat topology view
- Pre-configured template. A user that is assigned the service management scope of command role can create a composite-service template. The service management user can also create a connector template. See the *5620 SAM Scripts and Templates Developer Guide* for more information about the administrative tasks associated with creating and using templates.

If a service that is specified for inclusion in a composite service does not currently belong to a composite service, it is added to the composite service regardless of its administrative or operational state. If the specified service is part of an existing composite service, it can be moved to a different composite service. However, SCs that are connected to the specified service are also moved to the new composite service upon confirmation of the action by the 5620 SAM operator. The 5620 SAM performs no such action confirmation for OSS applications.

When services within a composite service have the same service ID, the 5620 SAM raises an alarm. For example, a VPLS with service ID 5 on one NE and an IES service with service ID 5 on another NE are combined to create a composite service. The operational status of the composite service is up and the composite service functions correctly, however, an alarm is raised because the 5620 SAM does not support the configuration of two services using the same service ID. This situation may arise when services are created on NEs using a CLI rather than through the 5620 SAM.

Hierarchical organization of composite services

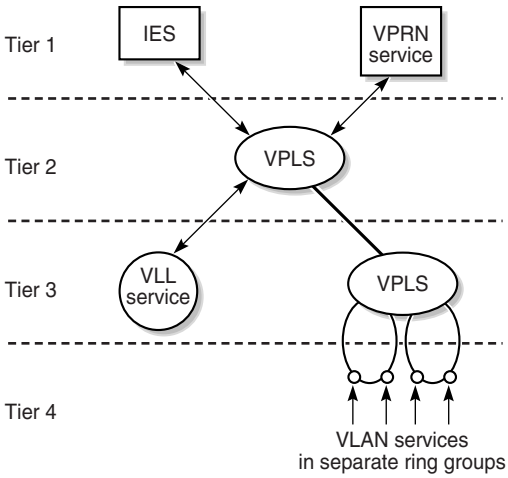
The 5620 SAM organizes the SCs in a composite service by tiers within a hierarchy during network discovery and for display purposes. When you add an SC to a composite service, the 5620 SAM assigns a default tier value to the SC according to the service type. Table 72-1 lists the default tiers for different service types.

Table 72-1 Default tiers for service types

Service type	Default tier
IES and VPRN	1
VPLS and MVPLS	2
VLL	3
VLAN	4

The default tier values reflect common deployment configurations. Figure 72-1 shows a composite service hierarchy. SCs are not restricted to the default tiers, as in the case of the VPLS in Tier 3 that forms an HVPLS with the VPLS in Tier 2.

Figure 72-1 Default SC tier assignments



You can change the tier of an SC at any time and can specify a value other than one of the defaults that the 5620 SAM assigns; composite services can have many tiers.

The tier value of an SC determines the relative position of the SC within a composite service topology map. The 5620 SAM displays SCs in rows by tier, in numerical order from the top of the panel downward, beginning with tier 1.

You can move SC icons in a composite service topology map from one tier to another for a customized view, then use the Rearrange by Service Tiers button to organize the SC icons in the map panel according to tier.

Caution — The composite service topology map is redrawn when you click on the Rearrange by Service Tiers button, and you cannot revert to the former layout of the composite service topology map.

See chapter 4 for more information about 5620 SAM map management.

Network discovery of composite services

The 5620 SAM associates SCs and connectors with composite services during network discovery. The following rules apply to this process.

- When the 5620 SAM discovers a valid connector between two services that do not belong to a composite service, a composite service that contains the services and connector is automatically created.
- When the 5620 SAM discovers a valid connector between two services and one of the services belongs to a composite service, the other service is added as an SC of the composite service.
- When the 5620 SAM discovers a valid connector between two services and the two services are SCs of different composite services, an alarm is raised and the connector is excluded from the 5620 SAM database.

The 5620 SAM assigns a default tier value to a service upon creation and to a new SC during network discovery. The tiered hierarchy provides a common framework for service configurations that are provisioned through the 5620 SAM and CLI. A 5620 SAM operator can assign a different tier value to an SC after discovery.

A composite service has Aggregated Operational State, Connection State, and Service Component Degraded status indicators. The General tab of the Composite Service management form displays these indicators.

The Aggregated Operational State indicator has four possible values: Up, Down, Partially Down, and Unknown. The value is derived from the aggregated SC operational states as follows.

- Up—All SCs are operationally up
- Partially Down—At least one SC is operationally down
- Down—All SCs are operationally down
- Unknown—The status of at least one SC is undetermined

The Connection State indicator displays one of three values, as follows:

- No Connection—None of the SCs is connected to any other SC
- Partially Connected—One SC is not able to communicate directly or indirectly with all other SCs
- Strongly Connected—All SCs are able to communicate

For example, a composite service has five services named A, B, C, D, and E. A is connected to B, C is connected to D, and D is connected to E. The Connection State in this case is Partially Connected. When A or B becomes connected to C, D, or E, the Connection State becomes Strongly Connected.

The Service Component Degraded indicator shows whether there is an operational flag set on any of the service sites under this composite service.

Connector types

The following types of connectors join SCs in a composite service:

- SCP-to-SCP
- internal cross-connect
- PW spoke
- routed VPLS

SCP-to-SCP connectors

SCP-to-SCP connectors can join any two SC types that have service interfaces on the same device or on different devices. A connector between VPLS and VPRN SAPs is an SCP-to-SCP connector, as is a connector between a dot1Q-encapsulated VPLS SAP and L2 switch uplink port in a VLAN ring group. Table 72-2 describes the supported encapsulation types.

Table 72-2 Supported encapsulation types

SAP type	Encapsulation type
Ethernet	Dot1 Q
	Q in Q
	Null
ATM	VPI/VCI
	VPI
FR	DLCI
SONET/SDH	BCP Null
	BCP Dot1 Q
	IPCP
	PPP Auto
	cHDLC
	WAN Mirror
LAG	Null
	Dot1 Q

The operational status of an SCP-to-SCP connector depends on the operational status of its endpoints. An alarm raised against one of the endpoints causes an alarm to be raised against the connector. Such alarms are aggregated within the composite service.

Internal cross-connect connectors

An internal cross-connect connector can join any SC types. It uses a CCAG to join two SCs that have SAPs or network interfaces on the same device. This functionality is available in the 7450 ESS, 7710 SR, and 7750 SR. The following rules apply to internal cross-connect connectors.

- A SAP can be connected to another SAP or to a network interface using a CCAG.
- When a SAP or network interface is deleted, the connector associated with it is also deleted.
- The deletion of an internal cross-connect connector causes the associated interfaces and SAPs to be deleted.

The operational state of an internal cross-connect connector depends on the operational state of the CCAG. An alarm raised against the CCAG causes an alarm to be raised against the connector. Such alarms are aggregated within the composite service.

PW spoke connectors

A PW spoke connector generally joins VPLS instances to create an HVPLS. In the 7450 ESS, 7710 SR, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, and 7750 SR, a PW spoke can, for example, connect IES and VPLS instances to provide distributed Internet access service. The endpoints of a PW spoke connector must be on different devices. PW spoke connectors are subject to restrictions on the SC types that they can join. Table 72-3 shows the SC types that can be linked by PW spoke connectors.

Table 72-3 Valid PW spoke interconnections

SC type	Valid PW spoke SC interconnections
VLL	IES, VPLS
VLAN	—
VPLS	IES, VLL, VPLS
MVPLS	MVPLS
IES	VLL, VPLS
VPRN	VLL, VPLS

The operational state of a PW spoke connector depends on the operational state of the underlying SDP bindings. An alarm raised against one of the SDP bindings causes an alarm to be raised against the connector. Such alarms are aggregated within the composite service.

Routed VPLS connectors

A routed VPLS connector joins an L3 access interface within an IES or VPRN service context to a VPLS on the same site. When an IES or VPRN IP interface is bound to a VPLS site name, the site name cannot be bound to another IP interface. Although an IES or VPRN IP interface can only be bound to a single VPLS site, the service context that contains the IP interface can have other IP interfaces bound to other VPLS sites. Both the IES or VPRN IP interface and VPLS site must be located on the same NE.

If a VPLS site name does not exist within the system, the binding between the IP interface and the VPLS site remains operationally down until a VPLS site name is assigned to the VPLS site. When an IP interface is bound to a VPLS site, the operational state of the binding depends on the operational state of the VPLS site, or whether the IP interface binding is enabled on the VPLS site.

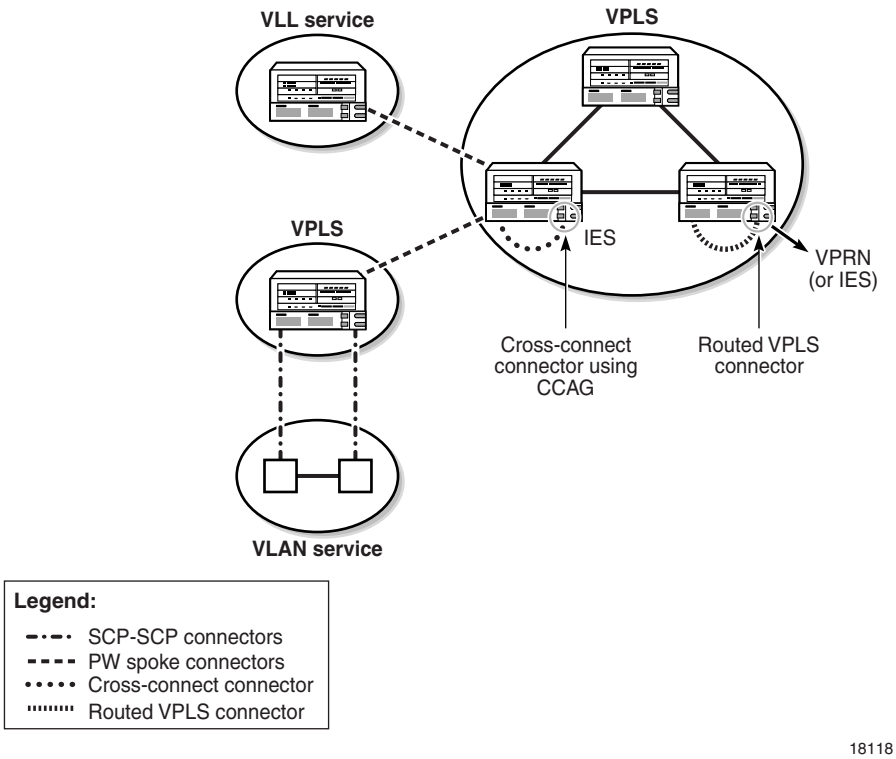
The operational state of the routed VPLS connector depends on the operational state of the binding and the operational state of the L3 IP interface.

This functionality is only supported on IOM3 cards on the 7450 ESS in mixed mode, Release 8.0R4, 7750 SR, Release 8.0R4, and 7750 SR-c4, Release 8.0R5.

72.2 Sample composite service configuration

Figure 72-2 shows a sample composite service configuration that involves a variety of customer services and uses the three SC connector types.

Figure 72-2 Sample composite service configuration



72.3 Workflow to create a composite service

1 Set up group and user access privileges.

2 Configure the network.

   i Build the IP or IP/MPLS core network.

   ii Configure service tunnels.

3 Create the customer services that are to be SCs of the composite service.

4 Create the composite service.

   i Define general properties for the composite service.

   ii Specify the services that are participating in the composite service. You can specify multiple services in one operation.

   iii Create connectors to link the SCs of the composite service.

5 Turn up the composite service.

72.4 Composite service management procedures

Use the following procedures to perform composite service creation and management tasks.

Procedure 72-1 To create a composite service

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Click on the Create button. The Composite Service (Create) form opens.

3 Configure the parameters.

- Composite ID
- Auto-Assign ID
- Name
- Description

4 Click on the Apply button. The form title changes to Composite Service *Service Name* (Edit) and the form displays an additional tab button and Status and OLC panels.

5 Configure the OLC State parameter.

6 Perform one of the following:

   a Add an SC to the composite service. Go to step 7.

   b Complete composite service creation if SCs and connectors are to be added later. Go to step 18.

7 Click on the Components tab button.

8 Right-click on the Services icon and choose Add Services. The Add Services form opens.

Note — You can also create a service for inclusion in the composite service by right-clicking on the Services icon and choosing Create *Service Type*.

9 Click on the Search button. A list of available services is displayed.

10 Select a service and click on the OK button. You can select multiple services. The CompositeService - *Service Name* (Edit) form refreshes with the SC information displayed.

11 Perform one of the following:

a Add a connector to the composite service. Go to step 12.

b Complete composite service creation if connectors are to be created later. Go to step 18.

12 Right-click on the Connector icon on the Components tab and choose one of the following options:

a Create CrossConnect. Go to step 13.

b Create RoutedVplsConnector. Go to step 14.

c Create ScpConnector. Go to step 15.

d Create SpokeConnector. Go to step 16.

13 The Cross Connect (Create) form opens.

Note — The service endpoints of a cross-connect connector must be on the same NE.

i Configure the parameters.

- Name
- Description

ii Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - Cross Connect form opens with a list of available SCs displayed.

iii Choose an SC and click on the OK button. The Select Service A - Cross Connect form closes and the Cross Connect (Create) form refreshes.

iv Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - Cross Connect form opens with a list of available SCs displayed.

v Choose an SC and click on the OK button. The Select Service B - Cross Connect form closes and the Cross Connect (Create) form refreshes.

vi Click on the Select button in the Site A panel to choose a site to associate with the connector. The Select Site - Cross Connect form opens with a list of available sites displayed.

vii Choose a site and click on the OK button. The Select Site - Cross Connect form closes and the Cross Connect (Create) form refreshes.

viii Click on the Select button in the Site B panel to choose an SC to associate with the connector. The Select Site - Cross Connect form opens with a list of available sites displayed.

ix Choose a site and click on the OK button. The Select Site - Cross Connect form closes and the Cross Connect (Create) form refreshes.

x Click on the Transport tab button.

xi Click on the Select button to choose a CCAG for the connector. The Select CCAG - Cross Connect form opens with a list of available CCAGs displayed.

xii Choose a CCAG and click on the OK button. The Select CCAG - Cross Connect (Create) form closes and the Cross Connect (Create) form refreshes.

xiii Configure the parameters.

- CC Id
- Auto-Assign

xiv Click on the OK button. The Cross Connect (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

xv Go to step 17.

14 The RoutedVplsConnector (Create) form opens.

i Configure the parameters:

- Name
- Description

ii Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - RoutedVplsConnector form opens with a list of available SCs displayed.

iii Select an SC and click on the OK button. The Select Service A - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.

iv Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - RoutedVplsConnector form opens with a list of available SCs displayed.

v Select an SC and click on the OK button. The Select Service B - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.

vi Click on the Select button in the Site A panel to choose a site to associate with the connector. The Select Site - RoutedVplsConnector form opens with a list of available sites displayed.

vii Select a site and click on the OK button. The Select Site - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.

viii Click on the Select button in the Site B panel to choose a site to associate with the connector. The Select Site - RoutedVplsConnector form opens with a list of available sites displayed.

ix Select a site and click on the OK button. The Select Site - RoutedVplsConnector form closes and the RoutedVplsConnector (Create) form refreshes.

Note — The sites that you select in substeps vii and ix must be located on the same NE.

x Click on the Routed-VPLS L3 Connection Point tab button.

xi Click on the Select button to choose an interface for the connector. The Select L3 Access Interface - RoutedVplsConnector form opens with a list of available L3 Access Interfaces displayed.

xii Select an L3 Access Interface and click on the OK button. The RoutedVplsConnector (Create) form refreshes.

xiii Click on the OK button. The RoutedVplsConnector (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

xiv Go to step 17.

15 The ScpConnector (Create) form opens.

i Configure the parameters.

- Name
- Description

ii Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - ScpConnector form opens with a list of available SCs displayed.

iii Select an SC and click on the OK button. The Select Service A - Scp Connector (Create) form closes and the ScpConnector (Create) form refreshes.

iv Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - ScpConnector form opens with a list of available SCs displayed.

v Select an SC and click on the OK button. The Select Service B - Scp Connector (Create) form closes and the ScpConnector (Create) form refreshes.

vi Click on the Select button in the Site A panel to choose a site to associate with the connector. The Select Site - ScpConnector form opens with a list of available sites displayed.

vii Select a site and click on the OK button. The Select Site - Scp Connector (Create) form closes and the ScpConnector (Create) form refreshes.

viii Click on the Select button in the Site B panel to choose a site to associate with the connector. The Select Site - ScpConnector form opens with a list of available sites displayed.

ix Select a site and click on the OK button. The Select Site - Scp Connector form closes and the ScpConnector (Create) form refreshes.

x Click on the Service Connection Point tab button.

xi Click on the Select button in the Service Connection Point A panel to choose an SCP to associate with the connector. The Select Service Connection Point A - Scp Connector form opens with a list of available SCPs displayed.

xii Select an SCP and click on the OK button. The Select Service Connection Point A - Scp Connector form closes and the ScpConnector (Create) form refreshes.

xiii Click on the Select button in the Service Connection Point B panel to choose an SCP to associate with the connector. The Select Service Connection Point B - Scp Connector form opens with a list of available SCPs displayed.

xiv Select an SCP and click on the OK button. The Select Service Connection Point B - Scp Connector form closes and the ScpConnector (Create) form refreshes.

xv Click on the OK button. the ScpConnector (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

xvi Go to step 17.

16 The SpokeConnector (Create) form opens.

Note — The service endpoints of a spoke connector must be on different NEs.

i Configure the parameters.

- Name
- Description

ii Click on the Select button in the Service A panel to choose an SC to associate with the connector. The Select Service A - Spoke Connector form opens with a list of available SCs displayed.

iii Select an SC and click on the OK button. The Select Service A - Spoke Connector (Create) form closes and the SpokeConnector (Create) form refreshes.

iv Click on the Select button in the Service B panel to choose an SC to associate with the connector. The Select Service B - Spoke Connector form opens with a list of available SCs displayed.

v Select an SC and click on the OK button. The Select Service B - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

vi Click on the Select button in the Site A panel to choose a site from service A to associate with the connector. The Select Site - Spoke Connector form opens with a list of available sites displayed.

vii Select a site and click on the OK button. The Select Site - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

viii Click on the Select button in the Site B panel to choose a site from service B to associate with the connector. The Select Site - Spoke Connector form opens with a list of available sites displayed.

ix Select a site and click on the OK button. The Select Site - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

x Click on the Transport tab button.

xi Configure the parameters.

- VC ID
- Auto-Assign
- Auto Select Tunnels
- Transport Type

The Transport Type parameter is configurable when the Auto Select Tunnels parameter is enabled.

xii If the Auto Select Tunnels parameter is enabled, go to step xvii.

xiii Click on the Select button in the Tunnel A panel to choose a service tunnel to associate with the connector. The Select Tunnel From Site A - Spoke Connector form opens with a list of available service tunnels displayed.

xiv Select a tunnel and click on the OK button. The Select Tunnel From Site A - Spoke Connector form closes and the SpokeConnector (Create) form refreshes.

xv Click on the Select button in the Tunnel B panel to choose a service tunnel to associate with the connector. The Select Tunnel From Site B - Spoke Connector (Create) form opens with a list of available service tunnels displayed.

xvi Select a tunnel and click on the OK button. The Select Tunnel From Site B - Spoke Connector (Create) form closes and the SpokeConnector (Create) form refreshes.

xvii The First L3 Access Interface panel is present, if one of the SCs in the composite service is an IES. If the First L3 Access Interface panel is not present, go to step xxii.

xviii Click on the Select button in the First L3 Access Interface panel to choose an access interface to associate with the spoke connector. The Select First L3 Access Interface - Spoke Connector (Create) form opens with a list of available L3 access interfaces displayed.

xix The Second L3 Access Interface panel is present, if another of the SCs in the composite service is an IES. If the Second L3 Access Interface panel is not present, go to step xxii.

xx Click on the Select button in the Second L3 Access Interface panel to choose an access interface to associate with the spoke connector. The Select Second L3 Access Interface - Spoke Connector (Create) form opens with a list of available L3 access interfaces displayed.

xxi Select an L3 access interface and click on the OK button. The Select L3 Access Interface - Spoke Connector (Create) form closes and the SpokeConnector (Create) form refreshes.

xxii Click on the OK button. The SpokeConnector (Create) form closes and the CompositeService - *Service Name* (Edit) form refreshes.

17 Perform one of the following:

a Add an SC to the composite service. Repeat steps 8 to 10.

b Add a connector to the composite service. Go to step 12.

c Complete site creation. Go to step 18.

18 Click on the OK button. The CompositeService - *Service Name* (Edit) form closes and a dialog box appears.

19 Click on the Yes button to confirm the action. The Manage Composite Services form reappears with the new composite service displayed in the list.

20 Close the Manage Composite Services form.

Procedure 72-2 To modify a composite service using the component tree

Caution — Modifying parameters can be service-affecting.

Note — You can also modify composite service components and add service connectors from the flat topology view. Refer to Procedure 72-4.

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria. A list of composite services appears at the bottom of the Manage Composite Services form.

3 Select a composite service and click on the Properties button. The CompositeService - *Service Name* (Edit) form opens with the General tab displayed.

4 To configure parameters for an item, click on the Components tab, select and right-click on the item, and choose Properties from the contextual menu.

Using the contextual menu, you can also:

- Add SCs and connectors to a composite service
- Create services for inclusion in the composite service. When you create services by using the contextual menu, the services are automatically added to the composite service.
- Remove SCs and connectors from a composite service
- Move SCs to another composite service
- Delete SCs

Warning — Deleting an SC is not the same as removing an SC from a composite service. Deleting an SC removes the service from the 5620 SAM database. To avoid a service outage, be certain of the action that you are taking.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button to confirm the action. The CompositeService - *Service Name* (Edit) form closes and the Manage Composite Services form reappears.

7 Click on the Close button to close the Manage Composite Services form.

Procedure 72-3 To view the service topology

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria. A list of composite services appears at the bottom of the Manage Composite Services form.

3 Select a composite service and perform one of the following steps:

a Click on the Topology View button. A Composite Service Topology - *Service Name* map opens.

b Click on the Topology View Flat button. A Composite Service Flat Topology - *Service Name* map opens. The Flat Topology map is a flattened view of a composite service, meaning that all the service objects are displayed simultaneously, along with the service sites, access interfaces, and the links or groups of links between them.

See chapter 4 for more information about composite service topology views.

Procedure 72-4 To modify a composite service using the flat topology view

You can modify composite service components and add service connectors from the flat topology view. The main advantage of creating connectors using the flat topology view is that most of the parameters in the associated configuration forms are automatically populated when you select an item in the map.

Caution — Modifying parameters can be service-affecting.

Note — You can also modify and add composite service components using the component tree. Refer to Procedure 72-2.

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Configure the filter criteria. A list of composite services appears at the bottom of the Manage Composite Services form.

3 Select a composite service and click on the Properties button. The CompositeService - *Service Name* (Edit) form opens with the General tab displayed.

4 Click the Flat Topology View button. The Composite Service Flat Topology map opens.

5 To configure parameters for any item on the map, right-click on the item, and choose Properties from the contextual menu. The configuration form for the item is displayed.

6 Edit the parameters as required. Refer to Procedure 72-1 for detailed configuration information on creating and configuring components.

7 You can also add service connectors from the flat topology view.

Depending on the sites or ports you select, when you right-click on a component, the contextual menu contains one or more of the following choices:

- Create Cross Connect. Go to step 8.
- Create Routed Vpls Connector. Go to step 9.
- Create Scp Connector. Go to step 10.
- Create Spoke Connector. Go to step 11.

Click on the required item in the contextual menu and proceed to the associated step indicated in this list.

Note — If you need to modify any of the automatically-populated parameters in the associated configuration forms while creating these connectors, refer to Procedure 72-2 for detailed information.

8 To create a Cross Connect Connector:

i Select the two site icons that you want to create the Cross Connect Connector for. These icons represent the same physical NE that exists in two separate services, since service endpoints of a Cross Connect Connector must be on the same NE.

ii Right-click on either of the icons and select Create Cross Connect from the contextual menu.

The CrossConnect (Create) form opens with the General tab page displayed.

iii Configure the parameters.

- Name
- Description (optional)

iv Click on the Transport tab button.

v Click on the Select button to choose a CCAG for the connector. The Select CCAG - Cross Connect form opens with a list of available CCAGs displayed.

vi Select a CCAG and click on the OK button. The Select CCAG - Cross Connect (Create) form closes and the CrossConnect (Create) form refreshes.

vii Click on the OK button. The CrossConnect (Create) form closes and the new Cross Connect Connector is displayed on the map.

viii Go to step 12.

9 To create a Routed Vpls Connector:

i Select a VPLS site icon and an L3 Access Interface icon that you want to create the Routed Vpls Connector for. These icons must belong to the same NE.

ii Right-click on either of the icons and select Create Routed Vpls Connector from the contextual menu.

The RoutedVplsConnector (Create) form opens with the General tab page displayed.

iii Configure the parameters.

- Name
- Description (optional)

iv Click on the OK button. The RoutedVplsConnector (Create) form closes and the new Routed Vpls Connector is displayed on the map.

v Go to step 12.

10 To create a Scp Connector:

i Select the port icons for the two sites that you want to create the Scp Connector for.

ii Right-click on either of the icons and select Create Scp Connector from the contextual menu.

The ScpConnector (Create) form opens with the General tab page displayed.

iii Configure the parameters.

- Name
- Description (optional)

iv Click on the OK button. The ScpConnector (Create) form closes and the new Scp Connector is displayed on the map.

v Go to step 12.

11 To create a Spoke Connector:

i Select the two site icons that you want to create the Spoke Connector for. These icons must be two different NEs that exist in two separate services.

ii Right-click on either of the icons and select Create Spoke Connector from the contextual menu.

The SpokeConnector (Create) form opens with the General tab page displayed.

iii Configure the parameters.

- Name
- Description (optional)

iv Click on the OK button. The SpokeConnector (Create) form closes and the new Spoke Connector is displayed on the map.

12 Click on the OK button in the CompositeService - *Service Name* (Edit) form. A dialog box appears.

13 Click on the Yes button to confirm your changes. The CompositeService - *Service Name* (Edit) form closes and the Manage Composite Services form reappears.

14 Click on the Close button to close the Manage Composite Services form.

Procedure 72-5 To delete a composite service

1 Choose Manage→Service→Composite Services from the 5620 SAM main menu. The Manage Composite Services form opens.

2 Use the configurable filter and Search button on the form to select the composite service that is to be deleted.

3 Click on the Delete button. A dialog box appears and prompts you to confirm that you understand the implications of deleting the service.

4 Click on the Yes button to confirm the action. The service is removed from the list and deleted.

5 Click on the Close button to close the Manage Services form.

73 — Application assurance

73.1 Application assurance overview

Application Assurance, or AA, is a service-enabling technology that is available for the 7450 ESS and 7750 SR. This technology enhances the existing hierarchical per-subscriber and per-service QoS capabilities with granular, per-AQP control. AA can be introduced in existing deployments of the Alcatel-Lucent TPSDA to evolve the HSI legacy into an EIS model that can support bandwidth-intensive Internet-based applications and content delivery.

AA enables deep packet inspection of subscriber traffic where policies are applied to HSI traffic on a per-subscriber basis to determine the action to perform on the traffic.

AA is applied to specific traffic on a per-subscriber basis. A subscriber can be associated with one of the following services:

- IES
- VPLS
- VLL
- VPRN

AA and dynamic subscriber policy control allow a broadband network to provide application-based subscriber management for Internet access. The following benefits for service providers are:

- content control of services
- control over network costs incurred by various uses of HSI
- complementary security aspects to existing network security
- improved QoS sophistication and granularity of the network
- ability to apply policy control on the transactions that traverse the network

The 5620 SAM can manage AA on all Release 7.0 or later 7450 ESS or 7750 SR chassis types except for the 7450 ESS-1 and 7750 SR-1. The 5620 SAM, Release 7.0 or later, does not support AA group policies from a release earlier than 7.0, or distribute AA components, such as policies, to NEs that are at a release earlier than 7.0. The 5620 SAM, Release 7.0 or later, uses an AA group policy instead of an AA profile policy.

Note — When you upgrade a 5620 SAM system from a release earlier than 7.0 to Release 7.0 or later, the existing AA components are automatically deleted from the 5620 SAM database.

NE traffic is selected to be processed by AA and then undergoes deep packet inspection on an ISA-AA MDA in the NE. See chapter 17 for information about using the 5620 SAM to configure an ISA-AA group that contains one or more ISA-AA MDAs.

You can configure Cflowd on an ISA-AA group. AA Cflowd supports basic Cflowd sampling as well as TCP performance data collection for AA applications and application groups. Each ISA-AA group supports one Cflowd instance.

You must enable Cflowd globally on an NE before you can configure AA Cflowd collectors. Each collector is deleted when Cflowd is disabled. See chapter 17 for information about enabling and configuring global Cflowd on an NE, and for information about enabling and configuring AA Cflowd on an ISA-AA group.

Note — AA policies can only be configured on an NE if an ISA-AA group is already configured on the system.

The two elements of AA processing are:

- identification of the traffic on a per-flow or per-session basis
- policy treatment of the identified traffic

Functional components

The 5620 SAM supports the creation and configuration of AA components using configuration forms and scripts.

Figure 73-1 shows the AA functional components.

Figure 73-1 AA functional components

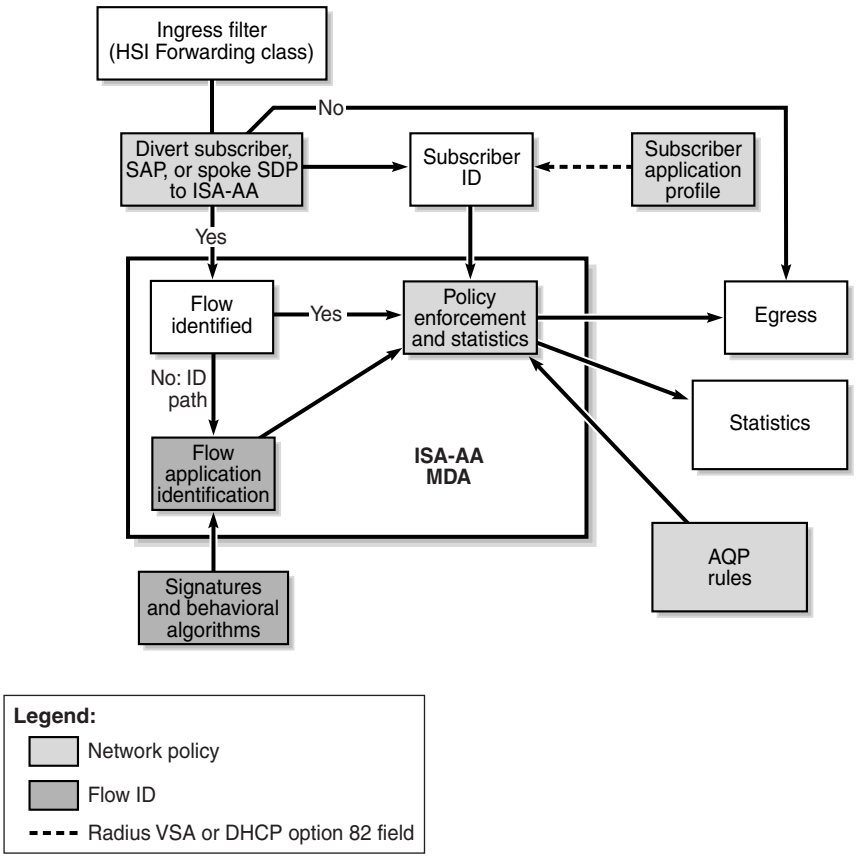
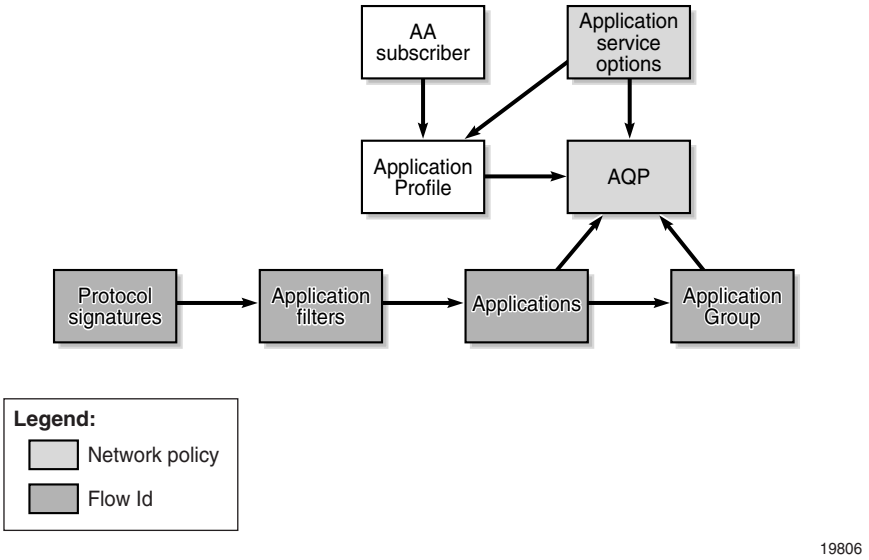


Figure 73-2 shows the relationship between the AA components that are used to identify applications and configure AA-related capabilities.

Figure 73-2 AA policy structure



AA protocol signatures

The 5620 SAM generates a set of signatures that identify AA protocols. The signature set includes:

- protocol support summary—list of protocols that can be identified with the load using a combination of pattern and behavioral techniques. The protocols are used to generate statistics by protocol and as input in combination with other information to identify applications.
- pattern signatures—set of pattern-match signatures used in analysis
- behavior signatures—set of diagnostic techniques used in analysis

Dynamic upgrades of protocol signatures are implemented by using an admin application-assurance upgrade command and then performing ISA-AA activity switches. Protocol signatures are updated as part of an ISSU that only updates ISA-AA software. Signature upgrades without an NE upgrade can be performed within a major release independent of system ISSU limits.

Because protocol signatures are intended to be the most basic block of application identification, other AA components, such as application filters, are provided to further customize protocol signatures. Customization reduces the need for a new protocol signature load when a new application may need to be identified.

Each protocol can be referenced in the definition of one or more applications by the application filter definition. The assignment of each supported protocol to an application filter or application is optional, allowing for the addition of new signature protocols without the need to update the application filter and applications.

Protocol shutdown

The 5620 SAM supports signature upgrades without automatically affecting policy behavior. All post-R1 new signatures are disabled, by default, during an upgrade to ensure that policies or services are not affected.

The protocols that are included in R1 of a release are designated as parent signatures and cannot be disabled. Within a major release, all protocols introduced after R1 of a release as part of an isa-aa.tim ISSU are, by default, shut down. The protocols must be enabled on a per-protocol basis to take effect. When shut down, protocols introduced after R1 do not change AA behavior. For example, traffic maps to the parent protocol on which the new signature is based. Enabling or disabling a new protocol takes affect for new flows only.

AA group policies

An AA group policy includes the following components:

- application filters
- applications
- application groups
- application profiles
- application service options
- application QoS policies
- custom protocols

Application filters

Application filters are provided as an indirect action between protocols and applications to allow the addition of variable parameters (for example, port numbers and IP addresses) to an application definition. Application filters are numbered rule entries that define the use of protocol signatures and other application criteria. Multiple application filter entries can be used to define an application, but each application filter entry maps to one application.

A traffic flow may have multiple rules. The rule with the lowest entry number that matches is applied. A traffic flow can only be assigned to one application.

Applications

Applications define and assign a description to the application names that are supported by the application filter entries. Each application is associated with one of the application groups. Applications are used by AA to identify the type of IP traffic in the subscriber traffic.

The application name is a key match criterion within the AQP rules that are applied to the IP traffic of a subscriber.

One predefined application (“unknown”) is provided by AA. The unknown application cannot be modified. All other applications must be configured. An application must be configured before the associated application filter is defined.

Network operators can:

- change the application group that an application is associated with
- view which application filters are defining the application

Application groups

An application group is a container for multiple applications. A set of default application groups is provided by AA. At least one default application group ("unknown") must be associated with each NE. The default application groups cannot be modified.

Multiple applications can be assigned to an application group. An application can only belong to one group. Applications that are not assigned to an application group are automatically placed in the "unknown" application group.

Application profiles

Application profiles enable AA service for traffic to and from an ESM subscriber, SAP, or spoke SDP. Each application profile is unique and defines the AA service that the AA subscriber receives. The type of traffic is configured in the system-wide configuration of QoS forwarding classes to be diverted to the ISA-AA MDA for subscribers with AA enabled. The forwarding class is used for any subscriber traffic that a service provider needs to inspect using AA.

An ESM subscriber can be assigned to an application profile that affects every host of the subscriber. For SAP or spoke SDP AA subscribers, an application profile can be assigned that affects the traffic originating from or destined over the SAP or spoke SDP.

For subscribers with application profiles that enable AA, traffic is diverted to the active ISA-AA MDA using ingress QoS policy filters. The filters identify forwarding and sub-forwarding classes that can be diverted for AA. The system identifies and diverts only traffic for any subscriber who is treated by the ISA-AA MDA, according to the application profile of the subscriber. Diversion to the ISA-AA MDA depends on the ISA-AA MDA status. If a subscriber is not configured to divert traffic to the ISA-AA MDA, normal ingress forwarding occurs.

The characteristics of application profiles are:

- By default, subscribers are not assigned to an application profile and traffic is not diverted for AA analysis.
- One or more application profiles can be configured.
- Application profiles are customer-defined and created using the configured application service options characteristics.
- Local instances of the application profile are configured to bind to specific objects of an NE (for example, L2 access interface, SAP, local subscriber explicit map entry, and so on).
- Application profiles can only be assigned when ISA-AA cards are assigned to an ISA-AA group
- Global application profiles must be manually distributed to the NEs.
- Application profiles can be assigned a capacity cost for subscriber load balancing among ISAs within the AA group.

ASOs

Application service options (ASOs) are used to define service provider and customer network functionality that is common among sets of subscribers. ASOs prevent subscribers from requiring each subscriber-specific entry in the application QoS policies for standard network services.

In a typical application, ASOs define the HSI service parameters.

- ASOs are optional; AA can check the subscriber IP traffic without the use of application service options.
- ASOs can be configured for each AA group policy.
- ASOs are a series of user-defined application characteristics.
- ASO characteristics are used to create application profiles and provide information to user-defined AQP rules.
- The set of ASOs represent network-wide menus of service capabilities that are available to subscribers.

Some examples of ASOs are:

- entry for each application group to be managed; for example, VoIP, P2P, and HTTP
- multiple entries (typically less than 20) where specific applications in an application group can be individually managed as service parameters; for example, HTTP content from a specific content provider or streaming video from network television or games
- HSI tiers (for example, Gold, Silver, and Bronze) that specify bandwidth levels
- bandwidth parameters for each service option

ASO characteristics are used:

- as input to application profiles
- by application QoS policies to influence how specific traffic is checked and how policies are applied

ASOs are defined and assigned to one or more values to define service offerings to customers.

You can configure ASO characteristics for an AA subscriber using an AA subscriber policy override. An AA subscriber policy override can be configured for a SAP or spoke SDP binding, but not for an ESM subscriber. The AA subscriber must have an application profile assigned, or the subscriber policy override is rejected.

You can retrieve on demand the ASO values that are assigned to an AA subscriber from the Edit form of the SAP or spoke SDP binding AA subscriber.

AQPs

Application Qos Policies, or AQPs, are lists of rules that define the match criteria and action to be performed on all traffic flows. The AQP rules use as the match criteria the application groups, applications, and so on. The output of the AQP rules defines the policy actions to perform.

AQP rules consist of match and action criteria:

- Match—Refers to the application identification determined by the application and application group configuration using protocol signatures and user-configurable application filters. The protocol signatures and user-configurable application filters allow customers to create a wide range of applications.
- Action—Defines AA actions to be applied to traffic. For example, you can apply a set of actions such as bandwidth policing, packet discards, QoS remarking, and flow count, and/or rate limiting to a flow.

Custom protocols

Custom protocols are supported using configurable strings (up to 16 hexadecimal octets) for pattern-matched application identification in the payload of TCP- or UDP-based applications. The match is specified for the client-to-server, server-to-client, or any direction for TCP based applications, and in the "any" direction for UDP-based applications.

You can configure a custom protocol description, custom protocol ID and shutdown. When a custom protocol's administrative status is disabled, traffic is identified as if the protocol is not configured

Custom protocols and Alcatel-Lucent-provided protocols are functionally equivalent. Custom protocols are used in the application definition without limitations. All application filter entries, except strings, are supported. Custom protocol statistics collection on an ISA-AA partition group or special study subscriber is supported.

Policy Sync Group

Use the Policy Sync Group menu option to designate an AA group policy as the master policy and add one or more AA group policies to Policy Sync Group members. You can overwrite or add the contents of the master policy to one or more of its members.

AA policers

AA policers can be bandwidth or flow limiting, and can have one of the following scopes:

- system scope—limits all traffic entering the ISA-AA MDA
- subscriber scope—limits apply to the traffic of a subscriber

After a policer is referred to by an AQP for one traffic direction, the same policer cannot be referred to in the other direction. AQP rules with policer actions must specify a traffic direction other than "both".

AA accounting policies

The AA accounting statistics provide information required to understand the application use in a network. You can configure AA accounting to collect and report statistics when at least one ISA-AA MDA is active. The AA accounting statistics provide information about application use on a SAP or spoke SDP, or by a subscriber during a collection interval. The collected information can be viewed in graphical or tabular form using the 5620 SAM GUI, or sent to a module such as the 5670 RAM for reporting and trend analysis.

AA accounting collects statistics on traffic flows. The 5620 SAM can collect the following AA statistics types:

- AA application
- AA application group
- AA protocol
- AA subscriber protocol (special-study)
- AA subscriber application (special-study)
- AA subscriber custom record

AA uses the existing 5620 SAM and NE accounting statistics and logging capabilities to collect statistics. See the *5620 SAM Statistics Management Guide* for general information about configuring and collecting accounting statistics. See Procedure 73-5 for information about configuring an AA accounting policy.

The 5620 SAM can be configured to generate statistics for each protocol and application for a specific subscriber. You can enable AA statistics collection on a specific NE for a subset of subscribers for detailed traffic monitoring. An NE can have one policy for each AA statistics type that is enabled.

The AA subscriber protocol and AA subscriber application statistics are special study statistics for detailed accounting statistics collection on a limited number of subscribers, SAPs , or spoke SDPs on an NE. The number of subscribers, SAPs, or spoke SDPs is limited to constrain the volume of generated statistics.

Special study statistics are enabled by adding subscribers, SAPs, or spoke SDPs to a list in an ISA-AA group on an NE for AA debugging purposes. When a subscriber is on a special study list, the ISA-AA creates one statistics record for each application and application group that is associated with the subscriber. When a SAP or spoke SDP is on a special-study list, the ISA-AA creates one statistics record for each application, application group, and protocol flow on the SAP or spoke SDP. See Procedure 17-17 for information about configuring special study objects in an ISA-AA group.

An AA custom record subscriber accounting policy applies to all subscribers, SAPs and spoke SDPs in an ISA-AA group for a specified set of AA protocols, applications, and application groups. The policy enables statistics collection on only the specified objects, which limits the volume of collected data and the statistics collection processing load. For example, a 5620 SAM operator may require statistics for only three application groups and 10 applications. You can view and configure the AA statistics objects from the AA Subscriber Stats Objects tab on the properties form of an ISA-AA group.

AA flow watermark policy

AA supports the configuration of high and low thresholds (watermarks) for logs and traps when there is a high consumption of the flow table. The flow table has a limited size and the thresholds are established to alert users that the flow table is approaching maximum capacity. When the high threshold is reached, an alarm is generated. The alarm is cleared when the flow table capacity has dropped below the specified low threshold.

ISA-AA groups and partitions

The 5620 SAM supports ISA-AA partitions. Each partition is an object with its own AA policy. You can partition an AA group into AA policy partitions with one partition for each VPN-specific AA service. The partition supports VPN-specific custom protocols, applications, application group definitions, policy definitions and reporting. Each partition policy can be divided into multiple application QoS policies using ASOs. Multiple ISA-AA groups are used to scale the number of VPN-specific AA policies.

Multiple ISA-AA groups

The following operations can be performed at the ISA-AA group level

- Define one or more ISA-AA groups to allow AA resource partitioning and reservation of different types of AA service.
- Assign physical ISA-AAs to a group.
- Specify forwarding classes to be diverted for inspection by the AA subscribers that belong to the group and choose the AA policy to be applied to the group.
- Configure redundancy and bypass mode features to protect against equipment failure.
- Configure QoS on IOMs that host ISA-AA traffic.
- Configure ISA capacity planning using low and high thresholds.
- Enable ISA-AA partitions for ISA-AA groups.

Residential services are an example where all AA services can be configured as part of a single group that encompasses all ISA-AAs. The configuration provides the management of common applications and reporting for all subscribers and services, with common or per-customer AQP (uses ASO characteristics to divide the AQP of the ISA-AA into per-application profile QoS policies).

Multiple ISA-AA groups can also be used to create separate services based on different sets of common applications, traffic diversion needs, or different redundancy models. Multiple ISA-AA groups can be used for:

- a mix of residential and business customers
- different business VPN verticals
- business services with a common template base but different levels of redundancy, forwarding class diversion, or scaling over what is supported per single group

ISA-AA partitions

ISA-AA groups and partitions improve the scaling of policies. If partitions are not configured, the ISA-AA group acts as a single partition. When partitions are configured, application identification, and policy and statistics configuration apply only to the partition and not any other partitions that are configured under the same AA group. Although the definition of application profiles and related ASO characteristics is in the context of a partition, the application profile names must be unique for the NE. Definition of applications, application groups, and AQPs are also specific and only apply to a specific partition.

The following operations can be performed at the ISA-AA partition level

- Define unique applications and application groups per partition.
- Define AQP policies per partition.
- Define common applications and application groups with per partition processing and accounting.

ISA-AA partitions support accounting and customized reporting for every AA subscriber associated with a partition. You can perform the following operations:

- Define different types of reporting and accounting policies for different partitions in a single AA group.
- Display AA group level protocol statistics with partition visibility (for example, you can view protocol counts that are reported for each partition of the group).

When you create or delete an ISA-AA partition, a default AA accounting policy is automatically created in or deleted from the ISA-AA partition. See Procedure 17-17 for information about how to create and configure ISA-AA groups and partitions.

73.2 Workflow to configure application assurance

1. Create the AA Policer and the AQPs.
2. Configure the AA group policy to distinguish the HSI traffic.
3. Create an AA accounting policy to specify when statistics are to be collected on the ISA-AA MDA.
4. Assign subscribers to “special study” AA collection tables, if required.
5. Distribute the AA policies.

73.3 Application assurance procedures

Use the following procedures to configure AA.

Procedure 73-1 To create an AA policer policy

1. Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Manage Application Assurance Policies form opens.
2. Choose AA Policer (Application Assurance) from the object drop-down list

3 Click on the Create button and choose Create AA Policer. The AA Policer (Create) form opens with the General tab displayed.

4 Configure the parameters:

- ISA-AA Group ID
- Displayed Name
- Type
- Granularity
- Description

Note — The distribution of an AA policer fails if the ISA-AA group ID it refers to does not exist on the NE.

5 Perform one of the following:

a If the Type parameter was set to Dual Bucket Bandwidth, go to step 7.

b If the Type parameter was set to Flow Count Limit, configure the Flow Count (flows) parameter.

c If the Type parameter was set to Flow Rate Limit, go to step 9.

d If the Type parameter was set to Single Bucket Bandwidth, go to step 11.

6 Go to step 12.

7 Configure the parameters:

- MBS (KB)
- CBS (KB)
- PIR (Kbps)
- CIR (Kbps)
- PIR
- CIR

8 Go to step 12.

9 Configure the parameters:

- MBS (flows)
- PIR (Kbps)
- PIR

10 Go to step 12.

11 Configure the parameters:

- Action
- MBS (KB)
- PIR (Kbps)
- PIR

12 Click on the OK button to close the AA Policer (Create) window.

13 Close the Manage Application Assurance Policies form.

Procedure 73-2 To create an AQP

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Manage Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list and click on the Search button. A list of AA group policies is displayed.

Note — The 5620 SAM does not create local AA Group policies for each applicable managed NE. Instead, the local AA Group Policy is created/deleted when the ISA-AA group is created/deleted.

3 Select the policy in the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

4 Click on the Application QoS Entries tab button.

5 Click on the Add button. The Application QoS Policy (create) form opens with the General tab displayed.

6 Configure the parameters:

- Entry ID
- Description
- Administrative State

7 Click on the Match Criteria tab button.

8 Configure the parameters:

- Traffic Direction
- Application Operator

9 Click on the select button beside the Displayed Name parameter in the Application panel. The Select Application Name - Application QoS Policy list form opens.

10 Select an application from the list and click on the OK button. The Select Application Name - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Displayed Name information.

11 Configure the Application Group Operator parameter.

12 Click on the select button beside the Displayed Name parameter in the Application panel. The Select Application Group Name - Application QoS Policy list form opens.

13 Select an application group from the list and click on the OK button. The Select Application Group Name - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Displayed Name information.

14 Configure the parameters in the DSCP panel:

- DSCP Operator
- DSCP

15 Click on the AA Subscriber tab button.

16 Configure the SubscriberType parameter.

Note 1 — The SAP and Spoke SDP Binding options are valid for the SubscriberType parameter only when you create a local AQP entry.

Note 2 — If the SubscriberType parameter is set to None, the values of all parameters on the AA Subscriber tab are reset.

17 Perform one of the following:

a If the SubscriberType parameter is set to ESM, go to step 18.

b If the SubscriberType parameter is set to SAP, go to step 20.

c If the SubscriberType parameter is set to Spoke SDP Binding, go to step 21.

d If the SubscriberType parameter is set to None, go to step 22.

18 Configure the parameters:

- ESM Subscriber Operator
- ESM Subscriber

19 Go to step 22.

20 Configure the parameters:

- SAP Subscriber Operator
- Port ID

21 Configure the parameters:

- Spoke SDP Binding Subscriber Operator
- Tunnel ID

22 Click on the Source and Destination tab button.

23 Configure the parameters in the Source Address panel:

- Address Operator
- Address
- Address Length

24 Configure the parameters in the Source Port panel:

- Port Operator
- Port Value Type
- Port Value/Low Value
- Port High Value

25 Configure the parameters in the Destination Address panel:

- Address Operator
- Address
- Address Length

26 Configure the parameters in the Destination Port panel:

- Port Operator
- Port Value Type
- Port Value/Low Value
- Port High Value

27 Click on the Characteristics tab button.

28 Click on the Add button.

29 Configure the parameters:

- ASO Characteristic
- ASO Characteristic Operator
- ASO Characteristic Value

30 Click on the Action tab.

31 Configure the Drop parameter.

32 Click on the Select button beside the Displayed Name parameter in the Bandwidth Limit Policer panel. The Select Bandwidth Limit Policer - Application QoS Policy list form opens.

33 Select a bandwidth limit policer from the list and click on the OK button. The Select Bandwidth Limit Policer - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Displayed Name information.

34 Click on the Select button beside the Displayed Name parameter in the Flow Rate Limit Policer panel. The Select Flow Rate Limit Policer - Application QoS Policy list form opens.

35 Select a flow rate limit policer from the list and click on the OK button. The Select Flow Rate Limit Policer - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Displayed Name information.

36 Click on the Select button beside the Displayed Name parameter in the Flow Count Limit Policer panel. The Select Flow Count Limit Policer - Application QoS Policy list form opens.

37 Select a flow count limit policer from the list and click on the OK button. The Select Flow Count Limit Policer - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Displayed Name information.

38 Click on the Select button beside the Service ID parameter in the Mirror Source panel. The Select Service ID - Application QoS Policy list form opens.

39 Select a mirror service from the list and click on the OK button. The Select Service ID - Application QoS Policy list form closes and the Application QoS Policy (create) form is refreshed with the Service ID information.

Note — The Service ID parameter can only be configured when creating a local AQP entry.

40 Configure the parameters:

- Mirror Source All Inclusive
- Forwarding Class
- Priority
- Remark DSCP In Profile
- Remark DSCP Out Profile

41 Click on the OK button to close the Application QoS Policy (create) form.

42 Click on the OK button to close the AA Group Policy (Edit) form.

43 Close the Manage Application Assurance Policies form.

Procedure 73-3 To configure an AA group policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Manage Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list and click on the Search button. A list of AA group policies is displayed.

Note — The 5620 SAM does not create local AA Group policies for each applicable managed NE. Instead, the local AA Group Policy is created/deleted when the ISA-AA group is created/deleted.

3 Select the policy in the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

4 Configure the Description parameter.

5 Perform the following steps to create an application group.

i Click on the Application Groups tab button. One default application group is displayed.

ii Click on the Add button. The Application Group (Create) form opens.

Note — You can also create an application group from the AA Identification Components tab of the AA Group Policy (Edit) form by selecting Application Groups and using the right-click contextual menu. This tab also allows for the deletion, modification, and resynchronization of Application Groups.

iii Configure the parameters:

- Displayed Name
- Description

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The AA Group Policy (Edit) form reappears.

6 Repeat step 5 to create an additional application group, if required.

7 Perform the following steps to create an application.

i Click on the Applications tab button. One default application is displayed in the form.

ii Click on the Add button. The Application (Create) form opens.

Note — You can also create an application from the AA Identification Components tab of the AA Group Policy (Edit) form by selecting Applications and using the right-click contextual menu. This tab also allows for the deletion, modification, and resynchronization of Applications.

iii Configure the parameters:

- Displayed Name
- Description

iv Click on the Application Groups tab button.

v Click on the Select button in the Application Group panel to choose an application group. The Select Application Group search form opens.

vi Select an application group in the list and click on the OK button. The Select Application Group form closes and the application group information appears on the Application (Create) form.

vii Click on the 5670 RAM Parameters tab button.

Note — The 5670 RAM can perform an application performance index analysis on an AA application. An application performance index configuration is not distributed to an NE as part of a policy distribution.

The 5670 RAM provides a comparative analysis of TCP and UDP application usage. For each application, you can specify whether the application is TCP or UDP. TCP or UDP data is not distributed to an NE as part of a policy distribution.

viii Configure the parameters:

- Application Flag
- Network Delay Tolerated Threshold (milliseconds)
- Network Delay Frustrated Threshold (milliseconds)
- Network Delay Weight
- Network Delay Variation Tolerated Threshold (milliseconds)
- Network Delay Variation Frustrated Threshold (milliseconds)
- Network Delay Variation Weight
- Packet Loss Tolerated Threshold (%)
- Packet Loss Frustrated Threshold (%)
- Packet Loss Weight
- Total Delay Tolerated Threshold (milliseconds)
- Total Delay Frustrated Threshold (milliseconds)
- Total Delay Weight

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The AA Group Policy (Edit) form reappears.

8 Repeat step 7 to create an additional application, if required.

9 Perform the following steps to create an application filter.

i Click on the Application Filters tab button.

ii Click on the Add button. The Application Filter (Create) form opens.

Note — You can also create an application filter from the AA Identification Components tab of the AA Group Policy (Edit) form by selecting Application Filters and using the right-click contextual menu. This tab also allows for the deletion, modification, and resynchronization of Application Filters.

iii Configure the parameters:

- Entry ID
- Description
- Administrative State

iv Click on the General Properties tab button.

v Configure the parameters:

- Flow Set-up Direction
- IP Protocol Operator
- IP Protocol Number
- Protocol Operator
- Protocol Type
- Server Address Operator
- Server Address
- Server Address Mask
- Server Port Operator
- Server Port Value Type
- Server Port/Low Value
- Server Port High Value
- Server Port First Packet Policy

vi Click on the Select button in the Protocol panel to choose a protocol. The Select Protocol form opens.

vii Select a protocol in the list and click on the OK button. The Select Protocol form closes and the protocol information appears on the Application Filter (Create) form.

viii Click on the Select button in the Protocol panel to choose a custom protocol name. The Select Custom Protocol form opens.

ix Select a custom protocol in the list and click on the OK button. The Select Custom Protocol form closes and the protocol information appears on the Application Filter (Create) form.

x Click on the Application tab button.

xi Click on the Select button in the Application panel to choose an application. The Select Application search form opens.

xii Select an application in the list and click on the OK button. The Select Application form closes and the application information appears on the Application Filter (Create) form.

xiii Click on the Application Filter Expressions tab button.

xiv Click on the Add button. The Application Filter Expression (Create) form opens.

xv Configure the parameters:

- Index
- Type
- Operator
- String

xvi Click on the OK button. The Application Filter Expression (Create) form closes and the expression information appears on the Application Filter (Create) form.

xvii Repeat step 9 xiv to xvi to create an additional application filter expression, if required. The maximum number of application filter expressions that can be created is 3.

xviii Click on the OK button. A dialog box appears.

xix Click on the OK button. The Application Filter (Create) form reappears.

10 Repeat step 9 to create an additional application filter, if required.

11 Perform the following steps to create an application service option.

i Click on the Application Service Options tab button.

ii Click on the Add button. The Application Service Option (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Displayed Name
- ASO Characteristic Default Value

iv Click on the Application Service Option Value Entries tab button.

v Click on the Add button. The Application Service Option Value Entry (Create) form opens.

vi Configure the ASO Characteristic Value parameter.

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Application Service Option Value Entry (Create) form closes and the entry information appears on the Application Service Option (Create) form.

ix Repeat steps 11 iv to viii to create an additional application service option value entry.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The AA Group Policy form reappears.

12 Repeat step 11 to create an additional application service option.

13 Perform the following steps to create an application profile.

i Click on the Application Profiles tab button.

ii Click on the Add button. The Application Profile (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Displayed Name
- Description
- Divert
- Capacity Cost

iv Click on the Characteristics tab button.

v Click on the Add button. The Application Profile Characteristic (Create) form opens.

vi Click on the Select button beside the ASO Characteristic parameter. The Select Application Service Option search form opens.

vii Select an application service option in the list and click on the OK button. The Select Application Service Option form closes and the application service option information appears on the Application Profile Characteristic form.

viii Click on the Select button beside the ASO Characteristic Value parameter. The Select Application Service Option Characteristic Value search form opens.

ix Select an ASO characteristic value in the list and click on the OK button. The Select Application Service Option Characteristic Value form closes and the ASO characteristic value information appears in the Application Profile Characteristic form.

x Click on the OK button. A dialog box appears.

xi Click on the OK button. The Application Profile Characteristic (Create) form closes and the entry information appears on the Application Profile (Create) form.

xii Repeat steps 13 v to xi to create an additional application profile characteristic, if required.

xiii Click on the OK button. A dialog box appears.

xiv Click on the OK button. The AA Group Policy form reappears.

14 Repeat step 13 to create an additional application profile, if required.

15 Create custom protocols.

i Click on the Custom Protocols tab button.

ii Click on the Add button. The Custom Protocol (Create) form opens with the General tab displayed.

iii Configure the parameters:

- Entry ID
- Description
- IP Protocol Number
- Administrative State

iv Click on the Custom Protocol Expressions tab button.

v Click on the Add button. The Custom Protocol Expressions (Create) form opens.

vi Configure the parameters:

- Index
- Custom Protocol Expression Offset
- Custom Protocol Expression Direction
- Operator
- String

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The Custom Protocol Expression (Create) form closes and the entry information appears on the Custom Protocol (Create) form.

ix Click on the OK button. The AA Group Policy form reappears.

16 Modify a local instance of an AA group policy, as required.

i Click on the Local Definitions tab. The AA policies for each managed NE are listed.

ii Select an AA policy in the list and click on the Properties button to modify the local instance of the policy.

iii Perform steps 4 to 14. Go to step 17.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The AA Group Policy form closes and the Manage Application Assurance Policies form reappears.

19 Close the Manage Application Assurance Policies form.

Procedure 73-4 To create a policy sync group

1 Choose Policies→Policy Sync Group from the 5620 SAM main menu. The Policy Sync Groups form opens.

2 Perform the following steps to create a Policy Sync Group.

i Click on the Create→Create Policy Sync Group. The Policy Sync Group (Create) form opens.

ii Configure the parameters:

- Auto-Assign ID
- Description
- Displayed Name

iii Click on the Select button in the Master Policy panel to choose a master policy. The Select Master Policy - Policy Sync Group form opens.

iv Choose a master policy in the list and click on the OK button. The Select Master Policy - Policy Sync Group closes and the Policy Sync Group (Create) form reappears.

v Click on the OK button. The Policy Sync Group Manager form reappears.

3 Add a member to a master AA group policy.

i From the Policy Sync Group Manager form, choose a Policy Sync Group from the list and click on the Properties button. The Policy Sync Group (Edit) form opens with the General tab displayed.

ii Click on the Members tab.

iii Click on the Add button. The Select AA Group Policy - Policy Sync Group form opens.

iv Choose one or more AA group policies in the list and click on the OK button. A dialog box appears.

v Choose one of the options and click on the OK button. The Select AA Group Policy - Policy Sync Group form closes and the member is displayed on the Policy Sync Group (Edit) form.

Note 1 — The Sync Members button performs the same function as the "Listed master policy classes will overwrite member classes" option. The Add to Members button performs the same function as the "Listed master policy classes will be added to member classes" option.

Note 2 — The Sync Members, Add to Members, and Update Master actions performed on an AA group policy only affect the classes listed under the Included Classes tab button.

4 Audit and compare a master AA group policy and its members for the classes listed under the Included Classes tab.

Note 1 — The Audit button displays the differences between a master AA group policy and its members.

Note 2 — The Compare button compares two selected policies between master-member, or member-member.

Note 3 — The Update Master button adds the contents of a selected AA group policy to the included classes of a master policy.

i Click on the Audit button. A dialog box appears.

ii Click on the Yes button. An Audit dialog box appears.

iii Click on the OK button.

iv View the alarm window to display the alarms raised against the member policy, if required.

5 Compare and view detailed differences between two policies.

i Hold down the Shift key to choose two policies in the list and click on the Compare button. The Compare - AA Group Policy form opens.

ii Click on the Compare button to view the differences between Policy A and Policy B.

Note 1 — You can use the Swap button to switch Policy A and Policy B.

Note 2 — You can use the Difference drop-down menu to choose a category that you need to filter on.

iii Choose a result and and click on the Properties button. The Difference - AA Group Policy (*class type*) form opens.

iv View the differences between the two policies.

Note — After a Sync Member or Add to Member action, the member policy mode changes to Draft. When the policy is in Draft mode, you must first release the policy for distribution. Releasing the global policy also distributes the policy to existing local definitions. See chapter 43 for more information.

Procedure 73-5 To configure an AA accounting policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Manage Application Assurance Policies form opens.

2 Choose AA Accounting Policy (Application Assurance) from the object drop-down list.

3 Perform one of the following:

a To create an AA accounting policy, click on the Create button and choose Create AA Accounting Policy from the drop-down menu. The AA Accounting Policy (Create) form opens.

b To modify an AA accounting policy:

i Click on the Search button. The AA accounting policies are displayed.

ii Select an AA accounting policy in the list and click on the Properties button. The AA Accounting Policy (Edit) form opens.

4 Configure the parameters:

- Group ID
- Partition ID
- Description

5 Click on the Apply button. The form displays additional tabs.

6 Click on the Accounting Policies tab button. A list of accounting policies is displayed.

7 Configure each accounting policy in the list, if required.

i Select the accounting policy and click on the Properties button. The AA Accounting Configuration form is displayed.

ii Configure the parameters:

- Description
- Collect Accounting Statistics

iii Click on the Select button to choose an accounting policy. The Select Accounting Policy form opens.

iv Select an accounting policy in the list and click on the OK button. The Select Accounting Policy form closes and the accounting policy information appears on the AA Accounting Configuration form.

v Click on the OK button. The AA Accounting Configuration (Edit) form closes.

8 Click on the Apply button. A dialog box appears.

9 Click on the Yes button.

10 Click on the General tab button.

11 Click on the Switch Mode button. A dialog box appears.

12 Click on the Yes button.

13 Click on the Distribute button to manually distribute the policy to one or more NEs. The Distribute - AA Accounting form opens.

14 Select one or more NEs in the Available Nodes panel to which you want to distribute the policy and click on the right arrow. The NEs move to the Selected Nodes panel.

15 Click on the Distribute button. The policy is distributed to the NEs.

16 Modify a local instance of the AA accounting policy, if required.

i Click on the Local Definitions tab button. The AA accounting policies for each managed NE are listed.

ii Select an AA accounting policy in the list and click on the Properties button to modify the local instance of the policy. The AA Accounting Configuration (Edit) form opens.

iii Click on the Switch Mode button.

iv Perform steps 4 to 12.

17 Click on the OK button. The AA Accounting Configuration (Edit) form closes and the Manage Application Assurance Policies form reappears.

18 Close the Manage Application Assurance Policies form.

Procedure 73-6 To configure an AA flow watermark policy

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Manage Application Assurance Policies form opens.

2 Choose AA Flow Watermark (aapolicy) from the object drop-down list.

3 Specify a filter to create a filtered list of flow watermark configurations, and click on the Search button. A list of flow watermark configurations is displayed.

4 Select an entry in the list and click on the Properties button. The AA Flow Configuration form opens.

5 Configure the parameters:

- Flow Full High Watermark
- Flow Full Low Watermark

6 Modify a local instance of the AA flow watermark configuration, if required.

i Click on the Apply button.

ii Click on the Local Definitions tab. The AA flow watermark configurations for each managed NE are listed.

iii Select a managed NE in the list and click on the Properties button to modify the local instance of the flow configuration.

iv Perform step 5.

v Click on the OK button. The Application Assurance Flow Configuration form closes.

7 Click on the OK button. The Application Assurance Flow Configuration form closes and the Manage Application Assurance Policies form reappears.

8 Close the Manage Application Assurance Policies form.

Procedure 73-7 To view AA summary information for subscribers, SAPs, and spoke SDPs on ISA-AA MDAs

If the ISA-AA group is partitioned, the AA summary tabs appear on the partition. This information is typically used for AA debugging purposes. You can view debug statistics information on the Statistics tab of an AA object. Because the AA summary information, especially the subscriber-based information, can change frequently, the summary information may not be current. If an object that is of interest is not displayed, you can resynchronize the ISA-AA group to refresh the list.

Caution — Alcatel-Lucent recommends that you consider the effect of resynchronizing an ISA-AA group. Resynchronizing an ISA-AA group typically involves the retrieval of a significant amount of information and may affect NE performance.

Note — You can view AA statistics using Stats Interval. Stats Interval allows you to choose realtime or snapshot for collecting AA statistics. Realtime specifies that the statistics retrieved include the sum of the statistics from the previous collection windows, the statistics for any closed flows since the last collection window, and the statistics accumulated from any currently open flows. Snapshot specifies that the statistics retrieved include the sum of the statistics from the previous collection windows, and the statistics for any closed flows since the last collection window.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose *device*→ISA-AA Groups→*ISA_group*.

3 Right-click on the ISA-AA Group icon and choose Properties. The ISA-AA Group (Edit) form opens.

4 Perform one of the following.

- **a** View the summary information for a subscriber.
  - **i** Click on the AA Subscriber Summary tab button. A list of subscribers is displayed.
  - **ii** Select an entry in the list and click on the Properties button. The AA Subscriber (Edit) form opens.
  - **iii** Click on the Properties button. The Residential Subscriber Instance (Edit) form opens.
- **b** View the summary information for a SAP.
  - **i** Click on the AA SAP Summary tab button. A list of SAPs is displayed.
  - **ii** Select an entry in the list and click on the Properties button. The AA SAP (Edit) form opens.
  - **iii** Click on the Properties button. The Access Interface (Edit) form opens.
- **c** View the summary information for a spoke SDP.
  - **i** Click on the AA Spoke SDP Binding Summary tab button. A list of spoke SDPs is displayed.
  - **ii** Select an entry in the list and click on the Properties button. The AA Spoke SDP Binding (Edit) form opens.
  - **iii** Click on the Properties button. The Access Interface (Edit) form opens.

5 Click on the Statistics tab button.

6 Choose an AA statistics class from the object drop-down list.

7 Perform one of the following:

a Click on the Collect button to perform an on-demand collection of the current performance statistics data. The collected statistics entries are listed on the form.

b Click on the Collect All button to collect one on-demand statistics record for each statistic type that the object supports. The collected statistics entries are listed on the form.

8 Select an entry from the list and click on the Properties button. The Statistics Record form opens.

9 View the statistics data.

10 Close the Statistics Record form.

11 Close the subscriber, SAP, or spoke SDP properties forms.

Procedure 73-8 To view the AA special study statistics data

Perform this procedure to view the AA special study statistics data for subscribers, SAPs, or spoke SDPs on an ISA-AA MDA. If the ISA-AA group is partitioned, the AA special study tabs appear on the partition.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose *device*→ISA-AA Groups→*ISA_group*.

3 Right-click on the ISA-AA Group icon and choose Properties. The ISA-AA Group (Edit) form opens.

4 Perform one of the following.

a View the special study statistics for a subscriber.

i Click on the AA Special Study Subscribers tab button. A list of subscribers is displayed.

ii Select an entry in the list and click on the Properties button. The AA Special Study Subscriber Config (Edit) form opens.

iii Click on the Properties button. The Access Interface (Edit) form opens.

b View the special study statistics for a SAP.

i Click on the AA Special Study SAPs tab button. A list of SAPs is displayed.

ii Select an entry in the list and click on the Properties button. The AA Special Study SAP Config (Edit) form opens.

iii Click on the Properties button. The Access Interface (Edit) form opens.

c View the special study statistics for a spoke SDP.

i Click on the AA Special Study Spoke SDP Bindings tab button. A list of spoke SDPs is displayed.

ii Select an entry in the list and click on the Properties button. The AA Special Study Spoke SDP Binding Config (Edit) form opens.

iii Click on the Properties button. The Access Interface (Edit) form opens.

5 Click on the Statistics tab button.

6 Choose an AA statistics class from the object drop-down list.

7 Perform one of the following:

a Click on the Collect button to perform an on-demand collection of the current performance statistics data. The collected statistics entries are listed on the form.

b Click on the Collect All button to collect one on-demand statistics record for each statistic type that the object supports. The collected statistics entries are listed on the form.

8 Select an entry from the list and click on the Properties button. The Statistics Record form opens.

9 View the statistics data.

10 Close the Statistics Record form.

11 Close the subscriber, SAP, or spoke SDP forms.

Procedure 73-9 To view AA statistics data for ISA-AA groups or ISA-AA partitions

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose *device*→ISA-AA Groups→*ISA_group*.

3 Right-click on the ISA-AA Group icon and choose Properties. The ISA-AA Group (Edit) form opens with the General tab button displayed.

4 Perform one of the following:

a View AA statistics data for an ISA-AA group.

i Click on the Statistics tab button.

ii Choose an AA statistics class from the object drop-down list.

b Perform the following steps to view AA statistics data for an ISA-AA partition.

i Click on the ISA-AA Partitions tab button. A list of ISA-AA partitions is displayed.

ii Select an entry in the list and click on the Properties button. The ISA-AA Group Partition (Edit) form opens with the General tab button displayed.

iii Click on the Statistics tab button.

iv Choose an AA statistics class from the object drop-down list.

5 Perform one of the following:

a Click on the Collect button to perform an on-demand collection of the current performance statistics data. The collected statistics entries are listed on the form.

b Click on the Collect All button to collect one on-demand statistics record for each statistic type that the object supports. The collected statistics entries are listed on the form.

6 Select an entry from the list and click on the Properties button. The Statistics Record form opens.

7 View the statistics data.

8 Close the Statistics Record form.

9 Close the ISA-AA forms.

Procedure 73-10 To configure AA protocol signatures

1 Choose Manage→ISA Functions→ISA-AA from the 5620 SAM main menu. The ISA-AA form opens.

2 Choose AA Protocol (Application Assurance) from the object drop-down list.

3 Specify a filter to create a filtered list of protocols, and click on the Search button. A list of protocols is displayed.

4 Select an entry in the list and click on the Properties button. The AA Protocol (Edit) form opens.

5 View the entry information.

6 Configure the Protocol Administrative State parameter, if required.

Note 1 — You can only configure the Protocol Administrative State parameter for a local protocol.

Note 2 — The Protocol Adminstrative State parameter is read-only for some protocols.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The AA Protocol (Edit) form closes and the ISA-AA form reappears.

9 Click on the Close button to close the ISA-AA form.

Procedure 73-11 To delete an AA application, application group, or custom protocol

1 Choose Policies→ISA Policies→Application Assurance from the 5620 SAM main menu. The Manage Application Assurance Policies form opens.

2 Choose AA Group Policy (Application Assurance) from the object drop-down list and click on the Search button. A list of AA group policies is displayed.

Note — The 5620 SAM does not create local AA Group policies for each applicable managed NE. Instead, the local AA Group Policy is created/deleted when the ISA-AA group is created/deleted.

3 Select a policy in the list and click on the Properties button. The AA Group Policy (Edit) form opens with the General tab displayed.

4 Perform one of the following.

a Delete an AA application.

i Click on the Applications tab button. A list of AA applications is displayed.

ii Choose an application in the list and click on the Delete button. A warning box appears.

iii Click on the View Dependencies button.

Note — When the AA application is on a global AA group policy, the counts include all of the dependencies on the global and local NEs. When the AA application is on a local AA group policy, the counts include all of the dependencies on the local NE only.

b Delete an application group.

i Click on the Application Groups tab button. A list of application groups is displayed.

ii Choose an application group in the list and click on the Delete button. A warning box appears.

iii Click on the View Dependencies button.

Note — If the application group is on a global AA group policy, the counts include all of the dependencies on the global and local NEs. If the application group is on a local AA group policy, the counts include all of the dependencies on the local NE only.

c Delete a custom protocol.

i Click on the Custom Protocols tab button. A list of custom protocols is displayed.

ii Choose a custom protocol in the list and click on the Delete button. A warning box appears.

iii Click on the View Dependencies button.

Note — If the custom protocol is on a global AA group Policy, the counts include all of the dependencies on the global and local NEs. If the custom protocol is on a local AA group policy, the counts include all of the dependencies on the local NE only.

5 Review the dependencies and click on the OK button.

6 Select the I understand the implications of this action check box.

7 Click on the Yes button, and then click on the OK button. The AA Group Policy (Edit) form appears.

8 Click on the Apply button, and then click on the Yes button.

9 If you deleted an AA application, application group, or custom protocol on a global AA group policy, you must distribute the changes to the local AA Group Policy. Go to step 10, otherwise, go to step 13.

10 Click on the General tab button.

11 Click on the Switch Mode button. A dialog box appears.

12 Click on the OK button.

13 Close the AA Group Policy (Edit) form.

74 — Scheduling

74.1 Scheduling overview

The 5620 SAM scheduling functions allow the creation of 5620 SAM-based schedules for the automatic execution of tasks at designated times.

You can associate a schedule that you create using the 5620 SAM with a task that supports scheduling. A task such as running an STM test suite can be immediately processed, scheduled for later execution, or retained for future use. A task that is associated with a schedule is called a scheduled task. A scheduled task must be created in the configuration form for the task. For example a STM test suite scheduled task must be created in the STM test suite configuration form. After scheduled tasks are created they are associated with a schedule.

A 5620 SAM schedule is configurable for one-time or ongoing task execution. You can optionally specify the time at which an ongoing schedule is to stop functioning.

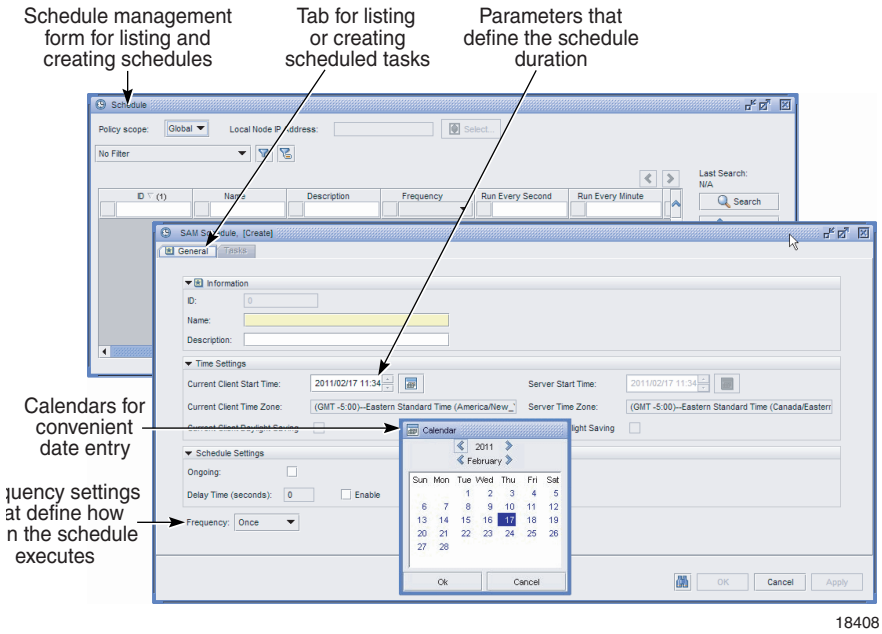
To simplify creating 5620 SAM-based schedules when the user and server are in different time zones, the 5620 SAM converts and displays schedule times specific to the user and server. For example, if a user in Ottawa wants to schedule a task on a 5620 SAM server in London, the 5620 SAM calculates the time difference and displays the user and server local times.

User time zones are configured in the user preferences form. If a time zone is not configured on the main server, the 5620 SAM uses the default time zone on the single-user client or client delegate server station, If the default time zone is not one of the 5620 SAM time zone options, the 5620 SAM displays the time zone ID and uses the UTC value without the time zone offset.

The 5620 SAM displays whether daylight saving time is in effect for the client and the server. Daylight saving time is specified for the user start time and is based on the client time zone. Daylight saving time does not specify the current time and end time.

Figure 74-1 shows the Schedule management form and the SAM Schedule configuration form.

Figure 74-1 Schedule management and configuration forms



SAM schedules

A SAM schedule exists only in the 5620 SAM and is not deployed to the target NEs. When a configured SAM schedule run time arrives, the 5620 SAM executes the associated task and compiles the task results for presentation to 5620 SAM clients.

A delay time for executing SAM scheduled runs can be configured to delay the execution of a run within a scheduled task in cases when a previously scheduled run is still executing. The 5620 SAM attempts to execute the new run at the configured delay time; if the run cannot execute at the delay time, the 5620 SAM skips the scheduled run. When a previous run completes and the next scheduled run is triggered, the run executes and is not delayed, whether a delay time is configured.

The SAM schedule functionality in the 5620 SAM uses the 5620 SAM server time zone to trigger the scheduled tasks.

A 5620 SAM-based schedule supports the following tasks:

- STM test suites. See chapter 75 for more information about STM test suites.
- NE software upgrades. See chapter 21 for more information about NE software upgrades.

Consider the following when you create a SAM schedule or a scheduled task.

- Ensure that scheduled tasks are run sufficiently far apart to allow one task to finish before the next starts. Otherwise, the next occurrence of the task is skipped or delayed, if the delay time is configured.
- Do not create schedules that overlap, as no validation is performed to ensure that a newly configured schedule does not overlap with an existing schedule.
- A new SAM scheduled task is shut down by default and must be turned up before it can be executed.
- Users with write access permissions to a specific schedule package can view or delete all the created schedules and scheduled tasks related to the package. Other users can only view schedules. See chapter 8 for more information about user permissions.
- By default, the 5620 SAM associates a scheduled task with the user account that is used to create the scheduled task. You can assign a different user account to a scheduled task. The user account must have the assigned scope of command role that is appropriate for the task, or the 5620 SAM does not execute the scheduled task.
- When you create a scheduled task that runs on a weekly or monthly schedule, you must reset the scheduled task when daylight savings time is in effect. See Procedure 74-11 for information about resetting schedules.
- If a schedule is not synchronized with the server time, you must reset the scheduled task. See Procedure 74-11 for information about resetting schedules
- SAM schedules are not distributed to the target NEs.
- You cannot delete a schedule that has a dependency, for example, one that is associated with a task.
- One minute is added to the default start and end time values of a 5620 SAM-based schedule to allow time for schedule configuration.
- A monthly SAM schedule with the Run Every Month or Run Every Months parameter configured uses a 30-day interval.
- When you create a monthly SAM schedule using the Run Every parameter and specify a date that does not exist for the specified months, the last date of the month is used. For example, if you create a monthly scheduled task, starting January 31st, the scheduled task will run on February 28th, March 31st and April 30th when those months are specified in the schedule.

74.2 Workflow to manage scheduling

1. Create a task, such as an STM test suite, that supports the 5620 SAM scheduling function.
2. Perform one of the following.
   a. Create a SAM schedule.
3. Create a SAM scheduled task by associating the task with the schedule.
4. For a SAM scheduled task that requires user account privileges other than the default privileges, assign a different user account to the scheduled task.
5. Turn up the scheduled task.

6 After the schedule executes the task, review the current status of the SAM scheduled task.

7 Perform one of the following.

a Allow the 5620 SAM to continue to perform the task according to the schedule.

b Modify the schedule.

c Reuse the schedule.

i Shut down the scheduled task.

ii Delete the scheduled task.

iii Create a scheduled task by associating a different task with the schedule.

d Delete the scheduled task and the schedule.

i Shut down the scheduled task.

ii Delete the scheduled task.

iii Delete the schedule.

74.3 Scheduling procedures

Use the following procedures to manage 5620 SAM schedules and scheduled tasks.

Procedure 74-1 To create a SAM schedule

1 Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

2 Click on the Create button. A SAM Schedule (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- User Start Time
- User End Time
- Ongoing
- Delay Time (seconds)
- Enable
- Frequency

The User End Time parameter is configurable when the Ongoing parameter is disabled and the Frequency parameter value is set to something other than Once.

When a SAM Schedule is not Ongoing and is assigned to a task, the 5620 SAM raises an alarm when the User End Time expires.

4 Perform one of the following that corresponds to the Frequency parameter value that is specified in step 3:

a When the parameter is set to Once, go to step 5.

b When the parameter is set to Per Second, configure the following parameters:

- Run Every Second
- Run Every Seconds

c When the parameter is set to Per Minute, configure the following parameters:

- Run Every Minute
- Run Every Minutes

d When the parameter is set to Per Hour, configure the following parameters:

- Run Every Hour
- Run Every Hours

e When the parameter is set to Per Day, configure the following parameters:

- Run Every Day
- Run Every Days
- Run Every

f When the parameter is set to Per Week, configure the following parameters:

- Run Every Week
- Run Every Weeks
- Run Every

The Run Every parameter is not configurable when the Ongoing parameter is enabled.

g When the parameter is set to Per Month, configure the following parameters:

- Run Every Month
- Run Every Months
- Run Every

The Run Every parameter is not configurable when the Ongoing parameter is enabled.

5 Click on the OK button to save the changes. The SAM Schedule (Create) form closes and the Schedule form reappears.

6 Close the Schedule form.

Procedure 74-2 To list schedules

1 Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

2 Choose SAM Schedule from the object drop-down list.

3 Configure the filter criteria. A list of schedules is displayed.

4 Close the Schedule form.

Procedure 74-3 To modify a schedule

Perform this procedure to change the configuration of a schedule. You cannot modify a schedule that is in use by a scheduled task.

Note — You can modify a schedule only when you are logged in as the user that is assigned to the schedule. To assign a different user account to the schedule, perform Procedure 74-8.

1 Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

2 Choose SAM Schedule from the object drop-down list.

3 Configure the filter criteria. A list of schedules is displayed.

4 Select an entry in the list and click on the Properties button. The SAM Schedule (Edit) form opens.

5 Modify the parameters, as required.

6 Click on the OK button. The SAM Schedule (Edit) form closes and the Schedule form reappears.

7 Close the Schedule form.

Procedure 74-4 To associate a task with a 5620 SAM schedule

1 Perform one of the following.

a Assign a SAM schedule to a task.

i Open the properties form for a task that supports SAM schedules, such as an STM test suite.

ii Click on the Schedule button. The *task_name* (Edit) form opens, go to step 2.

b View scheduled tasks associated with a SAM schedule.

i Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

ii Choose SAM Schedule (Schedule) from the object drop-down list.

iii Configure the filter criteria. Click on the Search button. A list of SAM schedules is displayed.

iv Select a SAM schedule in the list and click on the Properties button. The SAM Schedule (Edit) form opens.

v Click on the Tasks tab button. A list of scheduled tasks appears.

vi Choose a task from the list. Click on the Properties button to view the scheduled tasks.

2 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

Note — When you set the Administrative State parameter to Enabled, the scheduled task goes into effect, according to the schedule parameters. Ensure that the task is appropriately configured before you set the parameter to Enabled.

3 Click on the Select button to choose a schedule. The Select Schedule - STM Scheduled Task *task_name* form opens with a list of schedules.

Note — The form lists only the schedules that are associated with the current 5620 SAM user.

4 Select a schedule in the list and click on the OK button. The Select Schedule - STM Scheduled Task *task_name* form closes and the scheduled task is displayed on the STM Scheduled Task (Create) form.

5 Click on the OK button. The STM Scheduled Task (Create) form closes.

6 Close the SAM Schedule (Edit) or task properties form.

7 Close the Schedule form if the form is open.

Procedure 74-5 To list scheduled tasks

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria. A list of scheduled tasks is displayed.

4 Close the Scheduled Task form.

Procedure 74-6 To modify a scheduled task

Note — You can modify a SAM scheduled task only when you are logged in as the user that is assigned to the SAM scheduled task. To assign a different user account to the SAM scheduled task, perform Procedure 74-8.

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria. A list of scheduled tasks is displayed.

4 Select a scheduled task in the list and click on the Properties button. The scheduled task (Edit) form opens.

5 Modify the parameters, as required.

6 Click on the OK button. The SAM Scheduled Task (Edit) form closes and the Scheduled Task form reappears.

7 Close the Scheduled Task form.

Procedure 74-7 To turn up or shut down a scheduled task

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task (Schedule) from the object drop-down list.

3 Configure the filter criteria. A list of scheduled tasks is displayed.

4 Select an entry in the list and click on the Task Action button.

5 Choose one of the following from the menu that appears:

a Turn Up—enable the scheduled task. The administrative state changes to enabled.

b Shut Down—disable the scheduled task. The administrative state changes to disabled.

6 Close the Scheduled Task form.

Procedure 74-8 To assign a different user account to a SAM scheduled task

Perform this procedure to associate a SAM scheduled task with a different user account. By default, the 5620 SAM associates a scheduled task with the user account that is active when the SAM scheduled task is created.

Note — The 5620 SAM does not execute a SAM scheduled task unless the scheduled task is associated with an existing 5620 SAM user account. If you delete the user account that is associated with a SAM scheduled task, you must assign a different user account to the SAM scheduled task. A 5620 SAM user with an assigned administrator scope of command role can assign a user account to a SAM scheduled task.

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task list form opens.

2 Choose SAM Scheduled Task (schedule) from the object drop-down list.

3 Configure the filter criteria. A list of SAM scheduled tasks is displayed.

4 Select a scheduled task and click on the Reassign User button. A dialog box informs you that the new user must have the appropriate access permissions to manage the scheduled task. See "Scope of command" in section 8.1 for more information.

5 Set the Change Current User To parameter.

6 Click on the OK button.

Procedure 74-9 To execute a SAM scheduled task

1 Turn up the SAM scheduled task, as described in Procedure 74-7.

2 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

3 Choose SAM Scheduled Task from the object drop-down list.

4 Configure the filter criteria. A list of SAM scheduled tasks is displayed.

5 Select an entry and click on the Task Action button.

6 Choose Execute from the menu that appears. The 5620 SAM executes the SAM scheduled task.

7 Close the Scheduled Task form.

8 Perform Procedure 74-10 to view the SAM scheduled task execution status, if required.

Procedure 74-10 To view the current status of a SAM scheduled task

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria. A list of SAM scheduled tasks is displayed.

4 Select a SAM scheduled task in the list.

5 Click on the Task Action button and choose View Result from the menu that appears.

6 View the Execution Status indicator. The value is one of the following:

- None
- In Progress
- Skip Requested
- Skipped
- Stop Requested
- Stopped
- Succeeded
- Failed
- Delay Requested
- Delayed
- Started

7 View the Status indicator. The value is one of the following:

- Running—The scheduled task is running.
- Not Running—The scheduled task is not running.
- Completed—The scheduled task execution completed successfully.

8 Close the Scheduled Task form.

Procedure 74-11 To reset a scheduled task

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria to list tasks that the administrative state is enabled, and click on the Search button. A list of scheduled tasks is displayed.

4 Select a scheduled task in the list.

5 Click on the Task Action button and choose Shut Down from the menu that appears. The Turn Up button is enabled.

6 Click on the Task Action button and choose Turn Up from the menu that appears. The Shut Down button is enabled.

7 Close the Scheduled Task form.

Procedure 74-12 To delete a scheduled task

Note — You can delete a SAM scheduled task only when you are logged in as the user that is assigned to the SAM scheduled task. To assign a different user account to the SAM scheduled task, perform Procedure 74-8.

1 Choose Tools→Schedules→Scheduled Task from the 5620 SAM main menu. The Scheduled Task form opens.

2 Choose SAM Scheduled Task from the object drop-down list.

3 Configure the filter criteria. A list of scheduled tasks is displayed.

4 Select a scheduled task in the list.

5 Click on the Task Action button and choose Shut Down from the menu that appears. The Delete button is enabled.

6 Click on the Delete button. A dialog box appears.

7 Click on the Yes button. The 5620 SAM deletes the scheduled task.

8 Close the Scheduled Task form.

Procedure 74-13 To delete a schedule

Note 1 — You cannot remove a schedule that is associated with a scheduled task; you must first delete the scheduled task.

Note 2 — You can delete a SAM scheduled task only when you are logged in as the user that is assigned to the SAM scheduled task. To assign a different user account to the SAM scheduled task, perform Procedure 74-8.

1 Perform Procedure 74-12 to delete the scheduled tasks associated with the schedule.

2 Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

3 Choose SAM Scheduled from the object drop-down list.

4 Configure the filter criteria. A list of schedules is displayed.

5 Select a schedule in the list and click on the Delete button. A dialog box appears.

6 Click on the Yes button. The 5620 SAM deletes the schedule.

7 Close the Schedule form.

75 — Service Test Manager

75.1 Service Test Manager overview

The 5620 SAM service test manager (STM) system provides the ability to group various OAM tests into test suites for network troubleshooting and for verifying compliance with SLAs. You can schedule the execution of a test suite to provide continual performance feedback, or run a test suite on demand to investigate service issues. The test results are logged for monitoring and trend analysis.

The grouping of tests into a test suite allows a 5620 SAM operator to use one schedule for the periodic execution of multiple OAM diagnostics against multiple network objects; for example, services, NEs, or transport components. An operator can choose to include existing tests, use the 5620 SAM to generate the tests that comprise a test suite, or both. Groups of tests in a suite can be configured to execute sequentially or concurrently. In addition, you can configure a test suite as an OAM validation test to verify the operational status of a service.

You can configure threshold-crossing parameters to generate alarms when rising or falling threshold values are reached due to the reach, latency, or jitter issues discovered by the OAM tests.

The 5620 SAM STM allows the deployment of the maximum number of tests to a 7450 ESS or 7750 SR. The 5620 SAM raises an alarm when the number of tests on an NE is 60% of the configured maximum. Attempts to create or execute a test using the 5620 SAM fail when the number of deployed tests on an NE is too high.

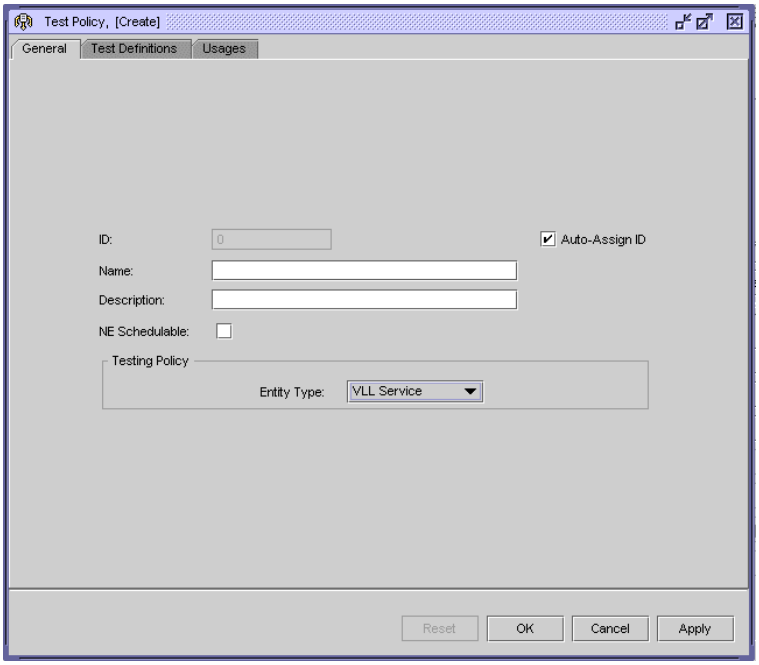
OmniSwitch testing

The Service Test Manager facilitates the CPE Test Head capability for SLAs on the OS 6250. This test is critical when a new service is provisioned in the Metro Ethernet network and when you need to troubleshoot a live service. You can validate the Metro Ethernet network between the endpoints of the customer Ethernet service. The CPE Test Head supports unidirectional traffic and IPv4. See Procedure 75-5 for more information about configuring CPE SLA tests.

Test policies

Figure 75-1 shows the Test Policy (Create) form with VLL service specified as the entity type for the policy.

Figure 75-1 Test Policy (Create) form



To enable the automatic generation of tests for a test suite, the 5620 SAM requires a test policy that contains a set of test definitions and pre- and post-processing rules. A test policy also specifies the order of execution for the generated tests. A test policy applies to only one test suite, and a test suite can have only one associated test policy.

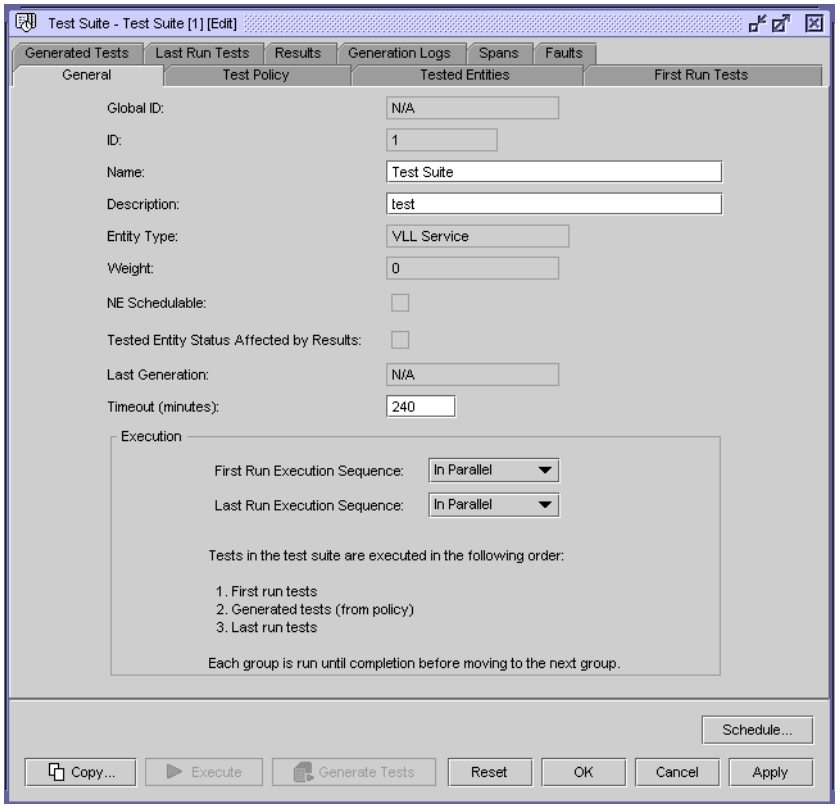
Test policy parameters can be configured to display test results only if a test fails or generates a threshold crossing alarm. In large networks, this can substantially reduce the amount of test data that the 5620 SAM needs to collect.

A test policy is specific to one type of entity; for example, a VLL service or service tunnel. The test definitions in the policy are restricted to the tests that apply to the entity type specified in the policy. A test policy is applied to a test suite during test suite creation.

Test suites

Figure 75-2 shows the Test Suite (Create) form with VLL service specified as the entity type.

Figure 75-2 Test Suite (Create) form



Note — The 5620 SAM does not attempt to discover tests or test suites that are configured locally on an NE, for example, using a CLI.

A test suite contains three test groups:

- **First-run tests**

  First-run tests are the tests in a suite that the 5620 SAM executes before the tests in the other groups. First-run tests are chosen from a list of existing tests and might typically include high-level diagnostics; for example, a service site ping or VPRN ping. No restrictions apply to the types of tests that are selectable as first-run tests.

- **Generated tests**

  Generated tests are created by the 5620 SAM for use against a specific network entity, based on the entity type specified in the suite and the specific tested entities that are named in the associated test policy. For example, a service site ping test policy associated with a three-site VPRN test suite causes the 5620 SAM to generate six tests: one site ping test from each site in the VPRN to the other two sites. When you change the configuration of a network entity, such as a service, you must regenerate the generated tests that apply to the entity. Test regeneration removes previously generated tests from a test suite.

- **Last-run tests**
  Last-run tests are the tests in a suite that the 5620 SAM executes after the tests in the other groups. Last-run tests are chosen from a list of existing tests and might typically include transport-layer diagnostics; for example, an LSP trace or a tunnel ping. No restrictions apply to the types of tests that are selectable as last-run tests.

To create a test suite that contains tests for different entity types, you can specify that the test suite applies to no specific entity type. In this way, you can create a group of disparate tests to which no test policy restrictions apply. Specifying none as the entity type in a test suite has the following effects.

- It allows you to choose any predefined test as a first-run or last-run test.
- It disables test generation in the test suite, because test generation requires a test policy that is based on a specific entity type.

To manage the system resources that test execution consumes, the 5620 SAM assigns a weight value to a test. When the 5620 SAM executes a test, it attempts to reserve the test weight from a resource pool, performs the test, then returns the test weight to the pool. The weight of a test suite is the sum of the weights of the individual tests in the suite. The 5620 SAM attempts to reserve the weight of the whole suite for the duration of suite execution. If the required weight for a test or test suite is unavailable, execution is halted and the Status value contained in the test result is set to Not Enough Resources.

You can create an OAM service validation test to verify the operational status of a service. The operational status of a service depends on the operational states of its service sites or instances. It is possible for a service to be operationally up when communication between sites is not operational. For example, a VRF can be operationally up but the routes to its peers might not be populated because of the routing policy, route target, or ACL configuration. The State Cause of the service indicates the success or failure of the OAM validation test, and therefore, service connectivity.

You can configure an OAM validation test when you create a test suite and run the OAM validation test from the service configuration form.

Note — OAM validation tests are not supported for HVPLS.

Consider the following when you create or execute test suites.

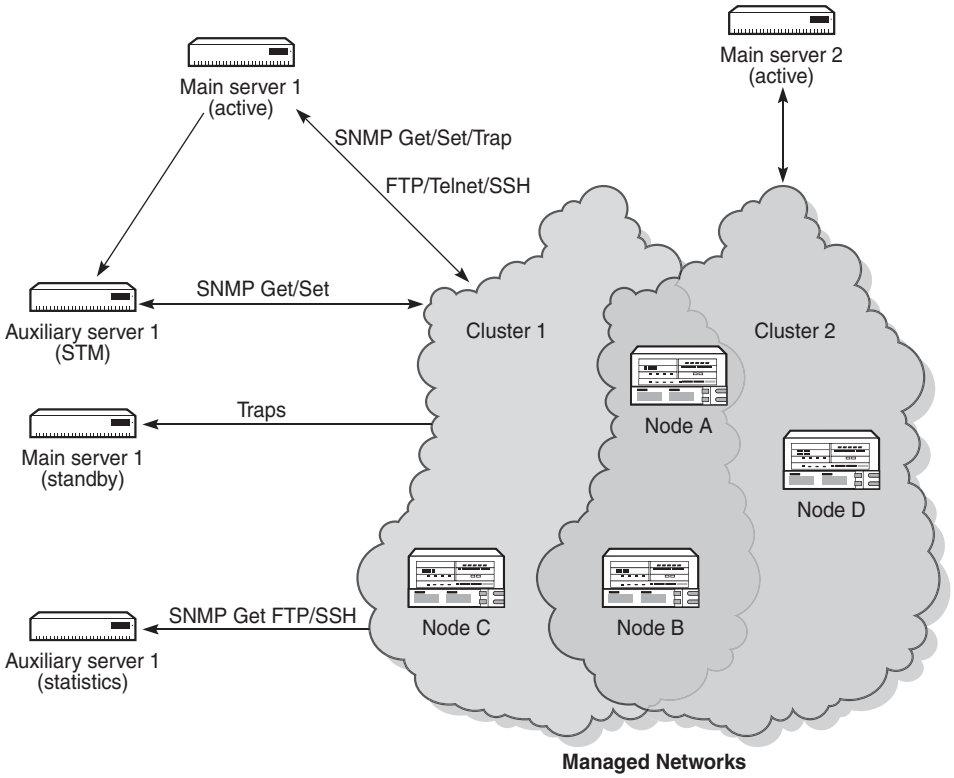
- A test, whether pre-existing or generated, is associated with only one test suite.
- You can execute a generated test on demand, not just in the context of a test suite.
- STM test suites can be configured as scheduled tasks. See chapter 74 for information about using the 5620 SAM to schedule tasks.
- Using an NE schedule does not ensure that the target NEs perform the actions in an associated STM scheduled task in the order specified; the NEs that execute an NE scheduled task operate independently and are not directed by the 5620 SAM. As soon as an NE completes an action in an NE scheduled task, it performs the next action.

- The 5620 SAM database logs test results only for scheduled test suites that are associated with SAM schedules. Logging for test suites that are associated with NE schedules is performed locally on each target NE.
- Size constraint policies control the number of historical records that the 5620 SAM retains in the database. You can configure size constraint policies to limit the number of database objects that are associated with specific test types. See chapter 43 for information about size constraint policies.
- A 5620 SAM user that is assigned the admin or QoS/ACL management scope of command role can create and modify all tests, test policies, and test suites. A user that is assigned the service management scope of command role can create and modify only STM components that are related to services. A user that is assigned the topology management role can create and modify only STM components that are related to network transport elements.
- OAM test suites in which the Validation Test Suite parameter is enabled are used to test the operational status of a service or service-related entity such as a service tunnel. The result of the test is indicated by the OAM Validation Failed state cause indicator on the General tab of the management form for the object.
- You can view test-suite results for an object from the Tests tab of the configuration form for the object.

OAM test ID ranges

You can configure a test ID for the OAM tests in multiple server environments. A test ID allows you to identify the source server that initiated the OAM test. Figure 75-3 shows an example of a network configuration on which a user could run OAM tests on Node A and Node B from the 5620 SAM main 1 or main 2 servers. In this example, Node A and Node B are members of two network clusters that are managed by separate 5620 SAM servers, Main server 1 (active) and Main server 2 (active).

Figure 75-3 Multiple STM implementation



You can execute OAM tests from the new main server after a redundancy switch from Main server 1 (active) tom Main server 1 (standby).

You can configure the nms-server.xml file to configure the range for the test IDs. You must use the same ID range for the 5620 SAM main and standby servers that are managing a distinct network cluster. The OAM tests always have a test ID in the specified range.

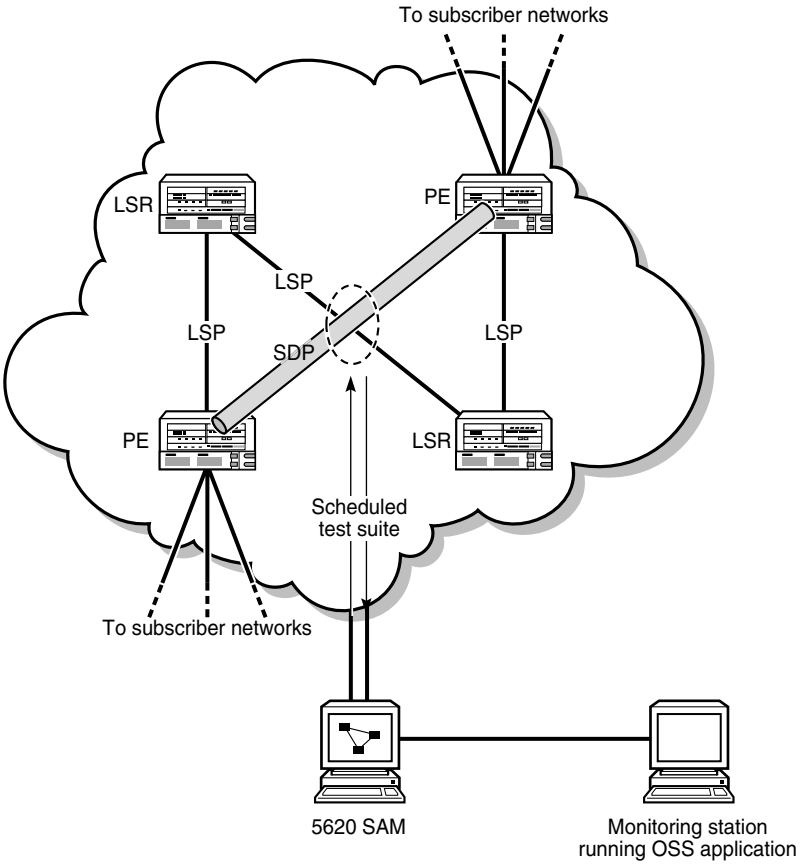
The 5620 SAM does not validate the range values for the test IDs. However, the 5620 SAM raises a major alarm upon receipt of a test with a test ID outside the range, or when the range is changed in the nms-server.xml file.

See Procedure 75-1 for info on how to change the test ID range.

75.2 Sample Service Test Manager implementation

Figure 75-4 shows a sample STM implementation that illustrates how you can use STM suites to verify service operation and identify network problems.

Figure 75-4 Sample STM implementation



In the sample network, two scheduled STM test suites run constantly to ensure that the transport elements are functioning properly. One test suite monitors the SDPs, and the other test suite monitors the LSPs. A 5620 SAM administrator can quickly update the test suites, as required, to reflect network topology changes by revising the list of tested entities in the suite and regenerating the tests. An OSS application collects the test result information which is then available for monitoring by NOC staff.

Note — This sample configuration uses a SAM schedule to create a scheduled task. See chapter 74 for information about SAM schedules.

The SDP test suite contains the following generated tests for each SDP:

- tunnel ping
- MTU ping

The LSP test suite contains the following generated test for each LSP path:

- LSP ping (tested entity type is LSP path)

NOC monitoring staff become aware that tunnel ping operations fail occasionally on one SDP. Packet loss is not yet significant enough to affect SLAs, but threatens to become so, based on the observed trend. NOC staff run a test suite against the LSPs in the affected LSP path. The test suite contains the following generated test for each LSP in the LSP path:

- LSP ping (tested entity type is LSP)

Test results show that the packet loss is related to a specific LSP in the path. Investigation of the LSP traffic pattern indicates that a recently provisioned service is causing the LSP to be oversubscribed. The problem is addressed by a network designer and is corrected through configuration changes.

Table 75-1 lists the high-level tasks necessary to configure and use the STM elements in this sample.

Table 75-1 Sample STM implementation configuration sequence

Task	Description
1. Scheduled STM test-suite creation	Create STM test policies for transport-layer elements. • Create a test policy for the SDPs. Specify Tunnel (SDP) as the Entity Type for the policy, and choose Tunnel Ping and MTU Ping as the test definitions. Create separate tunnel ping definitions for different forwarding classes, as required. • Create a test policy for the LSP paths. Specify LSP as the Entity Type for the policy and choose LSP Ping as the test definition. In the test definition, specify LSP Path as the Target Type. Create separate LSP ping definitions for different forwarding classes, as required. Create STM test suites for transport-layer elements. • Create a test suite for the SDPs. Specify Tunnel (SDP) as the Entity Type for the suite, choose the SDP test policy, choose the SDPs against which the suite is to run, and use the 5620 SAM to generate the tests in the suite. Create a schedule for the test suite according to network monitoring requirements, and apply the schedule to the test suite to create a scheduled task. • Create a test suite for the LSP paths. Specify LSP as the Entity Type for the suite, choose the LSP test policy, choose the LSP paths against which the suite is to run, and use the 5620 SAM to generate the tests in the suite. Create a schedule for the test suite according to network monitoring requirements, and apply the schedule to the test suite to create a scheduled task.
2. Data presentation	Customize the tabular display of test results in the 5620 SAM, or create an OSS application that retrieves test-result data from the 5620 SAM and presents it as information in graphical format for NOC staff.
3. Creation of non-scheduled STM test suite or individual OAM tests for network troubleshooting	Create an STM test policy for the LSPs for use during network troubleshooting. • Create a test policy for the LSPs. Specify LSP as the Entity Type for the policy and choose LSP Ping as the test definition. In the test definition, specify LSP as the Target Type. Create separate LSP ping definitions for different forwarding classes, as required. Create a non-scheduled STM test suite (or individual OAM tests, depending on the number of LSPs involved) for the LSPs in the LSP path. • Specify LSP as the Entity Type for the suite, choose the newly created LSP test policy, choose the LSPs in the LSP path against which the suite is to run, and use the 5620 SAM to generate the tests for the suite.
4. Network monitoring	Use the 5620 SAM to display the scheduled test results in tabular format, or use an OSS application to monitor the LSP ping, tunnel ping, and MTU ping diagnostic results in real time. Record inconsistencies and trends, and troubleshoot the network as required. Use the threshold-crossing alarm capabilities to raise alarms when traffic characteristics rise above or fall below specific values.

(1 of 2)

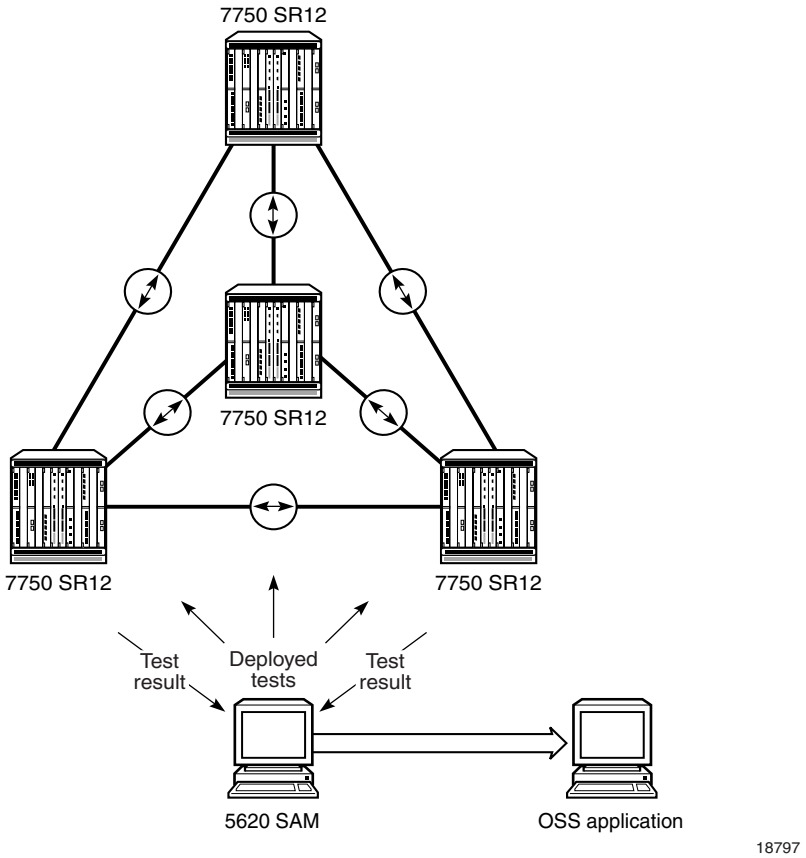
Task	Description
5. Network troubleshooting	When potential trouble arises, use a non-scheduled STM test suite or individual STM tests to help identify the cause. • Create individual tests or edit the existing non-scheduled test suite. Include as tested entities the LSPs that comprise the LSP path and regenerate the tests for the suite, as required. • Execute the non-scheduled test suite and monitor the test results. • Edit the test definition in the test policy. Change test parameter values as required, regenerate the tests in the suite, and re-execute the suite. Continue to refine the diagnostic test results until the problem manifests itself in the test results.

(2 of 2)

75.3 Sample network monitoring configuration

Figure 75-5 shows the high-level flow of tests and test results in a simple network topology that the network provider wants to continually monitor using the STM. See section 75.4 for the explicit steps required to create the STM configuration.

Figure 75-5 Continual network topology monitoring



A 5620 SAM administrator creates and schedules an STM test suite to monitor the LSP mesh and identify potential overloading and reachability problems before they affect service traffic. The test suite contains ping and trace test definitions for three different classes of in-profile traffic and is scheduled to run every 15 minutes.

Note — This sample configuration uses a SAM schedule to create a scheduled task. See chapter 74 for information about SAM schedules.

Because the same group of tests is to be run on multiple entities of the same type, the test suite consists of generated tests only. The test policy that the 5620 SAM uses to generate the tests contains the following six test definitions:

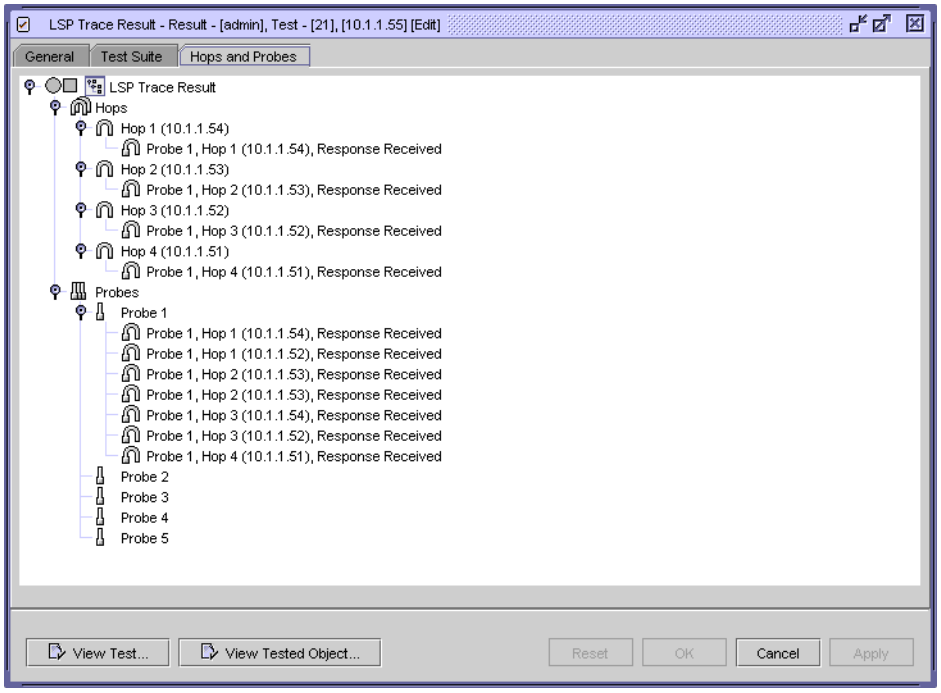
- LSP ping - be in
- LSP ping - af in
- LSP ping - nc in
- LSP trace - be in
- LSP trace - af in
- LSP trace - nc in

The 5620 SAM generates 72 tests for the test suite—3 ping tests and 3 trace tests for each of the 12 LSPs and LSP paths. Every 15 minutes, the 5620 SAM scheduler executes the tests and stores the results. An OSS application periodically retrieves the test results, performs trend analysis and presents the transport utilization information to NOC monitoring staff.

The 5620 SAM generates an alarm in the event of an LSP ping probe failure or an LSP trace path change, as specified in the test policy, so 5620 SAM operators become aware of new transport faults as they arise.

Figure 75-6 shows the result of a generated LSP trace test. The form lists the LSP hops for each test probe and indicates the success or failure of each hop. As shown in Figure 75-6, the success of probe 1 means that probes 2 through 5 are not sent.

Figure 75-6 LSP trace test result



75.4 Sample network monitoring configuration steps

The following steps explicitly define the end-to-end configuration of the network monitoring sample in section 75.3. For conciseness, the procedure lists only the configuration steps and parameters that are specific to and necessary for the sample. See the procedures in section 75.10 for complete STM configuration information.

Create test policy for test generation

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Create Test Policy from the Create contextual menu. The Test Policy (Create) form opens.

4 Configure the parameters in Table 75-2 using the supplied values:

Table 75-2 Test policy General tab parameters

Parameter	Value	Comment
Name	LSP Test Policy	—
NE Schedulable	disabled	NE-schedulable test results are not returned to the 5620 SAM.
Entity Type	LSP	—

5 Click on the Test Definitions tab button.

6 Click on the Add button to add a test definition to the test policy. A menu appears.

7 Choose MPLS→Add LSP Ping. The LSP Ping Definition (Create) form opens with the General tab displayed.

In the sample configuration, the operator creates a separate LSP Ping test definition for each of the following forwarding classes:

- be (best effort - low priority, delivery not guaranteed)
- af (assured forwarding - medium priority, delivery guaranteed)
- nc (network control - high priority, delivery guaranteed)

8 Configure the parameters in Table 75-3 using the supplied values, most of which are common to the three test definitions:

Table 75-3 LSP Ping Definition parameters

Parameter	Value	Comment
General tab		
Name	LSP Ping - be in LSP Ping - af in LSP Ping - nc in	First test definition Second test definition Third test definition
Target Type	LSP	—
Test parameters tab		
Number of Test Probes	5	This provides more analysis granularity than a single test packet without affecting network performance.
Size (octets)	108	This is the minimum packet size for this type of test on the 7450 ESS and 7750 SR. The minimum packet size varies, depending on the type and version of device against which a test runs.
Forwarding Class	be af nc	For LSP Ping - be in test definition For LSP Ping - af in test definition For LSP Ping - nc in test definition To cover a range of traffic streams and to test different network queues, multiple test definitions are necessary. The sample configuration uses three LSP ping definitions that differ only by forwarding class.
Forwarding Profile	in	All test packets are marked in-profile. This means that they follow the same path as service traffic.
Results configuration tab		
Probe History Size (rows)	100	—
Trap Generation	Probe Failure	Test-probe failures provide early notification of LSP congestion or reachability issues to a 5620 SAM operator. OSS analysis of the results indicates trends for further investigation.

9 Click on the OK button. The LSP Test Definition (Create) form closes and a dialog box appears.

10 Click on the OK button. The test definition is listed on the Test Policy (Create) form.

11 Repeat steps 6 to 10 for the remaining test definitions listed in step 7.

12 Click on the Add button to add a test definition to the test policy. A menu appears.

13 Choose MPLS→Add LSP Trace. The LSP Trace Definition (Create) form opens with the General tab displayed.

In the sample configuration, the operator creates a separate LSP Trace test definition for each of the following forwarding classes:

- be (best effort - low priority, delivery not guaranteed)
- af (assured forwarding - medium priority, delivery guaranteed)
- nc (network control - high priority, delivery guaranteed)

14 Configure the parameters in Table 75-4 using the supplied values. Values that are not common to the three test definitions are so indicated.

Table 75-4 LSP Trace Definition parameters

Parameter	Value	Comment
General tab		
Name	LSP Trace - be in LSP Trace - af in LSP Trace - nc in	For first test definition For second test definition For third test definition
Target Type	LSP Path	—
Test parameters tab		
Number of Test Probes	5	This provides more analysis granularity than a single test packet without affecting network performance.
Size (octets)	108	This is the minimum packet size for this type of test on the 7450 ESS and 7750 SR. The minimum packet size varies, depending on the type and version of device against which a test runs.
Forwarding Class	be af nc	For LSP Trace - be in definition For LSP Trace - af in definition For LSP Trace - nc in definition To cover a range of traffic streams and to test different network queues, multiple test definitions are necessary. The sample configuration uses a different LSP ping definition for each forwarding class.
Forwarding Profile	in	All LSP ping test definitions in the sample involve in-profile traffic.
Results configuration tab		
Probe History Size (rows)	100	—

(1 of 2)

Parameter	Value	Comment
Trap Generation	Test Failure Path Change	A test failure trap may indicate a routing or congestion issue, but it also indicates test misconfiguration when the Maximum Time to Live parameter value is too low to allow a test probe to reach the destination LSP. A path change trap may indicate an intermittently congested or unresponsive LSP.

(2 of 2)

15 Click on the OK button. The LSP Test Definition (Create) form closes and a dialog box appears.

16 Click on the OK button. The test definition is listed on the Test Policy (Create) form.

17 Repeat steps 12 to 16 for the remaining test definitions listed in step 13.

18 Click on the OK button. A dialog box appears.

19 Click on the Yes button. The Test Policy (Create) form closes and the Service Test Manager form reappears.

Create schedule

20 Choose Tools→Schedules→Schedule from the 5620 SAM main menu. The Schedule form opens.

21 Click on the Create button and choose Create SAM Schedule. The SAM Schedule (Create) form opens.

22 Configure the parameters in Table 75-5 using the supplied values:

Table 75-5 SAM Schedule parameters

Parameter	Value	Comment
Name	LSP Assurance	—
User Start Time	a future time	Specify the date and time at which the schedule is to be first triggered. This value is used to calculate the times of subsequent triggers, based on the Frequency parameter value. Compare this value and the Frequency parameter value with those in other 5620 SAM schedules to ensure that the schedule trigger times are staggered and the resulting NE task load is balanced.
Ongoing	enabled	This setting tells the 5620 SAM to continually trigger execution of the task associated with the schedule.
Frequency	Per Minute / 15	You must also select the Run Every Minutes radio button and specify 15 as the number of minutes for the triggering frequency.

23 Click on the OK button. The SAM Schedule (Create) form closes.

24 Close the Schedule form.

Create test suite

25 Click on the Create button in the Service Test Manager form and choose Create Test Suite from the contextual menu. The Test Suite (Create) form opens with the General tab displayed.

26 Configure the parameters in Table 75-6 using the supplied values.

Table 75-6 Test suite parameters

Parameter	Value	Comment
Name	LSP Test Suite	—
Entity Type	LSP	—
NE Schedulable	disabled	NE-schedulable test results are not returned to the 5620 SAM.

27 Click on the Test Policy tab button.

28 Click on the Add button to choose a test policy that governs the generation of tests in the test suite. The Select Test Policy - Test Suite form opens.

29 Configure the filter properties and click on the Search button. A list of test policies is displayed.

30 Select the LSP Test Policy entry and click on the OK button. The test policy is listed on the Test Suite (Create) form.

31 Click on the Tested Entities tab button.

32 Click on the Add button to choose the LSPs that are to be regularly assessed by the test suite. The Select Tested Entity - Test Suite form opens.

33 Configure the filter properties and click on the Search button to display a list of LSPs.

34 Select the LSPs that you want to include and click on the OK button. The LSPs are listed on the Test Suite (Create) form.

35 Click on the Apply button to save the changes. Additional buttons appear and the form name changes to Test Suite (Edit).

36 Click on the Generated Tests tab button.

37 Click on the Generate Tests button. The 5620 SAM generates a test for each LSP listed on the Tested Entities tab. The tests are listed on the form as they are generated.

Apply a span of control to a test suite

38 Click on the Spans tab button.

39 Click on the Add button. The Select Spans - Test Suite form opens with a list of available spans.

40 Select one or more spans to apply to the test suite.

41 Click on the OK button. The Select Spans - Test Suite form closes and a dialog box appears.

42 Click on the OK button to confirm the action.

Create scheduled task

43 Click on the Schedule button and choose Create SAM Scheduled Task. The SAM Scheduled Task (Create) form opens with LSP Test Suite displayed in the Task panel.

44 Configure the parameters in Table 75-7 using the supplied values.

Table 75-7 SAM scheduled task parameters

Parameter	Value	Comment
Scheduled Task Name	Periodic LSP Check	—
Administrative State	Enabled	The 5620 SAM executes the scheduled task at regular intervals based on the specified User Start Time and Frequency.

45 Click on the Select button. The Select Schedule - SAM Scheduled Task form opens.

46 Select LSP Assurance and click on the OK button. The 5620 SAM automatically populates the Schedule panel with the schedule information.

47 Click on the OK button. The SAM Scheduled Task (Create) form closes and the Test Suite (Edit) form reappears.

48 Close the Test Suite (Edit) form.

49 Close the Service Test Manager form.

75.5 Sample SAA accounting files configuration

The following sample configuration focuses on the configuration of SAA accounting files that are to be collected following the generation of an NE schedulable test of VLL services.

A network provider wants to use the 5620 SAM to view test result information for a NE schedulable test of VLL services and wants the 5620 SAM to process the OAM results MIB entries and produce a compressed XML record that is stored in SAA accounting files on the nodes.

A 5620 SAM administrator must create an NE schedulable test for VLL services that records test result information in SAA accounting files. The administrator creates one accounting policy, one file policy, one test policy, and one test suite. Section 75.6 describes the steps that are required to create a test.

75.6 Sample SAA accounting files configuration steps

The following steps explicitly define the end-to-end configuration of the SAA accounting files sample in section 75.5. For conciseness, the procedure lists only the configuration steps and parameters that are specific to and necessary for the sample. See the procedures in section 75.10 for complete STM configuration information.

Create accounting policy

1 Choose Tools→Statistics→Accounting Policies from the 5620 SAM main menu. The Manage Accounting Policies form opens.

2 Click on the Create button. The Accounting Policy (Create) form opens.

3 Configure the parameters in Table 75-8 using the supplied values.

Table 75-8 Accounting policy parameters

Parameter	Value	Comment
Displayed Name	SAA Accounting Policy	—
Type	NE Schedulable Tests	You must choose this value to allow the configuration of SAA accounting files

4 Click on the Select button beside the File ID parameter. The Select A File Policy form opens.

5 Click on the Create button. The File Policy (Create) form opens.

6 Configure the Displayed Name parameter. For the purposes of this sample, the value shall be SAA File Policy.

7 Click on the OK button. The File Policy (Create) form closes and the Select A File Policy form reappears.

8 Select the SAA File Policy entry and click on the OK button. The Select A File form closes and the file policy is listed on the Accounting Policy (Create) form.

9 Click on the OK button. The Accounting Policy (Create) form closes and the Manage Accounting Policies form reappears.

10 Configure the filter properties and click on the Search button. A list of accounting policies is displayed

11 Select the SAA Accounting Policy entry and click on the Distribute button. The Distribute form opens.

12 Select the entities that you want to include and click on the OK button. The Distribute form closes.

13 Close the Manage Accounting Policies form.

Create test policy

14 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

15 Click on the Create button.

16 Choose Create Test Policy from the Create contextual menu. The Test Policy (Create) form opens.

17 Configure the parameters in Table 75-9 using the supplied values:

Table 75-9 Test policy parameters

Parameter	Value	Comment
Name	SAA Test Policy	—
NE Schedulable	enabled	You must enable this parameter to allow the configuration of SAA accounting files.
Entity Type	VLL Service	—
Accounting Files	enabled	You must enable this parameter to allow the configuration of SAA accounting files.

18 Click on the Test Definitions tab button.

19 Click on the Add button to add a test definition to the test policy. A menu appears.

20 Choose Service→Add VCCV Ping. The VCCV Ping Definition (Create) form opens with the General tab displayed.

21 Click on the OK button. The VCCV Ping Definition (Create) form closes and a dialog box appears.

22 Click on the OK button. The test definition is listed on the Test Policy (Create) form.

23 Click on the OK button. The Test Policy (Create) form closes and the Service Test Manager form reappears.

Create test suite

24 Click on the Create button in the Service Test Manager form and choose Create Test Suite from the contextual menu. The Test Suite (Create) form opens with the General tab displayed.

25 Configure the parameters in Table 75-10 using the supplied values:

Table 75-10 Test suite parameters

Parameter	Value	Comment
Name	SAA Test Suite	—
Entity Type	VLL Service	—

(1 of 2)

Parameter	Value	Comment
NE Schedulable	enabled	You must enable this parameter to allow the configuration of SAA accounting files.

(2 of 2)

26 Click on the Test Policy tab button.

27 Click on the Add button to choose a test policy that governs the generation of tests in the test suite. The Select Test Policy - Test Suite form opens.

28 Configure the filter properties and click on the Search button. A list of test policies is displayed.

29 Select the SAA Test Policy entry and click on the OK button. The test policy is listed on the Test Suite (Create) form.

30 Click on the Tested Entities tab button.

31 Click on the Add button. The Select Tested Entity - Test Suite form opens.

32 Configure the filter properties and click on the Search button to display a list of entities.

33 Select the nodes that were used in step 12 and click on the OK button. The nodes are listed on the Test Suite (Create) form.

34 Click on the Apply button to save the changes. Additional buttons appear and the form name changes to Test Suite (Edit).

35 Click on the Generated Tests tab button.

36 Click on the Generate Tests button. The 5620 SAM generates a test for each entity listed on the Tested Entities tab. The tests are listed on the form as they are generated.

75.7 Sample threshold-crossing alarm configuration

The following sample configuration focuses on the configuration of a threshold-crossing alarm that is to be included in a test suite. It does not describe the configuration of the test suite, schedule or scheduled task associated with the sample. No test policy is required for the configuration, as it does not involve generated tests.

A network provider wants to use the 5620 SAM to monitor a customer VPLS named VPLS 17 that carries VoIP traffic. He wants the 5620 SAM to raise an alarm when the round-trip jitter value rises above a specified threshold.

Network jitter values typically range from 10 to 15 ms, but are occasionally as high as 25 ms. Jitter buffers in the end-user VoIP sets can accommodate up to 80 ms of jitter. A network engineer determines that a jitter test threshold of 30 ms is low enough to allow NOC operators sufficient time for investigating a jitter increase, yet high enough to exclude spurious jitter events.

A 5620 SAM administrator wants to creates a scheduled CPE ping test suite for the VPLS that periodically measures the round-trip jitter between each VPLS site and an end device. The administrator creates one CPE ping test for each site in the VPLS. Section 75.8 describes the steps required to create one such test.

75.8 Sample threshold-crossing alarm configuration steps

The following procedure explicitly defines the configuration steps required to create the test with a threshold-crossing alarm described in section 75.7. See section 75.4 for information about sample test-suite, test policy, or scheduling configurations. See the procedures in section 75.10 for complete STM configuration information.

For conciseness, the procedure lists only the configuration steps and parameters that are specific to and necessary for the sample.

Create CPE ping test with threshold-crossing criteria

1 Click on the Create button in the Service Test Manager form and choose L2 Service→CPE ping from the contextual menu. The CPE Ping Test (Create) form opens with the General tab displayed.

2 Configure the parameters in Table 75-11 using the supplied values:

Table 75-11 General CPE Ping test parameters

Parameter	Value	Comment
General tab		
Name	CPE Ping Test - VPLS 17, Site A	A descriptive name such as this is helpful for quickly identifying the entity under test when viewing the test results.
NE Schedulable	enabled	You must enable this parameter to allow the configuration of threshold-crossing criteria.
Select button in Service panel	VPLS 17	Click on the Search button on the Select Service - CPE Ping form that opens to choose a service.
Select button in Site panel	Site A	Click on the Search button on the Select Site - CPE Ping form that opens to choose a service.
Destination IP Address	*IP address of an end device connected to Site A*	This is the IP address to which the CPE ping packets are sent.
Source IP Address	*IP address of the NE that originates the test packets*	This IP address must be in the same subnet as the Destination IP Address.
Source MAC Address	*MAC address of the NE that originates the test packets*	—
Test parameters tab		
Number of Test Probes	5	This provides more analysis granularity than a single test packet without affecting network performance.
Results configuration tab		

(1 of 2)

Parameter	Value	Comment
Probe History Size (rows)	100	This value provides a greater retained test-result history for occasional monitoring by a 5620 SAM operator.
Trap Generation	Probe Failure	Test-probe failures provide early notification of congestion or reachability issues to a 5620 SAM operator for troubleshooting purposes.

(2 of 2)

3 Click on the Apply button. Additional buttons and tab buttons appear, and the form name changes to CPE Ping *Test Name* (Edit).

4 Click on the Threshold Alarms tab button.

5 Click on the Add button to add threshold criteria. The NE Threshold Event (Create) form opens with the General tab displayed.

6 Configure the parameters in Table 75-12 using the supplied values:

Table 75-12 Threshold-crossing CPE Ping test parameters

Parameter	Value	Comment
Type	Round-Trip Jitter	—
Generate Alarm on Rising Threshold	enabled	This is the default setting. Alternatively or additionally, by enabling the Include Falling Threshold parameter, you can configure the 5620 SAM to generate an alarm when a test-result value falls below a specified threshold. You can also configure the 5620 SAM to clear a rising-threshold alarm when the test-result value falls below the value configured for the falling threshold.
Rising Threshold tab		
Threshold Value	30	This value specifies that the 5620 SAM is to generate an alarm when an individual test result contains a round-trip jitter value greater than 30 ms.

7 Click on the OK button. The NE Threshold Event (Create) form closes.

8 Close the CPE Ping *Test Name* (Edit) form.

75.9 Workflow to use the Service Test Manager

1 Create scheduled STM test suites for continual network monitoring, or non-scheduled STM test suites for on-demand troubleshooting, as required.

   i Create a schedule for an STM test suite that you want to execute regularly.

   ii Create a test policy for the test suite to define the generated tests for the test suite, as required.

iii Create the test suite.

- Choose the type of entity to which the suite applies.
  - Choose None if you want to include tests that are associated with different types of entities, such as VLL and Tunnel (SDP).
- Associate a test policy with the test suite, as required.
- Choose tests for the first-run test group, as required.
- Generate tests for the test suite, as required.
- Choose tests for the last-run test group, as required.

iv If required, modify the default size constraint policy or create additional size constraint policies to control the database resource usage by scheduled STM tasks.

The default size constraint policy limits the number of STM results to 50 000 to avoid system performance degradation. See chapter 43 for more information about creating size constraint policies to limit the space consumed by historical records in the 5620 SAM database.

v Apply schedules to test suites as required to create scheduled tasks.

vi Enable the scheduled tasks.

2 Monitor the diagnostic results from the scheduled test suites and the alarm list for indications of network or service faults and threshold-crossing alarms.

3 Use the scheduled or non-scheduled STM test suites and individual OAM tests to further investigate network or service faults.

75.10 Service Test Manager procedures

The following procedures describe how to perform 5620 SAM STM tasks.

Procedure 75-1 To configure OAM test IDs

Note — If the 5620 SAM is deployed in a redundant cluster configuration, you must perform this procedure on each 5620 SAM main server in the cluster.

1 Log in to the 5620 SAM main server station as a user with local administrator privileges.

Note — If the main server is installed on Solaris, you must log in as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory or folder, typically /opt/5620sam/server/nms/config on a Solaris station or C:\5620sam\server\nms\config on a Windows station.

3 Open the nms-server.xml file with a plain-text editor.

4 Locate the following tag that marks the beginning of the ID manager section:

```
<idManager>
```

5 Add the following before the end of the ID manager section:

<range name="testId" min="xx" max="yy"/>

where
xx is the minimum value for the test ID range; for example, 10000
yy is the maximum value for the test ID range; for example, 50000

Note 1 — The test ID ranges for the 5620 SAM servers must not overlap.

Note 2 — The primary and standby 5620 SAM servers must use the same test ID range.

The section reads as follows:

```
<idManager>

        <range name="routeDistinguisherType0AssignedValue" min="0"
max="4294967295"/>

        <range name="vrfTargetExtendedCommunityValue" min="0"
max="4294967295"/>

        <range name="outerEncapValue" min="1" max="4094"/>

        <range name="testId" min="10000" max="50000"/>

</idManager>
```

6 Save and close the nms-server.xml file.

7 Open a console window.

8 Navigate to the 5620 SAM server binary directory or folder, typically /opt/5620sam/server/nms/bin on Solaris or C:\5620sam\server\nms\bin on Windows.

9 Perform one of the following.

a If the 5620 SAM server is installed on a Solaris workstation, enter the following at the console prompt:

```
# ./nmsserver.bash read_config ↵
```

b If the 5620 SAM server is installed on a Windows PC, enter the following at the console prompt:

```
nmsserver.bat read_config ↵
```

The 5620 SAM server reads the nms-server.xml file and puts the configuration change into effect.

10 Close the console window.

Procedure 75-2 To modify the number of test results stored in the database

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Maximum Results button. The Service Test Manager (Edit) form opens.

3 Configure the Maximum Number of Results to Keep parameter.

4 Click on the OK button. The Service Test Manager (Edit) form closes.

5 Close the Service Test Manager form.

Procedure 75-3 To enable STM debug mode

1 Choose Application→User Preferences from the 5620 SAM main menu. The User Preferences form opens with the General tab displayed.

2 Configure the Debug STM Mode parameter.

3 Click on the OK button. The User Preferences form closes.

Procedure 75-4 To create a test policy

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Create Test Policy from the Create contextual menu. The Test Policy (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- NE Schedulable
- Entity Type
- Strategy
- Lightweight Execution
- Ignore Probe Results
- Accounting Files
- Continuously Executed

The Strategy parameter is only configurable when the Entity Type parameter is set to VLL Services.

The Lightweight Execution, Ignore Probe Results, Accounting Files, and Continuously Executed parameters are configurable when the NE Schedulable parameter is enabled.

The Continuously Executed parameter is only configurable when the Accounting Files parameter is enabled.

Note — You must enable the NE Schedulable parameter if the test suite that you create using the policy is to become an NE scheduled task.

5 Click on the Test Definitions tab button.

6 Click on the Add button to add a test definition to the test policy. A menu appears.

7 Choose an option from the menu. The options vary, depending on the Entity Type parameter value specified in step 4.

Each option in this step has three tabs that contain configurable parameters. The parameters that are common are listed in the following three paragraphs. Parameters that are specific to an option are displayed with the option.

The following configurable parameters appear on the General tab of the configuration form for every option in this step:

- Name
- NE Persistent
- Administrative State
- Description

The NE Persistent parameter is configurable only if you did not enable the NE Schedulable parameter in step 4.

The following configurable parameters appear on the Test Parameters tab of the configuration form for most options in this step:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)

A combination of the following configurable parameters appears on the Results Configuration tab of the configuration form for most options in this step:

- Probe History Size (rows)
- Test Failure Threshold
- Probe Failure Threshold
- Maximum Failures
- Trap Generation

8 To configure threshold-crossing alarms as required, perform the following:

a Click on the Thresholds tab.

b Perform steps 9 to 15 of Procedure 75-11.

9 Click on the OK button. The Definition Create form closes and a dialog box appears.

10 Click on the OK button. The Test Policy (Create) form reappears.

11 Perform steps 5 to 10 to add additional OAM tests to the policy.

12 Choose from the following options:

a To configure a site ping test definition for a VLL service, VPLS, VPRN service, mirror service, service connector, or router, click on the Add button and choose Service→Add Site Ping. The Service Site Ping Definition (Create) form opens.

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Use Local Tunnel
- Use Remote Tunnel

iii Click on the OK button and acknowledge the dialog box that appears. The Service Site Ping Definition (Create) form closes.

b To configure a VCCV ping test definition for a VLL service, click on the Add button and choose Service→Add VCCV Ping. The VCCV Ping Definition (Create) form opens.

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type

iii Click on the OK button and acknowledge the dialog box that appears. The VCCV Ping Definition (Create) form closes.

c To configure a VCCV trace test definition for a VLL service, choose Service→Add VCCV Trace. The VCCV Trace Definition (Create) form opens.

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Number of Test Probes
- Probe Interval (seconds)
- Probe Timeout (seconds)
- Size (octets)
- Forwarding Class
- Forwarding Profile
- Reply Type

iii Click on the OK button and acknowledge the dialog box that appears. The VCCV Trace Definition (Create) form closes.

d To configure a MAC ping test definition for a VLL service or VPLS, choose L2 Service→Add MAC Ping. The MAC Ping Definition (Create) form opens.

i Configure the following parameters on the General tab:

- Target MAC Address
- Source MAC Address

ii Click on the Test Parameters tab button.

iii Configure the parameters:

- Time To Live
- Forwarding Class
- Forwarding Profile
- Reply Control
- Control Plane

iv Click on the OK button and acknowledge the dialog box that appears. The MAC Ping Definition (Create) form closes.

e To configure an MEF MAC ping test definition for a VPLS, choose L2 Service→Add MEF MAC Ping. The MEF MAC Ping Definition (Create) form opens. This test is only supported on 7250 SAS-ES and 7250 SAS-ESA, Release 3.0 nodes.

i Configure the Target MAC Address parameter on the General tab.

ii Click on the Test Parameters tab button.

iii Configure the Size (octets) parameter.

iv Click on the Results Configuration tab button.

v Configure the Trap Generation parameter.

vi Click on the OK button and acknowledge the dialog box that appears. The MEF MAC Ping Definition (Create) form closes.

f To configure a multicast FIB ping test definition for a VPLS, choose Multicast→Add MFIB Ping. The MFIB Ping Definition (Create) form opens.

i Configure the following additional parameters on the General tab:

- Multicast Source
- Multicast Group

ii Click on the Test Parameters tab button.

iii Configure the parameters:

- Time To Live
- Reply via Control Plane

iv Click on the OK button and acknowledge the dialog box that appears. The MFIB Ping Definition (Create) form closes.

g To configure a ping test definition for a VPRN, choose L3 Service→Add VPRN Ping. The VPRN Ping Definition (Create) form opens.

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Time To Live
- Reply via Control Plane

iii Click on the OK button and acknowledge the dialog box that appears. The VPRN Ping Definition (Create) form closes.

h To configure a trace test definition for a VPRN, choose L3 Service→Add VPRN Trace. The VPRN Trace Definition (Create) form opens.

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Initial Time to Live
- Maximum Time to Live
- DiffServ Field
- Reply via Control Plane

iii Click on the OK button and acknowledge the dialog box that appears. The VPRN Trace Definition (Create) form closes.

i To configure a multicast routing information test definition for a VPRN or router, choose Multicast→Add mrinfo. The mrinfo Definition (Create) form opens.

There are no parameters that are specific to the mrinfo test definition.

i Configure the parameters.

ii Click on the OK button and acknowledge the dialog box that appears. The mrinfo Definition (Create) form closes.

j To configure a multicast trace test definition for a VPRN or router, choose Multicast→Add mtrace. The mtrace Definition (Create) form opens.

i Click on the Select button on the General tab to choose a multicast group to run the trace against.

ii Click on the Test Parameters tab button.

iii Configure the parameters:

- Initial Time to Live
- Maximum Number of Hops

iv Click on the OK button and acknowledge the dialog box that appears. The mtrace Definition (Create) form closes.

k To configure an ICMP ping test definition for a VPRN or router, choose ICMP→Add ICMP Ping. The ICMP Ping Definition (Create) form opens.

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Size (octets)
- Rapid
- Time To Live
- Data Pattern
- Positional Data Pattern
- DiffServ Field
- Bypass Routing
- Do Not Fragment
- Forwarding Class
- Forwarding Profile

iii Click on the OK button and acknowledge the dialog box that appears. The ICMP Ping Definition (Create) form closes.

l To configure an ICMP trace test definition for a VPRN or router, choose ICMP→Add ICMP Trace. The ICMP Trace Definition (Create) form opens.

i Click on the Test Parameters tab button.

ii Configure the parameters:

- DiffServ Field
- Time to Wait (milliseconds)

iii Click on the OK button and acknowledge the dialog box that appears. The ICMP Trace Definition (Create) form closes.

m To configure a tunnel ping test definition for a service tunnel, choose Service Transport→Add Tunnel Ping. The Tunnel Ping Definition (Create) form opens.

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Size (octets)
- Forwarding Class
- Forwarding Profile

iii Click on the OK button and acknowledge the dialog box that appears. The Tunnel Ping Definition (Create) form closes.

n To configure an MTU ping test definition for a service tunnel, choose Service Transport→Add MTU Ping. The MTU Ping Definition (Create) form opens.

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Size (octets)
- MTU Start Size (octets)
- MTU End Size (octets)
- MTU Step Size (octets)

iii Click on the OK button and acknowledge the dialog box that appears. The MTU Ping Definition (Create) form closes.

o To configure a ping test definition for an LSP, choose MPLS→Add LSP Ping. The LSP Ping Definition (Create) form opens.

i In the General tab, configure the Target Type parameter.

ii Click on the Test Parameters tab button.

iii Configure the parameters:

- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

iv Click on the OK button and acknowledge the dialog box that appears. The LSP Ping Definition (Create) form closes.

p To configure a trace test definition for an LSP, choose MPLS→Add LSP Trace. The LSP Trace Definition (Create) form opens.

i In the General tab, configure the Target Type parameter.

ii Click on the Test Parameters tab button.

iii Configure the parameters:

- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

iv Click on the OK button and acknowledge the dialog box that appears. The LSP Trace Definition (Create) form closes.

q To configure a ping test definition for a P2MP LSP, choose MPLS→Add P2MP LSP Ping. The P2MP LSP Ping Definition (Create) form opens.

i In the General tab, configure the Select All S2L Paths parameter.

ii Click on the Test Parameters tab button.

iii Configure the parameters:

- Size (octets)
- Time To Live
- Forwarding Class
- Forwarding Profile

iv Click on the OK button and acknowledge the dialog box that appears. The LSP Ping Definition (Create) form closes.

r To configure a trace test definition for a P2MP LSP, choose MPLS→Add P2MP LSP Trace. The P2MP LSP Trace Definition (Create) form opens.

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Size (octets)
- Initial Time to Live
- Maximum Time to Live
- Forwarding Class
- Forwarding Profile

iii Click on the OK button and acknowledge the dialog box that appears. The LSP Trace Definition (Create) form closes.

s To configure a ping test definition for an ATM PVC, choose L1/L2→Add ATM Ping. The ATM Ping Definition (Create) form opens.

i Click on the Test Parameters tab button.

ii Configure the parameters:

- Loopback Location (hex)
- Destination Type

iii Click on the OK button and acknowledge the dialog box that appears. The LSP Trace Definition (Create) form closes.

13 Repeat step 12 for each test definition that you want to include in the test policy.

14 Click on the OK button. The Test Policy (Create) form closes.

15 Close the Service Test Manager form.

Procedure 75-5 To configure a CPE SLA test (OS 6250 Metro only)

1 Configure the test components.

i Choose Tools→CPE Test-Head Profile from the 5620 SAM main menu. The Manage CPE Test-Head Profile form opens.

ii Click on the Create button. The CPE Test-Head Profile, Global Policy (Create) form opens.

iii Configure the following parameters:

- Name
- Description
- Source Endpoint
- Destination Endpoint
- Source MAC
- Destination MAC
- Direction
- Role
- Tx Rate (kbps)
- Frame Size (bytes)

2 Configure the Frame Type parameter, which causes the form to refresh and display additional parameters. Configure the following parameters:

- VLAN-Tag
- Priority
- Pattern
- Drop Enable

3 Perform one of the following:

a If the Frame Type parameter is set to Ethernet, configure the Ether Type parameter.

b If the Frame Type parameter is set to IPV4, configure the following parameters:

- Source IP
- Destination IP
- Source Port
- Destination Port
- TTL
- Protocol
- TOS

4 Click on the OK button.

5 On the General tab of the CPE Test-Head Profile - test, Global Policy (edit) form, click on the Switch mode button to change the Global policy configuration mode to Released.

6 Click on the Distribute button to manually distribute the test policy locally to managed OS 6250 devices. Policies are also automatically distributed to devices when they are used by resources on the device. See chapter 43 for more information about policies and policy distribution.

7 Configure the VLAN and port settings.

i Click on the Local Definitions tab button.

ii Choose an OS 6250 from the list and click on the Properties button. The CPE Test-Head Profile form opens with the General tab displayed.

iii In the VLAN panel, click on Select button for Service ID.

iv Choose a device from the list and click on the OK button.

v Click on the Switch mode button to change the mode to Local Edit only.

vi Click on the Select button for Port.

vii Choose a port from the list and click on the OK button.

viii Click on the Apply button and close the form.

8 Configure the test execution details.

i Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager (STM) form opens.

ii Click on the Create button and choose AOS CPE→CPE SLA Test. The CPE SLA Test form opens with the General tab displayed.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Persistent

iv In the Generator panel, click on the Select button. The Select Generator form opens.

v Choose a generator profile from the list and click on the OK button to close the form.

vi In the Analyzer panel, click on the Select button. The Select Analyzer form opens.

vii Choose an analyzer profile from the list and click on the OK button to close the form.

viii Click on the Test Parameters tab. Configure the following parameters:

- Number of Test Iteration
- Test Iteration Duration (seconds)
- Generator Tx Rate (kbps)
- Generator Frame Size (bytes)
- Increase Tx Rate Every Iteration by (kbps)

ix Click on the OK button.

9 In the Service Test Manager (STM) form, configure the drop-down menu to display CPE SLA Tests and click on the Search button.

10 Choose the CPE SLA test you created in this procedure and click on the Execute button to start the test.

11 To view the test results, click on the Results tab.

Procedure 75-6 To create a test suite

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click on the Create button.

3 Choose Create Test Suite from the contextual menu. The Test Suite (Create) form opens.

4 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Administrative State
- Entity Type
- Validation Test Suite
- NE Schedulable
- First Run Execution Sequence
- Last Run Execution Sequence

Note 1 — The Entity Type parameter specifies that only test policies created for the same entity type are available for the test suite. The parameter also restricts the predefined tests that are available as first-run or last-run tests to those that apply to the entity type.

Note 2 — To create a test suite that includes tests for different entity types, specify None as the Entity Type parameter value. This allows you to choose any predefined test as a first-run or last-run test.

Note 3 — Specifying None as the Entity Type parameter value disables the generation of tests in a test suite; the policy that STM uses to generate tests must be associated with a specific entity type.

Note 4 — The Validation Test Suite parameter specifies that the test suite is used to validate the connectivity of the tested service entity to which it is applied. OAM validation tests are not supported for HVPLS.

Click on the Validate button on the associated service or service tunnel configuration form to run the OAM validation test. The results of the OAM validation test are indicated by the OAM Validation Failed operational flag.

5 To create a scheduled task, see procedure 75-7.

6 If you chose None as the Entity Type parameter value in step 4, go to step 16. To create a scheduled task, go to step 7.

7 Click on the Test Policy tab button.

8 Click on the Add button to choose a test policy to associate with the test suite. The Select Test Policy - Test Suite form opens.

9 Click on the Search button to display a list of available test policies.

Note — Only test policies that apply to the type of entity specified by the Entity Type parameter in step 4 appear in the list.

10 Choose a test policy from the list and click on the OK button. The test policy appears on the Test Policy tab.

11 Click on the Tested Entities tab button.

12 Click on the Add button to choose a service, transport element, or device as the object against which the test suite is run. The Select Tested Entity - Test Suite form opens.

13 Click on the Search button to display a list of available entities.

Note — Only entities that match the type of entity specified in the test policy appear in the list.

14 Choose an entity from the list and click on the OK button. The Select Tested Entity - Test Suite form closes and an entry for the entity appears in the list on the Tested Entities tab.

15 Repeat steps 12 to 14 for each additional entity that you want to specify.

16 Click on the First Run Tests tab button.

17 Click on the Add button to choose a predefined test that is to execute before the generated tests in the suite. The Select Test - Test Suite form opens.

18 Click on the Search button to display a list of available tests.

19 Choose a test from the list and click on the OK button. The Select Test - Test Suite form closes and the test entry appears on the First Run Tests tab.

20 Repeat steps 17 to 19 for each additional first-run test that you want to specify.

21 When there is more than one test in the first-run list, the Move Up and Move Down buttons are active. Select a test entry and click on these buttons as needed to reorder the first-run test execution sequence, if required.

22 Click on the Last Run Tests tab button.

23 Click on the Add button to include a predefined test that is to execute after the other tests in the suite have completed. The Select Test - Test Suite form opens.

24 Click on the Search button to display a list of available tests.

25 Choose a test from the list and click on the OK button. The Select Test - Test Suite form closes and the test entry appears on the Last Run Tests tab.

26 Repeat steps 23 to 25 for each additional last-run test that you want to specify.

27 When there is more than one test in the last-run list, the Move Up and Move Down buttons are active. Select a test entry and click on these buttons as needed to reorder the last-run test execution sequence, if required.

28 Click on the Apply button to save the changes. Additional buttons at the bottom of the form become active.

29 If you chose None as the Entity Type parameter value in step 4, go to step 33.

30 Click on the Generated Tests tab button.

31 Click on the Generate Tests button. The 5620 SAM begins generating tests for the test suite based on the test policy. The tests appear in a list on the Generated Tests form as they are generated.

Note — When the test policy or the configuration of an entity on the Tested Entities tab changes, you must regenerate the tests in the test suite by clicking on the Generate Tests button.

32 Click on the Generation Logs tab button to view the log file that the 5620 SAM creates during test generation, as required.

Note — Generation Logs messages only appear if any failures occur during the test generation process.

33 Click on the OK button to close the Test Suite (Create) form.

34 Close the Service Test Manager form.

Procedure 75-7 To schedule the execution of a test suite using a SAM schedule

To schedule the execution of a test suite using a SAM schedule, you must first create the SAM schedule. See chapter 74 for information about creating schedules.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Suite (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test suites appears.

5 Double-click on the test suite that you want to schedule. The Test Suite (Edit) form opens with the General tab displayed.

6 Click on the Schedule button. The SAM Scheduled Task (Create) form opens with the General tab displayed.

7 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

Caution — Setting the Administrative State parameter to Enabled puts the scheduled task into effect according to the schedule parameters. Ensure that the test suite and the objects to which it applies are appropriately configured before you set the parameter to Enabled.

8 Click on the Select button. The Select Schedule - SAM Scheduled Task form opens.

9 Select a schedule and click on the OK button. The chosen schedule appears on the form.

10 Click on the OK button. The SAM Scheduled Task (Create) form closes and the Test Suite (Edit) form reappears.

11 Close the Test Suite (Edit) form.

12 Close the Service Test Manager form.

Procedure 75-8 To schedule the execution of a test suite using an existing NE schedule

To schedule the execution of a test suite using an existing NE schedule, perform Procedure 74-7 to turn up the NE scheduled task.

Procedure 75-9 To execute a test suite

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Suite (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test suites appears.

5 Select a test suite in the list and click on the Properties button. The Test Suite (edit) form opens with the General tab displayed.

6 Click on the Execute button. Execution of the test suite begins and the Test Suite (edit) form displays the Results tab. You can view the test results when the test execution is complete.

Note — You can run an OAM validation test from the Properties form of a service tunnel or an applicable service. See the applicable service management chapter for more information.

7 Close the Test Suite (edit) form.

Procedure 75-10 To configure threshold-crossing alarms on NE-schedulable OAM tests within a test policy

Perform this procedure to configure threshold-crossing alarms for test policies, test definitions, and assurance tests that are NE-schedulable. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level.

Configuring threshold-crossing alarms on a test definition within the test policy creates a threshold definition that applies to generated tests. Configuring threshold-crossing alarms directly on a test that is NE-schedulable applies just to the test.

Note — If you modify a test policy associated with a test suite, you must regenerate the generated tests in the test suite.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Policy (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test policies is displayed.

5 Choose an NE-schedulable policy from the list and click on the Properties button. The Test Policy (Edit) form opens with the General tab displayed.

6 Click on the Test Definitions tab. A list of tests associated with the policy opens.

7 Select a test from the list and click on the Properties button. The Test Definition—Test Policy (Edit) form opens with the General tab displayed.

8 Click on the Thresholds tab.

9 Click on the Add button. The Threshold Event Definition (Create) form opens with the General tab displayed.

10 Configure the parameters:

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

11 Click on the Rising Threshold tab.

12 Configure the Threshold Value parameter.

13 Click on the Falling Threshold tab.

Note — The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the Threshold Event Definition (Create) form.

14 Configure the Threshold Value parameter.

15 Click on the OK button. The Threshold Event Definition, (Create) form closes and a dialog box appears.

16 Click on the OK button. The test appears on the list.

17 Repeat steps 9 to 16 to configure threshold events on additional tests.

18 Click on the OK button. The Test Definition—Test Policy (Edit) form closes and the Test Policy (Edit) form reappears.

19 Click on the OK button. A dialog box appears.

20 Confirm the action. The Test Policy (Edit) form closes and the Service Test Manager form reappears.

21 Close the Service Test Manager form.

Procedure 75-11 To configure threshold-crossing alarms on non-NE-schedulable OAM tests within a test policy

You can configure threshold-crossing alarms for test policies, test definitions, and assurance tests that are non-NE-schedulable. An alarm is raised when a threshold is crossed, either because the value rose above or fell below the configured level.

Non-NE-schedulable OAM tests can be configured as NE persistent. NE persistent tests are deployed to the network node after the first execution and remain on the node each time the test is executed. The type of threshold-crossing event available for selection depends on the test type.

Configuring threshold-crossing alarms on a test definition within the test policy creates a threshold definition that applies to generated tests. Configuring threshold-crossing alarms directly on a test that is non-NE-schedulable applies just to the test.

Note — If you modify a test policy associated with a test suite, you must regenerate the generated tests in the test suite.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Policy (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test policies is displayed.

5 Choose a non-NE-schedulable policy from the list and click on the Properties button. The Test Policy (Edit) form opens with the General tab displayed.

6 Click on the Test Definitions tab. A list of tests associated with the policy opens.

7 Select a test from the list and click on the Properties button. The Test Definition—Test Policy (Edit) form opens with the General tab displayed.

8 Click on the Thresholds tab.

Note — The Thresholds tab is enabled or disabled depending on the test type selected in step 7. Threshold alarm events can not be configured for Site Ping, mrinfo, mtrace, VPRN Trace and Mtu Ping tests.

9 Click on the Add button. The Threshold Event Definition (Create) form opens with the General tab displayed.

10 Configure the parameters.

- Type
- Generate Alarm on Rising Threshold
- Clear Alarm on Falling Threshold
- Update Test Result Status
- Include Falling Threshold

11 Click on the Rising Threshold tab.

12 Configure the Threshold Value parameter.

13 Click on the Falling Threshold tab.

Note — The Falling Threshold tab can be accessed only when the Include Falling Threshold parameter is enabled on the General tab of the Threshold Event Definition, (Create) form.

14 Configure the Threshold Value parameter.

15 Click on the OK button. The Threshold Event Definition, (Create) form closes and a dialog box appears.

16 Click on the OK button. The test appears on the list.

17 Repeat steps 9 to 16 to configure threshold events on additional tests in the policy.

18 Click on the OK button. The Test Definition, Test Policy (Edit) form closes and the Test Policy (Edit) form reappears.

19 Click on the OK button. A dialog box appears.

20 Confirm the action. The Test Policy (Edit) form closes and the Service Test Manager form reappears.

21 Close the Service Test Manager form.

Procedure 75-12 To modify a test policy

Note — If you modify a test policy associated with a test suite, you must regenerate the Generated tests in the test suite.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Policy (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test policies appears.

5 Select a test policy and click on the Properties button. The Test Policy (Edit) form opens with the General tab displayed.

6 Configure the Name and Description parameters, as required.

7 Click on the Test Definitions tab button.

8 Perform one of the following:

   a Select a test definition in the list and click on the Properties button.

   b Click on the Add button to add a test definition to the test policy.

9 Click on the OK button to return to the Policy form.

10 Modify the parameters for the test definition, as required.

11 Click on the Update Test Suites button to apply the test policy changes to all test suites that are associated with the test policy.

Caution — The operation of scheduled test suites that use the test policy may be adversely affected if you modify the test policy while a scheduled task for the suite is enabled.

12 Click on the Usages tab button to view a list of the test suites that use the test policy.

13 Click on the OK button. A dialog box appears.

14 Click on the Yes button to confirm the action. The Test Policy (Edit) form closes and the Service Test Manager form reappears.

15 Click on the Close button to close the Service Test Manager form.

Procedure 75-13 To modify a test suite

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Suite (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test suites appears.

5 Select a test suite and click on the Properties button. The Test Suite (Edit) form opens with the General tab displayed. Use the parameters on this tab to change the execution order of tests in the First run and Last run test groups, as required.

The following tabs list the test-suite components that you can individually or collectively add to or remove from the test suite:

- Test Policy tab — displays the test policy that is associated with the test suite
- Tested Entities tab — lists the entities that are objects of the tests in the test suite
- First Run Tests tab — lists the group of tests in the test suite that run first
- Generated Tests tab — lists the generated tests that are included in the test suite
- Last Run Tests tab — lists the group of tests in the test suite that run last

The following tabs display information about the creation and execution of the test suite:

- Results tab — lists the historical results that are returned by each execution of the test suite
- Generation Logs tab — lists the log entries that are created during test generation for the test suite
- Faults tab — displays the faults associated with the test suite

Note — Generation Logs messages only appear if any failures occur during the test generation process.

6 Modify the parameters for the test suite, as required.

To configure an item on a tab that contains a list of test-suite components, select the item and click on the Properties button.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button to confirm the action. The Test Suite (Edit) form closes and the Service Test Manager form reappears.

9 Click on the Close button to close the Service Test Manager form.

Procedure 75-14 To view aggregated test suite results

Perform this procedure to view test suite results from the Test Suite Result (Edit) form.

Note 1 — You can also view the test suite results for an object from the Tests tab of the configuration form for the object.

Note 2 — You can reorder a column in a tabular information view by dragging the column heading to the desired position, then right-clicking on the column heading and choosing Save Table Preferences.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager (STM) form opens.

2 Choose Test Result (Assurance) from the object drop-down list.

3 Click on the Aggregated Result (Assurance) icon below the Result (Assurance) icon to expand the selection.

4 Choose one of the following objects in the tree display below Aggregated Result (Assurance).

   a Select Test Definition Result (Assurance) to create a search filter based on a test definition.

   b Select Test Policy Result (Assurance) to create a search filter based on a test policy.

   c Select Test Suite Result (Assurance) to create a search filter based on a test suite.

5 Configure the filter criteria.

Caution — Ensure that the filter properties chosen are sufficient to appropriately limit the number of returned result entries. Otherwise, the number of returned entries may exceed the maximum number that the 5620 SAM permits, and valid entries may not appear in the list.

6 Click on the Search button. A list of test suite results appears.

7 Select a test suite result and click on the Properties button. The Test Suite Result (Edit) form opens with the General tab displayed.

8 View the general results on the General tab.

Note — If the test suite uses a test policy with the Lightweight Execution parameter enabled, only the General and Failed Test tabs are available.

9 Click on the First Run Results tab button to view test results from individual tests in the first-run test group of the test suite.

10 Click on the Summary By Policy tab button to view test results for individual tests in the test suite, listed by test policy.

11 Click on the Summary By Definition tab button to view test results for individual tests in the test suite, listed by test definition.

12 Click on the Last Run Results tab button to view test results from individual tests in the last-run test group of the test suite.

13 Close the Test Suite Result (Edit) form.

14 Click on the Close button to close the Service Test Manager form.

Procedure 75-15 To view and compare test suite results for a tested entity

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Suite (Assurance) from the object drop-down menu.

3 Configure the filter criteria.

4 Click on the Search button. A list of test suites appears.

5 Choose a test suite in the list and click on the Properties button. The Test Suite (edit) form opens with the General tab displayed.

6 Click on the Tested Entities tab button to view a list of entities tested by the test suite.

7 Choose a tested entity from the list and click on the Show Results button. The Tested Entity Result (edit) form opens.

8 Configure the filter criteria.

9 Click on the Search button. A list of test results appears.

10 Choose a test result from the list and click on the Properties button. The result form for the selected test opens.

11 Close the result form.

12 If you need to compare the results of two tests of the same type, choose two results for the test from the displayed list and click on the Compare button; the Difference form opens. Otherwise, go to step 15.

13 Compare the results of the test results.

14 Close the Difference form.

15 Close the Tested Entity Result (edit) form.

16 Close the Test Suite (Edit) form.

17 Close the Service Test Manager (STM) form.

Procedure 75-16 To view and compare test suite results

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Choose Test Result (Assurance) from the object drop-down list.

3 Configure the filter criteria.

4 Click on the Search button. A list of test results appears.

5 Choose a test result and click on the Properties button to view the properties of the test. The selected test type result (Edit) form opens.

6 If you need to compare the results of two tests within a test suite, choose two test results of the same type within a test suite and click on the Compare button; the Difference form opens. You can view the test values for each test. Otherwise, go to step 8.

7 Close the Difference form.

8 Close the test type result (Edit) form.

9 Close the Service Test Manager (STM) form.

Procedure 75-17 To delete a test suite

1 If the test suite is scheduled, you must remove the scheduled task associated with the test suite before you can delete the test suite. See chapter 74 for more information.

2 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

3 Choose Test Suite (Assurance) from the object drop-down list.

4 Configure the filter criteria.

5 Click on the Search button. A list of test suites appears.

6 Select a test suite in the list and click on the Delete button. A dialog box appears.

7 Click on the Yes button to confirm the action. The test suite is deleted and removed from the list.

8 Click on the Close button to close the Service Test Manager form.

76 — Ethernet CFM

76.1 Ethernet CFM overview

The 5620 SAM Ethernet Connectivity Fault Management, or Ethernet CFM, function is implementation of the IEEE 802.1ag OAM standard. This standard describes protocols for detecting, isolating, and reporting connectivity faults in an Ethernet network. You can use Ethernet CFM for the following:

- path discovery
- fault detection
- fault isolation
- fault notification

The IEEE 802.1ag standard partitions a network into eight hierarchical levels called maintenance domains, or MDs. An MD is a network, or part of a network, that is provisioned with a set of maintenance entity groups, or MEGs, which are groups of service sites. Typically, a MEG represents one service and consists of a group of maintenance end points, or MEPs. Only one MEG can be associated with a service, but one service can be associated with multiple MEGs. MDs and MEGs are distributed to NEs using the 5620 SAM policy distribution framework.

Ethernet CFM diagnostic tests detect connectivity failures between pairs of local and remote maintenance end points, or MEPs, in a MEG. Each MEP is a reference point that can initiate or terminate one of the following diagnostic tests:

- CFM loopback
- CFM link trace
- CFM continuity check
- CFM one-way delay
- CFM two-way delay
- CFM Eth test
- CFM single-ended loss (7705 SAR only)

A CFM continuity check test is automatically generated when you create an MD. When you execute the test and a connectivity fault is present, the MEP that detects the fault raises an alarm. See Chapter 35 for information about a specific Ethernet CFM diagnostic test.

MEPs

MEPs are configured at the edge of an MD and perform the following functions:

- periodically send CFM continuity check messages
- validate CFM PDU replies
- discard CFM PDU messages that are not in the MEP configuration
- send and receive loopback and link trace messages

MEPs can be added to services directly, or during Ethernet CFM test configuration. Each MEP is assigned an up or down direction. An up MEP is provisioned on an ingress port, and monitors the forwarding path inside a bridge NE to the egress port. A down MEP is provisioned on an egress port, and monitors the forwarding path between bridge NEs.

You can configure an initial MEP ID for automatic MEP ID assignment on an NE. See Procedure 76-2 for more information.

An up MEP can be associated with the following object types:

- Epipe and VPLS SAPs
- Epipe spoke SDP bindings
- VPLS mesh and spoke SDP bindings
- VPLS and MVPLS B-sites, as virtual MEPs
- B-L2 access interfaces
- OmniSwitch VLAN SAPs

A down MEP can be associated with the following object types:

- Epipe, Ipipe, IES, VPLS, and VPRN SAPs
- Epipe and IES spoke SDP bindings
- VPLS mesh and spoke SDP bindings
- B-L2 access interfaces
- MVPLS access interfaces
- OmniSwitch VLAN SAPs

A virtual MEP is an up MEP that is created on a B-VPLS or B-MVPLS site when a CFM continuity check test is run. Each virtual MEP transmits a CFM continuity check stream on all SAPs and SDPs of the site. A virtual MEP uses the site B-MAC address, if configured; otherwise, it uses the shelf MAC address. See chapter 68 for information about assigning virtual MEPs in B-VPLS and B-MVPLS.

The following rules apply to virtual MEP management:

- One virtual MEP can be configured on a VPLS or MVPLS B-site.
- All regular MEPs on SAPs and SDP bindings in the same MEG as a virtual MEP must be configured as up MEPs.
- Regular MEPs in the same MEG and on the same B-site as a virtual MEP cannot be enabled when the virtual MEP is enabled.
- Virtual MEPs can be created in a MEG only when MIP creation in the MEG is disabled.

MIPs

Maintenance intermediate points, or MIPs, are internal points in an MD that perform the following functions:

- validate received CFM PDUs
- validate and respond to link trace messages
- validate and respond to loopback messages

A MIP consists of two half-function objects that allow the MIP to be recognized as a MIP in one MD level and as a MEP on a higher level.

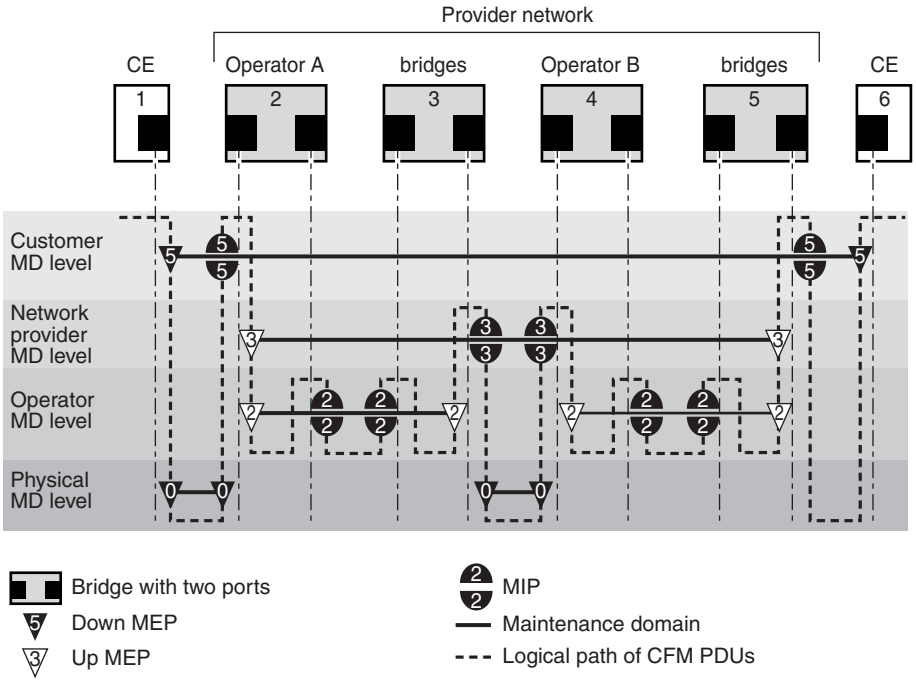
Sample Ethernet CFM implementation

Figure 76-1 shows an example of MDs, MEPs, and MIPs in a IEEE 802.1ag network that consists of two operator areas, for example, services in the provider network, that are joined to create a network path for customer traffic. The number on an object identifies the associated MD, which is one of the following:

- MD 5—end-to-end customer path
- MD 3—end-to-end network provider path
- MD 2—paths within services
- MD 0—physical path

MD 5 provides access to a down MEP on each CE device, and to a MIP on each PE bridge. MD 3 provides access to an up MEP on each PE bridge, and to a MIP on each bridge between groups of operator bridges. MD 2 provides access to the up MEPs and MIPs in each service. MD 0 provides access to MEPs for checking the physical connectivity between NEs.

Figure 76-1 Ethernet CFM objects in example network



76.2 Workflow to configure Ethernet CFM

1 Create an MD for each level at which Ethernet connectivity is to be monitored. If the MD is to be used for Y.1731 performance measurement tests, you must set the name type to none.

2 Create one or more global MEGs in each MD. Each MEG must be associated with one service or Ethernet path. Creating a global MEG generates a CFM continuity check test.

3 Execute the generated CFM continuity check test, as required.

4 Execute other Ethernet CFM tests, as required.

76.3 Ethernet CFM procedures

The following procedures describe how to configure and manage Ethernet CFM.

Procedure 76-1 To configure an Ethernet CFM MD

1 Choose Tools→Ethernet CFM→Maintenance Domain from the 5620 SAM main menu. The Maintenance Domain Policies form opens.

2 Perform one of the following.

a Edit an existing MD. Use the configurable filter to search for an MD and click on the Properties button. The Maintenance Domain (Edit) form opens.

b Create an MD. Perform the following steps.

i Click on the Create button. The Maintenance Domain (Create) form opens.

ii Configure the parameters:

- MD Mgr Object ID
- Auto-Assign ID
- Name Type
- Name
- Level

iii Click on the Apply button. The form displays additional tabs, and the form name changes to Maintenance Domain (Edit).

iv Click on the Switch Mode button. A dialog box appears.

v Click on the Yes button. The Configuration Mode changes to Released.

3 Configure the Description parameter.

4 To add a Global MEG to the MD, click on the Global Maintenance Entity Group tab button. Otherwise, go to step 19.

5 Click on the Add button. The Global Maintenance Entity Group (Create) form opens with the General tab displayed.

6 Configure the following parameters:

- Name
- Description
- Administrative State
- Name Format
- Name
- Initial CCM Interval
- Initial MHF-Creation

Note — When the Initial CCM Interval parameter is set to 10 ms or 100 ms, you cannot configure automatic MEP creation in step 8.

7 Click on the OK button.

8 To associate a service with the Global MEG, perform the following steps.

i Click on the Service tab button.

ii Click on the Add button. The Service (Create) form opens.

iii Click on the Select button. The Select Service form opens.

iv Click on the Search button. A list of services is displayed.

v Select a service in the list and click on the OK button. The Select Service form closes, and the service information is displayed on the Service (Create) form.

vi Configure the following parameters:

- Auto MEG Site Creation
- MEP(s) Creation on Access Interfaces
- Direction
- MEP(s) Creation on SDP Bindings
- Direction
- Virtual MEP(s) Creation on B-Sites
- MIP(s) Creation on Access Interfaces
- MIP(s) Creation on SDP Bindings

Note — When the Initial CCM Interval parameter in step 6 is set to 10 ms or 100 ms, you cannot configure the MEP(s) Creation on Access Interfaces, MEP(s) Creation on SDP Bindings, or Virtual MEP(s) Creation on B-Sites parameters.

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The service is listed on the Global Maintenance Entity Group (Create) form.

9 Perform the following steps to add an Ethernet path to the Global MEG, if required.

i Click on the Ethernet Path tab button.

ii Click on the Add button. The Ethernet Path (Create) form opens.

Note — You must specify an Ethernet tunnel path or Ethernet ring path on this form.

iii To add an Ethernet tunnel path, click on the Select button in the Ethernet Tunnel Path panel. The Select Ethernet Tunnel Path form opens. Otherwise, go to step 9 vi.

iv Select an Ethernet tunnel path in the list and click on the OK button. The Select Ethernet Tunnel Path form closes, and the Ethernet tunnel path is displayed on the Ethernet Path (Create) form.

v Go to step 9 viii.

vi Click on the Select button in the Ethernet Ring Path panel. The Select Ethernet Ring Path form opens.

vii Select an Ethernet ring path in the list and click on the OK button. The Select Ethernet Ring Path form closes, and the Ethernet ring path is displayed on the Ethernet Path (Create) form.

viii Configure the parameters:

- Auto-Assign ID
- Object ID
- Run Continuity Check Protocol
- Set Control MEP property on created MEPs

ix Click on the OK button. A dialog box appears.

x Click on the OK button. The Ethernet path is displayed on the Global Maintenance Entity Group (Create) form.

10 Perform the following steps to add a MEG to the MD.

i Click on the Maintenance Entity Group tab button.

ii Click on the Add button. The Maintenance Entity Group (Create) form opens with the General tab displayed.

iii Click on the Select button. The Select Site form opens.

iv Select an NE in the list and click on the OK button. The Select Site form closes, and the Maintenance Entity Group (Create) form displays the NE information.

v Configure the parameters:

- CCM interval
- VLAN ID
- MHF-Creation

The MHF-Creation and VLAN ID parameters are configurable only when the selected NE is an OmniSwitch.

vi To associate a template with the MEG, click on the Templates tab button. Otherwise, go to step 10 ix.

vii Click on the Select button. The Select Associated Template - Maintenance Entity Group form opens.

viii Select a template in the list and click on the OK button. The Select Associated Template - Maintenance Entity Group form closes, and the Maintenance Entity Group (Create) form displays the template information.

ix Click on the Service tab button. A list of services is displayed.

x Click on the Add button. The MEG Service (Create) form opens.

xi Configure the parameters:

- Service ID
- MHF-Creation
- VLAN ID
- Id-Permission

xii Click on the OK button. The MEG Service (Create) form closes.

xiii Click on the Apply button. A dialog box appears.

xiv Click on the OK button. The form name changes to Maintenance Entity Group (Edit), and the service is listed on the form, which displays additional tab buttons.

11 Perform the following steps to add a managed MEP to the MEG, if required.

i Click on the Managed MEP tab button.

ii Click on the Add button. The MEP (Create) form opens.

iii Configure the parameters:

- ID
- Auto-Assign ID
- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- Mac Address
- Fault Propagation
- Type
- Interface Type
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

Note — The Interface Type parameter is configurable when the Type parameter is set to Regular.

iv If the Type parameter is set to Virtual, go to step 10 ix.

v Click on the Select button in the bottom panel to choose an object of the type specified by the Interface Type parameter. The Select *object_type* form opens.

vi Click on the Search button. A list of objects is displayed.

vii Select an object in the list and click on the OK button. The Select *object_type* form closes, and the object information is displayed on the MEP (Create) form.

viii Go to step 10 xii.

ix Click on the Select button in the bottom panel to choose a site for the virtual MEP. The Select Service Site Pointer form opens.

x Click on the Search button. A list of sites is displayed.

xi Select a site in the list and click on the OK button. The Select Service Site Pointer form closes, and the site information is displayed on the MEP (Create) form.

xii If the MD has a Name Type of none and the global MEG has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable. Otherwise, go to step 10 xvii.

xiii Click on the Y.1731 Tests tab button.

xiv Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

xv Click on the AIS tab button.

xvi Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

xvii Click on the OK button. A dialog box appears.

xviii Click on the OK button. The MEP (Create) form closes, and the managed MEP is listed on the Maintenance Entity Group (Edit) form.

12 Perform the following steps to add a remote MEP to the MEG, if required.

Note 1 — You can add only one entry to the remote MEP list for a 7705 SAR.

Note 2 — When you execute a CCM test or synchronize the managed and unmanaged remote MEP lists, the 5620 SAM automatically distributes the local MEP and the remote MEP to the remote MEP list, except for 7705 SAR NEs, which are excluded from automatic MEP -distribution.

Note 3 — If a local MEP and the corresponding remote MEP are on the same OmniSwitch, deleting the remote MEP results also deletes the corresponding local MEP.

i Click on the Remote MEP tab button. The Remote MEP (Create) form opens.

ii Configure the MEP ID parameter.

iii Click on the OK button. A dialog box appears.

iv Click on the OK button. The remote MEP is listed on the Maintenance Entity Group (Edit) form.

13 Click on the OK button. The Maintenance Entity Group (Edit) form closes, and the MEG is listed on the Global Maintenance Entity Group (Edit) form.

14 Perform the following steps to add an unmanaged remote MEP to the global MEG, if required.

i Click on the Unmanaged Remote MEP tab button.

ii Click on the Add button. The Unmanaged Remote MEP form opens.

iii Configure the parameters:

- MEP ID
- MEP Mac Address

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The unmanaged remote MEP is listed on the Global Maintenance Entity Group (Edit) form.

15 Perform the following steps to add a managed MEP to the global MEG, if required.

i Click on the Managed MEP tab button.

ii Click on the Add button. The MEP (Create) form opens.

iii Click on the Select button. The Select Maintenance Entity Group form opens.

iv Select a MEG in the list and click on the OK button. The Select Maintenance Entity Group form closes, and the MEG information is displayed on the MEP (Create) form.

v Configure the parameters:

- Direction
- Administrative State
- CCM Messages Enabled
- Priority Level for CCM Messages
- Low-priority Defect
- Mac Address
- Fault Propagation
- Type
- Interface Type
- Fault Alarm Time (centiseconds)
- Fault Reset Time (centiseconds)

Note — The Interface Type parameter is configurable when the Type parameter is set to Regular.

vi If the Type parameter is set to Virtual, go to step 15 xi.

vii Click on the Select button in the bottom panel to choose an object of the type specified by the Interface Type parameter. The Select *object_type* form opens.

viii Click on the Search button. A list of objects is displayed.

ix Select an object in the list and click on the OK button. The Select *object_type* form closes, and the object information is displayed on the MEP (Create) form.

x Go to step 15 xiv.

xi Click on the Select button in the bottom panel to choose a site for the virtual MEP. The Select Service Site Pointer form opens.

xii Click on the Search button. A list of sites is displayed.

xiii Select a site in the list and click on the OK button. The Select Service Site Pointer form closes, and the site information is displayed on the MEP (Create) form.

xiv If the MD for the MEP has a Name Type of none and its Maintenance Association has a Name Format of icc-based, the Y.1731 Tests and AIS tabs are configurable. Otherwise, go to step 15 xix.

xv Click on the Y.1731 TEST tab.

xvi Configure the parameters:

- Eth Test Enabled
- Eth Test Pattern
- Eth Test Threshold (number of bit errors)
- One-way-delay Test Threshold (seconds)

The Eth Test Pattern parameter is configurable when the Eth Test Enabled parameter is enabled.

xvii Click on the AIS tab.

xviii Configure the parameters:

- AIS Enabled
- AIS Meg Level
- AIS Priority
- AIS Interval (seconds)

The AIS Meg Level parameter is configurable when the AIS Enabled parameter is enabled.

xix Click on the OK button. A dialog box appears.

xx Click on the OK button. The MEP is listed on the Global MEG (Create) form.

16 Click on the Synchronize Remote MEPs button to distribute the MEPs to the NEs.

17 Click on the OK button. A dialog box appears.

18 Click on the Yes button. The Global MEG (Create) form closes, and the Maintenance Domain (Edit) form reappears.

19 Close the Maintenance Domain (Edit) form.

20 Close the Manage Maintenance Domain Policies form.

Procedure 76-2 To configure automatic MEP ID assignment on an NE

Perform this procedure to configure an initial MEP ID value on an NE for automatic MEP creation.

1 Choose Equipment from the navigation tree view selector.

2 Right-click on an NE instance and choose Properties from the contextual menu. The NE properties form opens.

3 Click on the Globals tab button.

4 Configure the MEP Id parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The NE properties form closes.

Procedure 76-3 To configure a default MD on an OmniSwitch

Perform the following procedure to configure a default NE-level MD on an OmniSwitch.

1 Choose Equipment from the view selector in the navigation tree. The navigation tree displays the Equipment view

2 Right-click on an OmniSwitch NE object and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Globals tab button.

4 Click on the CFM tab button.

5 Configure the parameters:

- Level
- MHF-Creation
- Id-Permission

6 Close the Network Element (Edit) form.

77 — RCA audit

77.1 RCA audit overview

The 5620 SAM RCA audit tool allows you to perform on-demand verifications of the configuration of services and physical links to identify possible configuration problems. Except for physical links, the 5620 SAM provides a solution, which, at your request, can automatically be implemented to make all the required configuration changes.

Note — The adjustments are made only to the 5620 SAM database and are not deployed to the network.

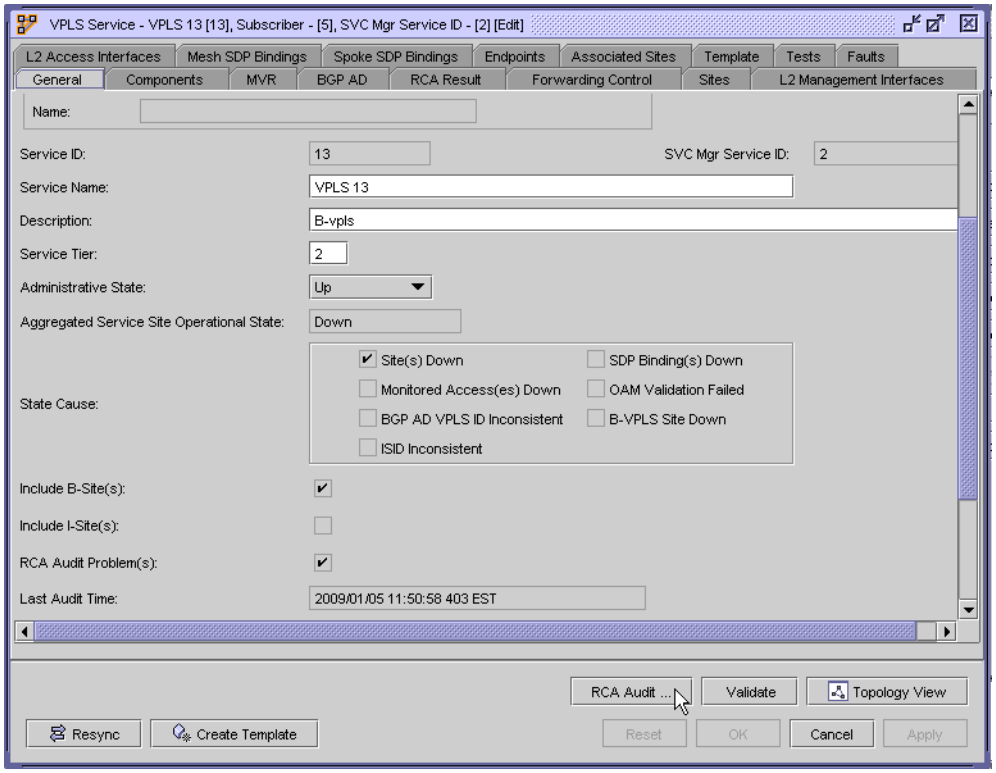
You can perform RCA audits of the following objects:

- VLL services
- VPLSs
- VPRN services
- physical links
- OSPF interfaces, areas, and area sites (5620 SAM/5650 CPAM integration only)
- IS-IS interfaces and sites (5620 SAM/5650 CPAM integration only)

Note — You need the 5650 CPAM license to perform the OSPF and IS-IS RCA audits. See the *5650 CPAM User Guide* for more information.

The RCA Audit Problem(s) indicator on the General tab of a network object properties form identifies whether configuration problems were detected in previous audits. The Last Audit Time indicator displays a timestamp of the last audit that was performed. Figure 77-1 shows the RCA Audit button on the properties form.

Figure 77-1 VPLS properties form - General (RCA audit)



After you associate an audit policy with the object, you can perform an RCA audit and view the results. If no problems are detected, the RCA Result tab does not appear.

The properties form of a problem displays the following information:

- problem severity
- probable cause
- description
- solution

The Caused By Objects tab lists the network objects that caused the problem, as shown in Figure 77-2. For service audits, the sites that should be moved out of a service, and the service they should move to, if there is only one destination service, are listed. If only one group of sites is listed, a new service is created and the sites are moved to the created service.

Figure 77-2 Problem properties form - Caused By Objects tab

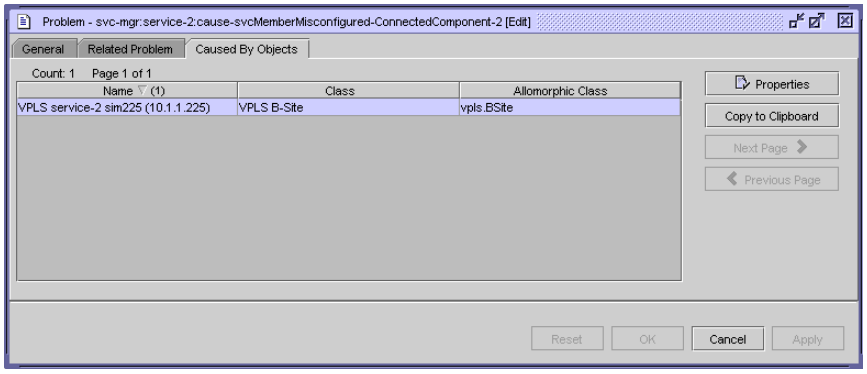


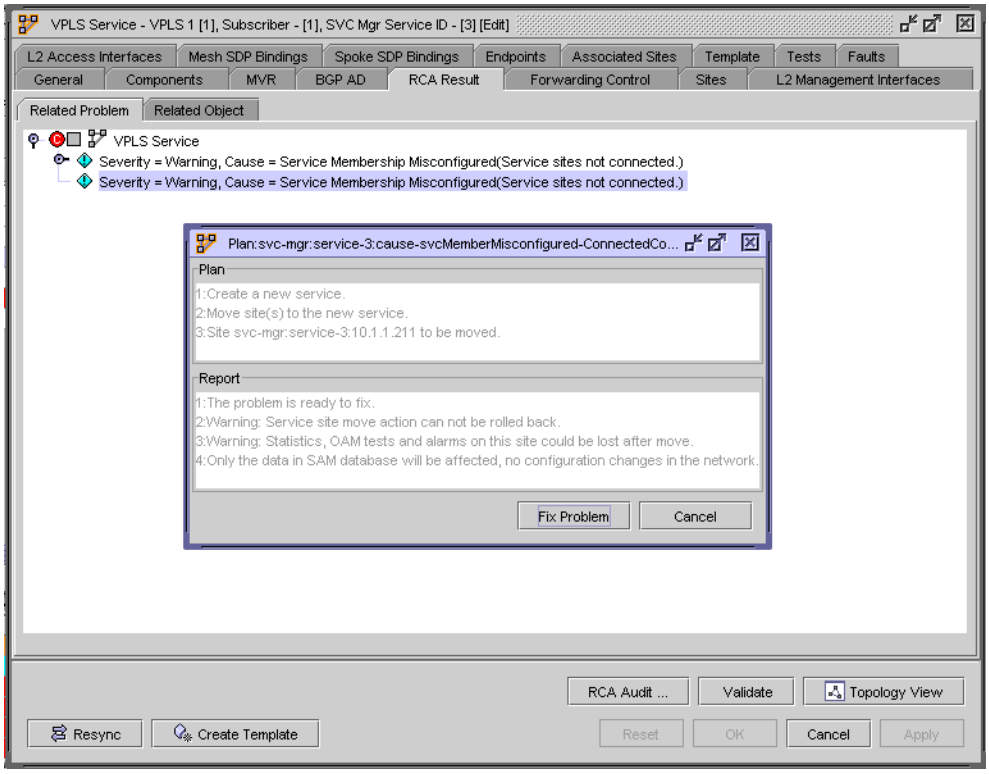
Table 77-1 describes the probable causes of problems.

Table 77-1 Probable causes

Probable cause	Description
Unknown	The probable cause could not be determined.
Underlying Resource Operational Down	The underlying resource of the object is operationally down.
Misconfiguration	There is a misconfiguration error.
Admin Down	The object is administratively down.
Underlying Resource Admin Down	The underlying resource of the object is administratively down.
Underlying Resource Missing	An underlying resource is missing.
Underlying Resource Problem	Problem with an underlying resource
Aggregated	Aggregated cause
Service Membership Misconfigured	The service membership is not configured correctly.
Route Targets are misconfigured for VPLS BGP Multi-homing	One of the following misconfigurations exists: • No matching RT for peered multi-homing sites • There are multiple RTs configured for a VPLS site that has BGP multi-homing sites configured under it. Multiple RTs will make the BGP multi-homing sites appear under multiple topologies or multiple services. • Multi-homing sites have the same multi-homing ID but different RTs (different RTs mean the sites are in different topologies or services)
No valid Route Targets configured for VPLS BGP Multi-homing	No valid Route Targets currently exist for a VPLS site that has BGP multi-homing sites configured under it.
No members configured for this Multi-homing site	The BGP VPLS multi-homing site does not have other sites as members that share the same multi-homing ID in order to comprise a group.

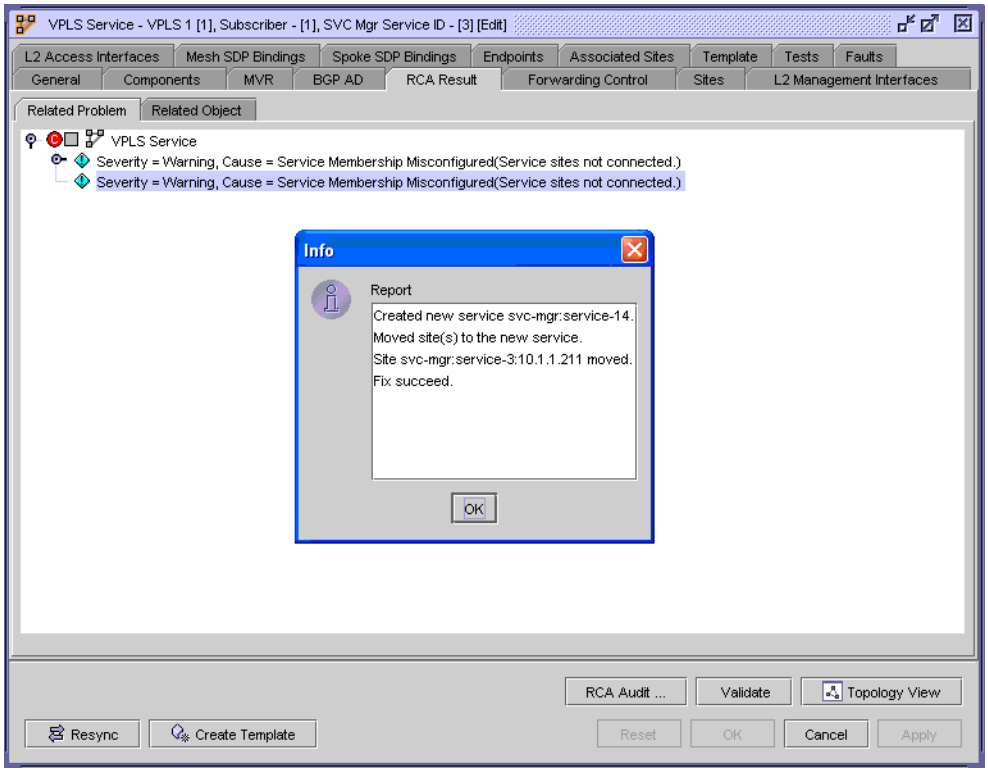
You can use the RCA audit tool to correct a detected configuration problem from the RCA Result tab on the network object properties form. The 5620 SAM lists the operations to fix the problem, as shown in Figure 77-3.

Figure 77-3 Correction plan for a problem



When you accept the proposed solution, a summary of the correction operation that the 5620 SAM implemented appears, as shown in Figure 77-4. To view the result in the server or client log, you must enable the logging option in the nms-server.xml or nms-client.xml file.

Figure 77-4 Correction report



5620 SAM service audit

A 5620 SAM service is defined as a collection of service sites with the same customer ID, service type, and service ID. The 5620 SAM discovers services that are configured on a 7750 SR, 7450 ESS, 7710 SR, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, and 7210 SAS-E using the service ID on the NE. Configuration errors may occur in networks where the services were created and deployed on the NEs using CLI before the NEs were managed by the 5620 SAM.

For example, when two VPLSs with the same service ID and the same mesh VC ID on an NE are discovered by the 5620 SAM, they are discovered as a single service in the 5620 SAM.

Another example of a configuration error is when a switching Epipe has multiple Epipe sites and multiple VC IDs for different segments. If different service IDs are used when the sites are created, the 5620 SAM assumes that the sites are connected and creates multiple VLL services within a composite service.

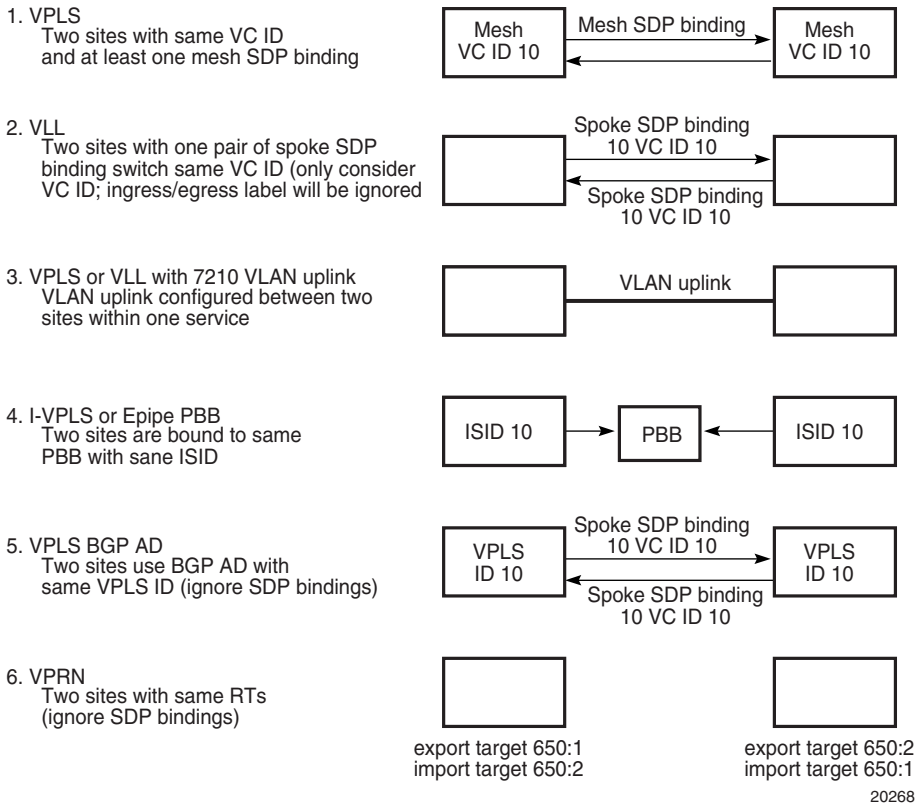
RCA audit policies allow you to modify the component membership of your 5620 SAM services to detect possible configuration problems. In addition, you can use the RCA audit to correct most configuration problems that are discovered in the audit.

Note — A 5620 SAM user that is assigned the Administrator or RCA scope of command role can create, modify, and execute all RCA audit policies. A 5620 SAM user that is assigned the Administrator or Service scope of command role can execute service audit adjustments.

Service membership rules

The 5620 SAM uses the rules in Figure 77-5 to identify whether two service sites are connected together. When two sites are identified as connected, they should belong to same service.

Figure 77-5 Rules to check whether two sites are connected



If service sites have different customer IDs, the 5620 SAM discovers the sites as belonging to different services. After the audit, the 5620 SAM generates a problem for each service. You can specify to which service the 5620 SAM should move the site and whether the empty service should be removed after the sites are moved.

For VPLS or VLL services, if the same service ID is used for two groups of sites that are not connected, the 5620 SAM detects a duplicate service ID. Two problems are generated for one of the group of sites, and the solution is to separate the services. If there are other groups of isolated sites, additional problems are generated for each group.

Consider the following when you perform an audit of a VPLS.

- Although different service IDs may be used, I-sites that are bound to same backbone VPLS and have the same ISID are considered to be in the same VPN.
- For VPLS sites that use BGP auto-discovery, the VPLS ID is used to determine service membership.
- H-VPLS is discovered as composite service in the 5620 SAM if different service IDs are used.

Consider the following when you perform an audit of a VLL service.

- Service sites with different customer IDs are discovered as two services, and can reconfigured as one service.
- More than two groups of sites that are connected can be detected and can be separated into different services.
- Redundant VLLs are not be affected by the audit and are considered correctly configured.
- If two Epipe sites are connected to the same PBB with same B-VPLS service ID, and the source and destination MAC addresses match, the 5620 SAM determines that the two sites are connected. If they are in different 5620 SAM services, a problem is generated during the audit.

Consider the following when you perform an audit of a VPRN service.

- VPRN service membership is based on the RTs defined in the VRFs.
- Sites that are in different services but have common import and export route targets. Import target of Site 1 is equal to the Export target of Site 2.

Physical link audits

Physical links represent the actual physical configuration of network connections between ports. You can view and manage physical links from the equipment window, physical topology map, and the Manage Equipment list form of the 5620 SAM, on each router using the CLI. Because several key parameters on each end of the physical link depend on each other, configuration errors are possible. The 5620 SAM RCA audit tool allows you to identify configuration errors in physical links. The 5620 SAM does not provide a solution for configuration problems that the RCA audit identifies for physical links. By default, the RCA audit detects the following configuration errors in physical links:

- **physical port parameters**
  - mismatched MTU values
  - mismatched speeds
- **Ethernet port parameters**
  - Auto-negotiate parameter misconfiguration
  - Duplex parameter misconfiguration

You can configure the RCA audit policy for the physical link to include additional physical link properties in the audit.

77.2 RCA audit workflow

1. Create or configure an RCA audit policy. For service audits, configure one or more audit policies for each service type to detect different configuration problems.
2. Run the RCA audit policy for a specific object.
3. Identify the problems and view the suggested solutions. Solutions are not provided for physical links.
4. Implement the changes, as required.

77.3 RCA audit procedures

Use the following procedures to perform RCA audit tasks.

Procedure 77-1 To configure an RCA audit policy

1. Choose Policies→Network and Service Audits from the 5620 SAM main menu. The Network and Service Audits form opens.
2. Select Audit Policy (RCA) from the drop down list.
3. Perform one of the following.
   a. To create an RCA audit policy, click on the Create button. The Audit Policy (Create) form opens with the General tab displayed.
   b. To configure an existing RCA audit policy, click on the Search button and choose an entry from the list. Click on the Properties button. The Audit Policy (Edit) form opens with the General tab displayed. Go to step 5.
4. If you are creating an RCA audit policy, configure the following parameters. Otherwise, go to step 5.
   - Auto-Assign ID
   - ID
5. Configure the Description parameter.
6. If you are creating an RCA audit policy, click on the button that is labelled Select RCA Policy to run the audit. Otherwise, go to step 11. The RCA Policy form opens.

7 Choose one of the following options:

- RCA Audit Physical Link
- RCA Audit ISIS
- RCA Audit OSPF
- RCA Audit VLL
- RCA Audit VPLS
- RCA Audit VPRN

Note — You require a 5650 CPAM license to create an RCA Audit ISIS or RCA Audit OSPF policy.

8 Double-click on an entry to modify the policy description, if required.

9 Click on the OK button. The RCA Policy form closes.

10 Click on the Apply button.

11 Click on the Entry tab button. Depending on the option specified in step 7, a list of RCA audit policy entries is displayed.

The RCA audit policy entry for a VLL RCA audit is: RCA Audit for VLL Service Membership.

The RCA audit policy entry for a VPRN RCA audit is: RCA Audit for VPRN Service Membership.

The following are the RCA audit policy entries for a VPLS RCA audit:

- RCA Audit for VPLS Service Membership
- RCA Audit for B-VPLS PBB
- RCA Audit for BGP Multi-homing

The following are the RCA audit policy entries for a physical link RCA audit:

- RCA Audit For Physical Ports of Physical Links
- RCA Audit For Ethernet Port Specifics of Physical Links

12 Choose an entry from the list and click on the Properties button. The Audit Policy Entry - RCA Audit Policy - RCA Audit For *Network_Object* (Edit) form opens with the General tab displayed.

13 Configure the parameters:

- Enabled
- Remove Empty Service

14 If you are configuring an RCA audit policy for physical links, perform the following steps. Otherwise, go to step 15.

i Click on the Attributes tab button. A list of default attributes for the physical link entry is displayed.

ii Perform one of the following:

- To configure default attributes, go to step iii.
- To add an attribute, go to step v.

iii Enable or disable the RCA audit for each attribute by selecting or deselecting the checkbox in the Enabled column.

iv Choose one of the problem severity options for each attribute by clicking on the entry in the Severity column of the attribute. A contextual menu appears.

- Minor
- Conditional
- Info
- Critical
- Major
- Warning
- Indeterminate

v Click on the Add button to add an attribute. Otherwise, go to step 15. The Adding new Attribute(s) - RCA Audit For *entry_type* of Physical Links form opens with a list of attributes associated with the physical link entry.

vi Choose one or more attributes in the list and click on the OK button. The Adding new Attribute(s) - RCA Audit For *entry_type* of Physical Links form closes and the Audit Policy Entry - RCA Audit Policy - RCA Audit For *entry_type* of Physical Links (Edit) form refreshes with the attribute information.

15 Click on the OK button. The Audit Policy Entry - RCA Audit Policy - RCA Audit For *Network_Object* (Edit) form closes.

16 Click on the OK button. A dialog box appears.

17 Click on the Yes button. The Audit Policy (Edit) form closes.

18 Close the RCA Audit Policy form.

Procedure 77-2 To perform an RCA audit of a VLL

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and choose VLL from the object drop-down list.

3 Click on the Search button. A list of VLL services appears.

4 Choose an entry from the list and click on the Properties button. The *VLL_type* (Edit) form opens with the General tab displayed.

5 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

6 Click on the RCA Audit button. The Select RCA Policy list form appears with a list of configured policies.

7 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears.

8 Click on the OK button.

9 Click on the RCA Result tab button. The RCA audit information is displayed on the Related Problem tab.

Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

10 If required, expand the VLL Service object in the problems tree to view the problems, the associated severity, and the cause.

11 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

12 Configure the Disable Fix Window parameter.

13 Click on the Related Problem tab button to view related problems.

14 Click on the Caused By Objects tab button to view a list of objects that are causing the problem.

15 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

16 Click on the tab buttons to view information about the configuration.

17 Configure the parameters, as required.

18 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

19 Click on the Yes button.

20 Close the Problem (Edit) form.

21 To fix a problem:

i Click on the Related Problem tab button.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.

Note — The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 12.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

22 Close the *VLL_type* (Edit) form.

23 Close the Manage Services form.

Procedure 77-3 To perform an RCA audit of a VPLS

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Click on the Search button. A list of VPLS services appears.

Note — In addition to the standard audit checks, for BGP VPLS multi-homing sites the audit also checks:

- if no valid Route Targets are configured under a VPLS site that has BGP multi-homing sites configured under it.
- if there are no matching RTs for peered multi-homing sites
- if there are multiple RTs configured under a VPLS site that has BGP multi-homing sites configured under it. Multiple RTs will make the BGP multi-homing sites appear under multiple topologies (or multiple services, since the RT defines the service)
- if multi-homing sites have the same multi-homing ID but different RTs (different RTs mean the sites are in different topologies or services)
- if a multi-homing site does not have other sites as members (sharing the same multi-homing ID to comprise a group)

3 Choose an entry from the list and click on the Properties button. The VPLS Service (Edit) form opens with the General tab displayed.

4 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

5 Click on the RCA Audit button. The Select RCA Policy to run the audit list form appears with a list of configured policies.

6 Choose an entry and click on the OK button. The Select RCA Policy list form closes and the requested audit is performed. A dialog box appears.

7 Click on the OK button.

8 Click on the RCA Result tab button. The RCA audit information is displayed on the Related Problem tab.

Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

9 If required, expand the VPLS Service object in the problems tree to view the problems, the associated severity, and the cause.

10 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

11 Configure the Disable Fix Window parameter.

12 Click on the Related Problem tab button to view related problems.

13 Click on the Caused By Objects tab button to view a list of objects that are causing the problem.

14 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

15 Click on the tab buttons to view information about the configuration.

16 Configure the parameters, as required.

17 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

18 Click on the Yes button.

19 Close the Problem (Edit) form.

20 To fix a problem:

i Click on the Related Problem tab button.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.

Note — The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 11.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

21 Close the VPLS Service (Edit) form.

22 Close the Manage Services form.

Procedure 77-4 To perform an RCA audit of a VPRN

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and choose VPRN from the object drop-down list.

3 Click on the Search button. A list of VPRN services appears.

4 Choose an entry from the list and click on the Properties button. The VPRN Service (Edit) form opens with the General tab displayed.

5 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

6 Click on the RCA Audit button. The Select RCA Policy list form appears with a list of configured policies.

7 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears.

8 Click on the OK button.

9 Click on the RCA Result tab button. The RCA audit information is displayed on the Related Problem tab.

Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

10 If required, expand the VPRN Service object in the problems tree to view the problems, the associated severity, and the cause.

11 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

12 Configure the Disable Fix Window parameter.

13 Click on the Related Problem tab button to view related problems.

14 Click on the Caused By Objects tab button to view a list of objects that are causing the problem.

15 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

16 Click on the tab buttons to view information about the configuration.

17 Configure the parameters, as required.

18 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

19 Click on the Yes button.

20 Close the Problem (Edit) form.

21 To fix a problem:

i Click on the Related Problem tab button.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.

Note — The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 12.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

22 Close the VPRN Service (Edit) form.

23 Close the Manage Services form.

Procedure 77-5 To perform an RCA audit of multiple services

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Configure the filter criteria and choose one of the following from the object drop-down list.

- AbstractVpls (VPLS)
- VPRN Service (VPRN)
- Vll (VLL)

3 Click on the Search button. A list of services appears.

4 Select the services that you want to audit.

5 Click on the Service Audit button. The Select RCA Policy list form opens.

6 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears with the following information:

- number of services audited
- number of successful audits
- number of problems generated

7 Click on the OK button.

8 Scroll to the RCA Audit Problem column and set the filter to = true.

9 Click on the Search button. A list of services with problems appears.

10 Select a service and click on the OK button. The *Service* (Edit) form appears with the General tab displayed.

11 Click on the RCA Result tab button. The RCA audit information is displayed on the Related Problem tab.

Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

12 If required, expand the *Service* object in the problems tree to view the problems, the associated severity, and the cause.

13 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

14 Configure the Disable Fix Window parameter.

15 Click on the Related Problem tab button to view related problems.

16 Click on the Caused By Objects tab button to view a list of objects that are causing the problem.

17 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

18 Click on the tab buttons to view information about the configuration.

19 Configure the parameters, as required.

20 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

21 Click on the Yes button.

22 Close the Problem (Edit) form.

23 To fix a problem:

i Click on the Related Problem tab button.

ii Right-click on a problem icon and choose Fix Problem from the contextual menu. The Plan form appears.

Note — The Fix Problem menu option is disabled if you set the Disable Fix Window parameter to Enabled in step 14.

iii Check the recommended plan to fix the problem in the Plan panel.

iv Check the report about fixing the problem in the Report panel.

v Click on the Fix Problem button. The Plan form closes and a dialog box appears with a summary of the fix. Click on the OK button.

24 Close the *Service* (Edit) form.

25 Close the Manage Services form.

Procedure 77-6 To perform an RCA audit of a physical link

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Click on the Select Object Type button and choose one of the following from the object tree.

- Physical Link (Network)
- Discovered Physical Link (Network)

3 Click on the Search button. A list of physical links appears.

4 Choose an entry from the list and click on the Properties button. The Physical Link (Edit) form opens with the General tab displayed.

5 Check the following indicators:

- RCA Audit Problem(s)
- Last Audit Time

6 Click on the RCA Audit button. The Select RCA Policy list form appears with a list of configured policies.

7 Choose an entry and click on the OK button. The Select RCA Policy list form closes and a dialog box appears.

8 Click on the OK button.

9 Click on the RCA Result tab button. The RCA audit information is displayed on the Related Problem tab.

Note — The RCA Result tab appears only if the RCA audit detects one or more problems.

10 If required, expand the Physical Link object in the problems tree to view the problems, the associated severity, and the cause.

11 Double-click on a problem icon to view information about the problem. The Problem (Edit) form opens with the General tab displayed. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

12 Click on the Related Problem tab button to view related problems.

Note — The 5620 SAM does not provide a solution for physical link configuration errors.

13 Click on the Caused By Objects tab button to view a list of objects that are causing the problem.

14 Choose an entry from the list and click on the Properties button. The properties form for the object opens.

15 Click on the tab buttons to view information about the configuration.

16 Configure the parameters, as required.

17 Click on the OK button to save the configuration and close the properties form. A dialog box appears.

18 Click on the Yes button.

19 Close the Problem (Edit) form.

20 Close the Physical Link (Edit) form.

21 Close the Manage Equipment form.

Procedure 77-7 To create a service audit scheduled task

1 Choose Policies→Network and Service Audits from the 5620 SAM main menu.

2 The RCA Audit Policy form opens.

3 Specify a filter for the search, if required, and click on the Search button. A list of RCA audit policies appears.

4 Choose a service audit policy from the list and click on the Properties button. The Audit Policy (Edit) form opens with the General tab displayed.

5 Click on the Schedule button and choose Create Service Audit Schedule Task. The Service Audit Scheduled Task (Create) form opens.

6 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Administrative State

7 Click on the Select button in the Schedule panel. The Select Schedule - Service Audit Scheduled Task form opens.

8 Perform one of the following.

a Create a schedule to associate with the scheduled task.

b Associate an existing schedule to the scheduled task. Go to step 10.

9 Create a schedule.

i Configure the parameters:

- Name
- Description
- User Start Time
- User End Time
- Delay Time (seconds)
- Enable
- Ongoing
- Frequency

The User End Time parameter is configurable when the Ongoing parameter is disabled and the Frequency parameter value is set to something other than Once.

When a SAM Schedule is not Ongoing and is assigned to a task, the 5620 SAM raises an alarm when the User End Time expires.

ii Perform the step that corresponds to the Frequency parameter value specified in step i.

- When the parameter is set to Once, go to step iii.
- When the parameter is set to Per Second, configure the following parameters:
  - Run Every Second
  - Run Every Seconds
- When the parameter is set to Per Minute, configure the following parameters:
  - Run Every Minute
  - Run Every Minutes
- When the parameter is set to Per Hour, configure the following parameters:
  - Run Every Hour
  - Run Every Hours
- When the parameter is set to Per Day, configure the following parameters:
  - Run Every Day
  - Run Every Days
  - Run Every
- When the parameter is set to Per Week, configure the following parameters:

Note — The Run Every parameter is not configurable when the Ongoing parameter is enabled.

  - Run Every Week
  - Run Every Weeks
  - Run Every
- When the parameter is set to Per Month, configure the following parameters:

Note — The Run Every parameter is not configurable when the Ongoing parameter is enabled.

  - Run Every Month
  - Run Every Months
  - Run Every

iii Click on the OK button to save the changes. The SAM Schedule (Create) form closes and the Select Schedule - Service Audit Scheduled Task form reappears.

10 Choose an entry from the list and click on the OK button. The Select Schedule - Service Audit Scheduled Task form closes and the Service Audit Scheduled Task (Create) form reappears.

11 Ensure that the Administrative State parameter is set to Enabled.

12 Click on the OK button. The Service Audit Scheduled Task (Create) form closes. The RCA Audit Policy form reappears with additional tab buttons.

13 To apply a filter to the schedule, perform the following.

i Click on the Schedule Filter tab button.

ii Click on the Select button in the Audit Filter panel. The Select Audit Filter - Audit Policy form opens.

iii Click on the Search button. A list of filters appears.

Note — If no filters appear, click on the Audit Filter button to create a new filter. See chapter 2 for more information about how to create a filter.

iv Choose an entry and click on the OK button. The Select Audit Filter - Audit Policy form closes and the Audit Policy (Edit) form reappears with additional tab buttons.

14 Click on the Scheduled Objects to be Audited tab button to view the services that are included in the audit.

15 Click on the Scheduled Result tab button to view the results of the scheduled audit.

16 Click on the Problems tab button to view the problems associated with the audit.

17 Close the Audit Policy (Edit) form.

18 Close the RCA Audit Policy form.

Customer documentation and product support

Customer documentation

http://www.alcatel-lucent.com/myaccess

Product manuals and documentation updates are available at alcatel-lucent.com. If you are a new user and require access to this service, please contact your Alcatel-Lucent sales representative.

Technical Support

http://support.alcatel-lucent.com

Documentation feedback

documentation.feedback@alcatel-lucent.com

3HE 05719 AAAH TQZZA Edition 01