Release 13.0 R3 | June 2015 | 3HE 09807 AAAC TQZZA Issue 1.0

Alcatel-Lucent 5620

SERVICE AWARE MANAGER

OPTICAL USER GUIDE

Alcatel·Lucent

Disclaimers

When printed by Alcatel-Lucent, this document is printed on recycled paper.

Contents

Introduction

1830 PSS system management

1830 PSS device management

1830 PSS SDH trails and services

1830 PSS OTN layer management

1830 PSS power management

1830 PSS fault management

1830 PSS policy management

1830 PSS network management

Introduction

1 — What’s new?

1.1 What's new in 5620 SAM Release 13.0 for 1830 PSS

This section highlights new optical features for 5620 SAM Release 13.0 and provides pointers into the documentation for more information about using the features. Feature lists and high-level feature descriptions are also available in the *5620 SAM Release Description*.

Maintenance releases

Some releases may not be listed in this section, either because no new optical features are introduced, or the features introduced do not require documentation.

What's new in 5620 SAM Release 13.0 R3 for 1830 PSS

Table 1-2 lists the features and functions added in 5620 SAM Release 13.0 R3 for 1830 PSS support. See the *5620 SAM User Guide* for more information about non-1830 PSS features and functions.

Table 1-1 5620 SAM Release 13.0 R3 1830 PSS features

Feature ID	Feature	Description	Reference
—	HO UNTERM ODU trails	Support for the auto-configuration of the HO UNTERM ODU trails during data bearer link configuration.	Section 11.7
—	GMRE protection switching	The 5620 SAM allows you to switch from main to spare path or spare to main path for internal SNCP and PRC configurations.	Section 11.10
—	ASON SRG management	Support for the configuration of the SRG in the ASON domain.	Section 11.8
—	ASON color management	The 5620 SAM provides the ability to assign colors to the TE links, physical connections, logical connections, and O-GLSPs.	Section 11.11
—	Unterm ODU trail discovery	Support for the discovery of untern ODU trails.	Section 11.7
—	CP node ODU trail auto-configuration upon O-GLSP restoration	Support for the auto-configuration of the CP node ODU trails upon O-GLSP restoration.	Section 11.9
—	CP node ODU trail discovery	Support for the discovery of the CP node ODU trails.	Section 11.9
SAM-35713	10AN10GC card support	Support for the configuration of the 10AN10GC cards on the 1830 PSS-36 and 1830 PSS-64 devices.	Section 9.5
SAM-37186	10ET10GC card support	Support for the configuration of the 10ET10GC cards on the 1830 PSS-36 and 1830 PSS-64 devices.	Section 9.5
SAM-37637	SDH line timing	Support for the configuration of line timing references on 10SD10G card ports assigned with an STM-64 rate.	Section 12.6 Procedure 12-4
SAM-37640	Unidirectional and non-revertive 1+1 MSP	Support for the configuration of unidirectional and non-revertive 1+1 MSP, and creation of VC-4 service with 1+1 MSP configuration.	Section 12.5 Procedure 12-6

(1 of 3)

Feature ID	Feature	Description	Reference
SAM-41379	AES 256 support	Support for the AES 256 encryption module for SNMPv3 protocol.	Procedures 7-1 and 7-2
SAM-46767	GMRE licensing	Support for the licensing of the CP nodes.	Section 11.5
SAM-46781	GMRE node discovery	Support for the discovery of the GMRE devices.	Section 11.4
SAM-46785	GMRE CLI cut through	The 5620 SAM provides CLI cut through to the CP node.	Section 11.4
SAM-46788	ASON-GMRE in service upgrade	Support for the upgrade of the GMRE software.	Section 11.12
SAM-46796	ASON domain management	Support for the configuration of the ASON domain.	Section 11.3
SAM-46798	ASON TE link management	Support for the configuration of data bearers, data bearer links, and TE links.	Sections 11.6, and 11.7
SAM-46802	O-GLSP re-discovery	Support for the discovery of the O-GLSPs configured on the CP nodes.	Section 11.9
SAM-46812	ASON Layer 1 O-GLSP configuration	Support for the configuration of Layer 1 O-GLSPs.	Section 11.9
SAM-48215	OSPF support on OCS devices	Supports OSFP configurations on OCS devices.	Sections 24.1 or 24.3
SAM-48229	TL1 user configuration	Support for the configuration of TL1 users.	Procedures 7-2, 7-3, 7-4, and 7-5
SAM-49985	Support SDH gateway cards	Support for the following: • configuration of the 10SD10G and 24SDM SDH cards • configuration of unprotected STM trails between SDH cards • bind and collapse VC-4 sub-structures • configure VC-4 XCs and protect/unprotect the XCs • configure unprotected and ESNCP VC-4 services • configure VC-4 service with underlying asymmetric ODU trail after creating an STM trail	Sections 9.5, 9.6, and 12.3 Procedures 12-1, 12-2, 12-5, and 12-6
SAM-52918	130SNQ10 card support	Support for the configuration of the following for the second generation 10x10G OT that provides 100G transmission capacity in a single card: • client signal types, 10 GbE (all client interfaces QSFP+ or XFP) and OC-192/STM-64 (XFP client interfaces, C1 and C2 only). • OTU4 signal rate on the line port • SD-FEC or AFEC on the line port • pluggable module types 10GB-ZR, XI-64.1, XL-64.2C, XS-64.2B, XS-64.2C, AUTO, and USER for OC192 or SMT64 signal rates and 10GB-ZR, 10GB-SR, XI-64.1, XL-64.2C, XS-64.2B, XS-64.2C, AUTO, and USER for 10GbE signal rate on the client port • transmit and receive frequencies for the line port, and not applicable for the client ports • CBRLAN11.049, CBRLAN11.096, GFP-F and GFP-P encapsulation modes on 10GbE client ports • interworking with 112SCX10, 112SNX10, and 130SNX10 cards	See Procedure 9-7 for more information about configuring a card See Procedure 9-14 for more information about configuring a port

(2 of 3)

Feature ID	Feature	Description	Reference
SAM-52949	MVAC8B card support for CDC-F configuration	Support for the configuration of CDC-F using an MVAC8B card.	Section 16.10
SAM-52977	OTU4 Client for 260SCX2	Support for the single OTU4 client interface on 260SCX2.	Procedure 9-12
SAM-52986	MON-OCM card support	Support for the MON-OCM card configuration.	Section 9.5
SAM-53310	alarm correlation between IP and optics	The 5620 SAM fault management application displays the alarm correlation up to the SR ports for optical transport services terminating on SR ports.	Section 20.5
SAM-53387	1830 PSS-8 shelf support	Support for the configuration of the 1830 PSS-8 shelf and the subtending clip-on shelves.	Sections 2.2 and 9.4
SAM-54666	Alarm correlation	Support for the management and correlation of GMRE alarms.	Section 11.13

(3 of 3)

What's new in 5620 SAM Release 13.0 R1 for 1830 PSS

Table 1-2 lists the features and functions added in 5620 SAM Release 13.0 R1 for 1830 PSS support. See the *5620 SAM User Guide* for more information about non-1830 PSS features and functions.

Table 1-2 5620 SAM Release 13.0 R1 1830 PSS features

Feature ID	Feature	Description	Reference
-	Configure optical link as path constraints	The 5620 SAM supports the configuration of optical links as path constraints during service and trail configurations.	Procedures 13-3 and 16-6
SAM-20339	NTP server authentication	The 5620 SAM supports authentication of NTP packets arriving from the NTP Server.	Procedure 9-25
SAM-20917 SAM-55796	Preview optical transport service	The 5620 SAM allows you to preview an optical transport service before it is deployed in the network.	Procedure 16-1
SAM-30073	TTI attributes for SR-SR ODU and OTU trails	The 5620 SAM allows you to configure the TTI attributes for the OTU-enabled SR ports during the SR-SR ODU and OTU trail configurations.	Section 16.1
SAM-37266 SAM-37272	On-demand DM for ODU trails	The 5620 SAM allows you to initiate the on-demand DM for ODU trails.	Section 13.7
SAM-37561	Software upgrade, backup, and restore progress indication for 1830 PSS	The 5620 SAM displays the status of software upgrade, backup, and restore operations for an 1830 PSS.	Procedures 8-4, 8-7, 8-8, 8-9, 8-16
SAM-46084	100GBASE-LR4 CFP support	The 5620 SAM supports the configuration of dual-rate 100GBASE-LR4 CFP in the OTU4 mode on the L1 port.	Section 16.22

(1 of 2)

Feature ID	Feature	Description	Reference
SAM-49983	Enhancements for multipoint services for 1830 PSS OCS and WDM devices	The 5620 SAM supports the following enhancements for multipoint transport services: • configuration of unprotected multipoint transport services using the 11QPA4 card interworking with 1830 PSS OCS devices • configuration or discovery of multipoint drop and continue services with a protection level of segment protected, using dual-stage multiplexing of the 4DPA4 card with the 11DPM12 card	Section 16.12 Procedure 16-2
SAM-50083	AINS parameters for ports and facility objects	The 5620 SAM supports the configuration of the AINS parameters for the 1830 PSS OCS and WDM ports and facility objects.	Section 16.17
SAM-51807 SAM-51809	Support discovery of optical transport service between two 7750 SR devices connected to 112SDX11 cards on 1830 PSS devices	The 5620 SAM discovers optical transport services from SR to SR when one 100 GbE or one 40 GbE port is connected to ten or four client ports of the 112SDX11 card, respectively, using fan-out cables.	Section 16.22
SAM-51811	Support ISL trunking on FC ports	The 5620 SAM supports ISL trunking through client ports with FC400, FC800, or FC1600 rates on the 112SDX11 card.	Section 16.22
SAM-52808	2AN40G card support	The 5620 SAM supports the configuration of the I/O card 2AN40G on the 1830 PSS-36 and 1830 PSS-64 devices.	Sections 9.5 and 9.6
SAM-52817	Improvement of optical transport service discovery	The 5620 SAM displays the status of an optical transport service discovery as In Progress in the Task Manager form, until all the sub-tasks are completed successfully.	Procedure 16-3
SAM-52819	Support site name of unmanaged NE in optical link	You can configure the site name as the unmanaged NE identifier in an optical link.	Procedure 9-18
SAM-53613	Service and trail deletion	The 5620 SAM provides you an option of deleting the underlying trails when you delete an optical transport service or trail.	Section 16.14
SAM-56130	Filter alarms with severity Not Alarmed	The 5620 SAM allows you to hide or display the alarms generated on the 1830 PSS device with severity as Not Alarmed from the alarm list of the 5620 SAM.	Section 20.3

(2 of 2)

2 — 1830 PSS overview

2.1 1830 PSS OCS system overview

The OCS component of the 1830 Photonic Service Switch provides OTH switching and control functions using matrix cards. The 5620 SAM supports the 1830 PSS OCS product family of devices which includes:

- 1830 PSS-64
- 1830 PSS-36

See the current *5620 SAM Network Element Compatibility Guide* for information about the 1830 PSS support in a 5620 SAM release.

1830 PSS-64 and 1830 PSS-36 devices

The OCS component uses 1830 PSS-64 and 1830 PSS-36 devices. The 1830 PSS-36 is used for lower bandwidth requirements. The 1830 PSS-64 is used for higher bandwidth requirements and switching. The devices handle interfaces of OTH, SDH, SONET, and Ethernet. These devices support agnostic matrix cards which enable switching of WDM and OCS traffic.

For more information about the hardware and capabilities that are supported by the shelves, see the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide*.

2.2 1830 PSS WDM system overview

The 1830 Photonic Service Switch product family provides CWDM, DWDM, and OTN capabilities. Photonic networking increases flexibility and operational automation. The 5620 SAM supports the 1830 PSS WDM product family of devices which includes:

- 1830 PSS-32—central office device
- 1830 PSS-16—end office device
- 1830 PSS-8—metro device
- 1830 PSS-4—edge device platform
- 1830 PSS-1—edge aggregation devices that collect lower rate signals for input to the 1830 PSS network, which include:
    - 1830 PSS-1 GBE edge device
    - 1830 PSS-1 MD4H edge device
    - 1830 PSS-1 AHP

See the current *5620 SAM Network Element Compatibility Guide* for information about the 1830 PSS support in a 5620 SAM release.

1830 PSS-32 central office device/1830 PSS-16 end office device

The 1830 PSS-32 and 1830 PSS-16 provide multi-service and multi-reach solutions. The shelves are referred to collectively as the 1830 PSS-32/1830 PSS-16. They are scalable optical transport platforms for regional and metropolitan network transport and services delivery.

- The 1830 PSS-32 central office device provides a 32-slot platform for core, central office applications.
- The 1830 PSS-16 end office device provides a 16-slot platform that can be used for end office or smaller core office applications.

For information about the hardware and capabilities supported by the shelves, see the *Alcatel-Lucent 1830 Photonic Service Switch 32/16 Product Information and Planning Guide*.

The 1830 PSS-32 network consists of standalone NE, or two or more interconnected NEs that provide SDH/SONET/GigE aggregation and transport, 10G, FC (R1.1), or transponderless wavelength services in a metropolitan or regional networking environment.

The 1830 PSS-32 and 1830 PSS-16 support bidirectional transmission over a single fiber. The devices can be configured to support applications using CWDM filters. Each bidirectional transmission requires different CWDM wavelengths in each direction. Bidirectional transmissions over a single fiber is supported with the following filters and OTs:

- SFC-2
- SFC-4
- SFC-8
- 4DPA4
- 11STAR1
- 11STAR1A
- 11STMM10
- 11DPE12(E)

See the *Alcatel-Lucent 1830 Photonic Service Switch 36/32/16 Product Information and Planning Guide* and the *Alcatel-Lucent 1830 Photonic Service Switch 36/32/16 (PSS-36/PSS-32/PSS-16) User Provisioning Guide* for more information.

1830 PSS-8

The 1830 PSS-8 is a metro WDM-OTN device that provides scalability and flexibility in WDM and OTN metropolitan networks. The 1830 PSS-8 is 3 RU in height and has eight universal slots for OT, OA, and SFC, and SFD.The 1830 PSS-8 also includes the mandatory cards like the redundant AC and DC Power Filter cards, Fan Unit with dust filter, redundant EC, Shelf panel and User panel. The User panel is not a mandatory card and can only be placed in the protection EC slot of the master shelf.

See the *Alcatel-Lucent 1830 Photonic Service Switch 36/32/16/8 Product Information and Planning Guide* and the *Alcatel-Lucent 1830 Photonic Service Switch 36/32/16 (PSS-36/PSS-32/PSS-16/8) User Provisioning Guide* for more information.

1830 PSS-4 edge device platform

The 1830 PSS-4 edge device platform is designed for installation near the edge of the metropolitan networks. The edge device platform provides a flexible, power saving, OTN-based solution for metropolitan and access applications. The target application provides OTN-based multiple service aggregation for CWDM and DWDM networks. The application can also be configured to provide an FOADM terminal, and in-line amplifier solution for the 1830 PSS-32 networks. The platform supports non-switched and electrical switched configurations, and ensures full interworking and compatibility with other 1830 PSS product platforms.

The 1830 PSS-4 supports bidirectional transmission over a single fiber. See the *Alcatel-Lucent 1830 Photonic Service Switch 36/32/16 Product Information and Planning Guide* and the *Alcatel-Lucent 1830 Photonic Service Switch 36/32/16 (PSS-36/PSS-32/PSS-16) User Provisioning Guide* for more information.

See the *Alcatel-Lucent 1830 Photonic Service Switch 4 (PSS-4) User Guide* for more information.

1830 PSS-1 GBE edge device

The 1830 PSS-1 GBE edge device is a 1-RU device for installation in 19-in., ANSI, or ETSI racks. The device is based on a 12xGBE optical transponder that supports optional CWDM filters. The device provides an optimized WDM access platform that includes the following features:

- 1-RU height
- dc power (ac power adapter available)
- standard or temperature-hardened versions
    - standard 1830 PSS-1 GBE
    - hardened 1830 PSS-1 GBEH
- Black & White (B&W), CWDM, or DWDM optics
- in-band management using GCC
- stackable as a single NE
- alignment with the 1830 PSS service cards and operations
- support for single-fiber bidirectional transmission

See the *1830 Photonic Service Switch 1 (PSS-1) GBEH Edge Device User Guide* for more information.

1830 PSS-1 MD4H edge device

The 1830 PSS-1 MD4H edge device is a 1-RU device for installation in 19-in., ANSI, or ETSI racks. The MD4H designation represents the device as a multiservice dual module unit with 4 client ports per module, which is temperature hardened. The device is based on two 1830 PSS-32 4DPA4 optical transponders, which are remapped into an external device that also supports optional CWDM filters. The device provides an optimized WDM access platform that includes the following features:

- 1-RU height
- dc power (ac power adapter available)
- standard or temperature-hardened versions

- Black & White (B&W), CWDM, or DWDM optics
- in-band management using GCC
- alignment with the 1830 PSS service cards and operations
- support for single-fiber bidirectional transmission

See the *Alcatel-Lucent 1830 Photonic Service Switch 1 (PSS-1) MD4H Edge Device User Guide* for more information.

1830 PSS-1 AHP

The 1830 PSS-1 AHP is a 1-RU edge device that supports an adapted amplifier. Two devices can be used to provide a low-cost ILA for the 1830 PSS. The 1830 PSS-1 AHP software provides the following enhanced capabilities:

- multi-shelf NE management
- IP routing (OSPF) over OSC links
- wave key assignment distribution over OSPF LSAs
- automatic/manual power management between devices
- keyed-unkeyed DWDM OCH XC provisioning and OCH trail management
- DCM shelf/card/port management

See the *Alcatel-Lucent 1830 Photonic Service Switch 1 (PSS-1) AHP Amplifier User Guide* for more information.

Before you can use the 5620 SAM to manage one or more 1830 PSS devices, the required 1830 PSS modules and quantities must be included in the 5620 SAM software license. See “Software and license configuration procedures” in the *5620 SAM System Administrator Guide* for information about viewing and updating the license information.

2.3 About this guide

This guide provides information about how to access the 5620 SAM to configure and manage the 1830 PSS network. The 5620 SAM guides describe the GUI operations associated with each function, and indicate whether the function is available, using the OSSI. See the *5620 SAM XML OSS Interface Developer Guide* for information about using the OSSI to perform a 5620 SAM function. The guide is intended for optical network planners, administrators, and operators and is to be used in conjunction with other guides in the 5620 SAM documentation suite where management of optical devices does not differ from other network elements. Procedures that are unique to managing the 1830 PSS are included in this document and make reference to configurable parameters described in the *5620 SAM Optical Parameter Reference*.

The document describes the features, and configurations, for the 1830 PSS-32, 1830 PSS-16 and 1830 PSS-4 as well as their hardware components, NEs, and networks. See the *Alcatel-Lucent 1830 Photonic Service Switch 36/32/16 Product Information and Planning Guide* and the *Alcatel-Lucent 1830 Photonic Service Switch 4 (PSS-4) User Guide* for more information.

A high-level overview of the 1830 PSS-1 edge devices is included. For more information about the 1830 PSS-1 edge devices, see the *Alcatel-Lucent 1830 Photonic Service Switch 1 (PSS-1) GBEH Edge Device User Guide*, the *Alcatel-Lucent 1830 Photonic Service Switch 1 (PSS-1) MD4H Edge Device User Guide*, and the *Alcatel-Lucent 1830 Photonic Service Switch 1 (PSS-1) AHP Amplifier User Guide*.

The guide contains the following volumes:

- Introduction—contains general 1830 PSS information such as the following:
    - features supported
    - a system overview
- System management—contains information about map management and discovery of the 1830 PSS devices using the 5620 SAM, such as the following:
    - user security
    - GUI map management
    - navigation tree
    - CLI sessions and scripts
- Device and equipment management—contains information about the 1830 PSS device support and management tasks that can be performed using the 5620 SAM, such as the following:
    - device discovery
    - in and out-of-band management
    - SONET/SDH mode switching
    - file backup and restore
    - upgrade management
    - object resynchronization
    - connection management
    - shelf, card slots, and port management
    - equipment management
    - equipment view
- Control plane management
- SDH trails and services configuration
- OTN layer management—contains information about various OTN layers that can be managed using the 5620 SAM, such as the following:
    - ODU
    - OTU
    - OCH
    - OTS
- Service management—contains information about the 1830 PSS devices managing the optical transport services, VPLS and mirror services using the 5620 SAM, such as the following:
    - service creation and configuration
    - transport service discovery
    - VPLS service management
    - mirror service management

- Performance management—contains information about the 1830 PSS performance monitoring tasks performed using the 5620 SAM, such as the following:
  - performance statistics
  - TCA profiles
- Power management
- Fault management—contains troubleshooting information, such as the following:
  - alarm management
  - RCA audit
- Policy management—contains information about configuring and applying 5620 SAM policies that define rules for 1830 PSS management, or 5620 SAM operation
- Network management—contains information about the 1830 PSS network functions, such as the following:
  - Ethernet OAM
  - routing and forwarding
  - service tunnel management
  - MC LAG group

1830 PSS reference documentation

See the following documents for more information about the 1830 PSS:

- *Alcatel-Lucent 1830 Photonic Service Switch 1 (PSS-1) GBEH Edge Device User Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch 1 (PSS-1) MD4H Edge Device User Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch (PSS-1) AHP Amplifier User Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch 4 (PSS-4) User Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch User Provisioning Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch Maintenance and Trouble-Clearing Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch 32/16 (PSS-32/PSS-16) Installation and System Turn-Up Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch (PSS) Safety Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch (PSS) Command Line Interface Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch (PSS) TL1 Commands and Messages Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch (PSS) Engineering and Planning Tool User Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch (PSS) Commissioning and Power Balancing Tool User Guide*

2.4 IP/Optical management workflow

The following workflow describes the sequence of high-level tasks that are required to deploy the 1830 PSS and use the 5620 SAM for 1830 PSS management.

The 5620 SAM works in parallel to the planning and commissioning functions which are performed by EPT and CPB tools. There is no interaction between 5620 SAM and the EPT and CPB tools.

1 Plan the 1830 PSS deployment using the Engineering Planning Tool by considering, for example:

- network parameters
- sites
- fiber connectivity
- traffic patterns
- run automatic design synthesis
- create reports
- divide the network into downloadable systems for automatic commissioning
- create the commissioning files

See the *Alcatel-Lucent 1830 PSS Engineering and Planning Tool User Guide* for more information.

2 Install the CPB tool for provisioning, commissioning and power balancing functions of the 1830 PSS. See the *Alcatel-Lucent 1830 PSS Commissioning and Power Balancing Tool (CPB) User Guide* for more information.

3 Configure and manage the 1830 PSS device using the 5620 SAM.

i Use the 5620 SAM to discover the commissioned 1830 PSS devices; see chapter 7.

ii Configure SSH2 security for CLI sessions, if required; see chapter 6.

iii View, manage, and configure the discovered 1830 PSS device network objects.

- device objects; see chapter 8
- shelf, card, port, and LAG objects; see chapter 9
- equipment view on a specified browser; see chapter 10
- power levels; see chapter 19

iv Configure the 5620 SAM policies that specify the conditions for 5620 SAM management functions including:

- QoS policy; see chapter 21
- ACL IP filter; see chapter 22

v View, manage, and configure the OTN layers on 1830 PSS. See chapter 13

vi View, manage, and configure the network functions, as required

- routing and forwarding; see chapter 24
- service tunnels; see chapter 25

vii View, manage, and configure the GMRE devices, as required

- GMRE configuration; see chapter 11

viii View, manage, and configure the SDH trails and services, as required

- SDH trails and services; see chapter 12

ix View, manage, and configure the services and related functions.

- optical transport services; see chapter 16
- VPLS services; see chapter 15
- mirror services; see chapter 17

x Collect 5620 SAM and 1830 PSS statistics see chapter 18 and the *5620 SAM Statistics Management Guide*.

1830 PSS system management

3 — 1830 PSS user security

3.1 User security overview

The 5620 SAM provides security functions for user groups, devices, and paths.

Note — The administrator can restrict the access of some operators to equipment and services in their domain, for example, transport or data.

3.2 5620 SAM user and user group security

You can use the 5620 SAM to configure user accounts, user groups, and spans of control, which define the 5620 SAM objects the users can view and manage. For more information about user security, see “5620 SAM user security tasks” in the *5620 SAM System Administrator Guide*.

Span of control

The span of control allows you to assign access permissions to a functional group of 5620 SAM server objects; for example, a group of NEs or services.

You can use the 5620 SAM to create a span of control, or to copy an existing span of control and modify the list of associated objects to create a span of control. The objects that are in a span of control, or that can be added to a span of control, are called span objects. The 5620 SAM has several pre-defined spans of control. Each new 5620 SAM object, for example, a discovered NE, is added to the corresponding pre-defined span of control. Optical objects, such as the wavelength service on the 1830 PSS, are added to the Default Transport Span.

For more information about the span of control, see “Span of control” in the *5620 SAM System Administrator Guide*.

You can filter the objects the map or the list 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 control of the user.

Table 3-1 User security references

Topics	Chapter	Document
User account and group management	5620 SAM user security tasks	*5620 SAM System Administrator Guide*
User activity logging	5620 SAM user security tasks	*5620 SAM System Administrator Guide*
Sample span rule configuration	5620 SAM user security tasks	*5620 SAM System Administrator Guide*
Sample 5620 SAM user authentication configuration	5620 SAM user security tasks	*5620 SAM System Administrator Guide*
Remote authentication and authorization	5620 SAM user security tasks	*5620 SAM System Administrator Guide*
5620 SAM user security procedures	5620 SAM user security tasks	*5620 SAM System Administrator Guide*

4 — 1830 PSS map management

4.1 Map management overview

This chapter describes the network topology and grouping in the 5620 SAM that apply to the 1830 PSS. The 5620 SAM uses map windows to represent network objects and paths. For the 1830 PSS, the 5620 SAM supports physical network topology maps. Each map displays network objects and information, and provides contextual menus to open forms that display additional information. See "5620 SAM topology map management overview" in the *5620 SAM User Guide* for more information about network topology.

4.2 Network topology maps

Service topology map

A service topology map can be viewed from the service properties form. See Procedure 4-1. If you move an NE in the service topology map view, the associated ports are also moved with the NE. To view the optical link properties from the topology map, double-click on the optical link. The Optical Link form opens.

Note — The optical link properties are displayed on the topology map only for external optical links.

The active path (working path or protected path) of a service or trail is highlighted in green and the standby path in blue in the Topology view, when the service or trail is operationally up. For a protected service, when the working and protection ports of an APS group are switched, using the Protection Switch parameter, the colors of the active path and standby path also changes. If the service or trail is operationally down, then both active and standby paths are highlighted in red in the topology view.

Physical topology map

When the 5620 SAM client GUI starts, the physical topology map is open in the working panel by default. The default view displays the interconnections between IP and optical devices. The 5620 SAM allows you to filter the view to display only optical interconnections or IP interconnections. See Procedures 4-2 and 4-3. See the *5620 SAM Parameter Guide* for descriptions of the parameters.

Table 4-1 5620 SAM topology map management references

Topics	Chapter	Document
5620 SAM topology map management overview	5620 SAM topology map management	*5620 SAM User Guide*
5620 SAM topology map types	5620 SAM topology map management	*5620 SAM User Guide*
Basic 5620 SAM topology map procedures	5620 SAM topology map management	*5620 SAM User Guide*
5620 SAM topology map management procedures	5620 SAM topology map management	*5620 SAM User Guide*

4.3 Map management procedures

Procedure 4-1 To view a service topology map

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Choose Optical Transport Service from the object drop-down menu. The list of optical transport services appears.
3. Choose an entry and click Properties. The Optical Transport Service (Edit) form opens.
4. Click Topology View. The service topology map appears.

Procedure 4-2 To view optical interconnections only

1. Open a physical topology map.
2. Click on the Filter icon. The Topology Filter - Physical Topology form opens.
3. Choose Optical Link from the Object Filters to Add drop-down menu.
4. Click on the Add object filter icon. The Optical Link Filter panel appears.
5. Choose Endpoint A Type from the Attribute drop-down menu.
6. Choose EQUALS from the Function drop-down menu.
7. Choose Port from the Value drop-down menu.
8. Click on the Add to Filter icon.
9. Choose AND from the Operators drop-down menu. Repeat steps 5 to 8 to add Endpoint B Type.
10. Click Save. The Save Filter dialog box appears.
11. Enter a Filter Name and Description and click Save.
12. Choose Network Element from the Object Filters to Add drop-down menu.
13. Click on the Add object filter icon. The Network Element Filter panel appears.
14. Choose Chassis Type from the Attribute drop-down menu.
15. Choose EQUALS from the Function drop-down menu.
16. Choose the required 1830 PSS chassis from the Value drop-down menu.
17. Click on the Add to Filter icon. The Chassis Type appears on the Filter panel.
18. Choose AND from the Operators drop-down menu. Repeat steps 12 to 17 to add the different 1830 PSS chassis types.

19 Click Save, the Save Filter dialog box appears.

20 Enter a Filter Name and Description and click Save. The filter is saved.

21 Click Apply to apply the Optical Link filter. The Topology Filter - Physical Topology form closes and the map view is refreshed to display only devices with optical interconnections.

Procedure 4-3 To view IP interconnections only

1 Open a physical topology map.

2 Click on the Filter icon. The Topology Filter - Physical Topology form opens.

3 Choose Physical Link from the Object Filters to Add drop-down menu.

4 Click on the Add object filter icon. The Physical Link Filter panel appears.

5 Choose Chassis Type from the Attribute drop-down menu.

6 Choose NOT EQUAL from the Function drop-down menu.

7 Choose the required 1830 PSS chassis from the Value drop-down menu.

8 Click on the Add to Filter icon. The 1830 PSS chassis appears on the Filter panel.

9 Choose OR from the Operators drop-down menu to add other 1830 PSS chassis types. Repeat steps 5 to 7. The 1830 PSS chassis appears on the Filter panel.

10 Click Save, the Save Filter dialog box appears.

11 Enter a Filter Name and Description and click Save. The filter is saved.

12 Click Apply to apply the Physical Link filter. The Topology Filter - Physical Topology form closes and the map view is refreshed to display only devices with IP interconnections.

5 — 1830 PSS equipment navigation tree

5.1 Equipment 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. 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.

Using the 1830 PSS external element manager

You can start the 1830 PSS external element manager, ZIC interface, from the 5620 SAM GUI. The ZIC interface provides WebUI to access the 1830 PSS. The WebUI supports provisioning, administration, performance monitoring, and displaying alarms and conditions from the NE. For more information about using the WebUI with the 1830 PSS, see the *Alcatel-Lucent 1830 Photonic Service Switch 36/32/16 (PSS-36/PSS-32/PSS-16) User Provisioning Guide*. Procedure 5-1 describes how to start the 1830 PSS external element manager from the 5620 SAM GUI in the normal mode. Procedure 5-2 describes how to start the 1830 PSS external element manager from the 5620 SAM GUI in the secure mode.

Procedure 5-1 To start the 1830 PSS external EMS browser in normal mode

Note — The 1830 PSS external EMS browser is supported on Internet Explorer 6.0 or later or FireFox 3.6.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on an 1830 PSS device object and choose Launch External EMS Browser. The WebUI main view screen appears in the normal mode (http).

Procedure 5-2 To start the 1830 PSS external EMS browser in secure mode

Note — This procedure requires actions to be performed both in the WebUI and the 5620 SAM GUI.

1 Start the 1830 PSS external EMS bowser in the normal mode. See Procedure 5-1. The WebUI main view screen appears.

2 Connect to the 1830 PSS device using admin credentials. The WebUI opens with the System Properties form displayed.

3 Choose Administration→Security→Encryption→SSH Key. The SSH KEY form opens.

4 Click Generate and click OK. The SSH key is generated.

5 Click Close. The SSH KEY form closes and the System Properties form reappears.

6 Configure the UI Mode parameter as Encrypted and click Submit.

7 Click OK. The 1830 PSS device reboots.

8 Connect to the 1830 PSS device using admin credentials. The WebUI opens with the System Properties form displayed and the UI Mode parameter set to Encrypted.

9 Choose Administration→Security→SNMP v3 Users. The SNMP v3 Users form opens.

10 Click Create. The Create SNMP v3 Users form opens.

11 Configure the required parameters and click Apply.

12 Perform the remaining steps in the 5620 SAM GUI.

Create an SNMPv3 user account. See Procedure 7-2.

Note — Provide the same user name and password that was provided during the SNMPv3 user creation using the WebUI.

13 Create a new SNMP mediation security policy using the SNMPv3 user created in step 12. See Procedure “To configure NE mediation” in the *5620 SAM User Guide* for more information about configuring a SNMP mediation security policy.

14 Create a discovery rule using the new SNMP mediation security policy created in step 13. See Procedure “To configure a discovery rule” in the *5620 SAM User Guide* for more information about configuring a discovery rule.

15 Right-click on the discovered 1830 PSS device in the Equipment view and choose Launch External EMS Browser. The WebUI main view screen appears in the secure mode (https).

Note — The 1830 PSS external EMS browser is supported on Internet Explorer 6.0 or later or FireFox 3.6.

6 — 1830 PSS CLI sessions

6.1 CLI sessions overview

You can perform most NE management functions using the 5620 SAM client GUI. The functions that require CLI access to a managed NE include:

- validating GUI configuration actions
- configuring items that cannot be configured using the GUI; for example, creating a community on the NE
- 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. See the chapter Device CLI sessions of the *5620 SAM User Guide* and the *1830 Photonic Service Switch (PSS-1) Command Line Interface Guide* for more information.

6.2 1830 PSS CLI scripts

Before you perform the following procedure, you must change the user name and password in the mediation policy. See “Mediation and SNMP MIBs” in the *5620 SAM User Guide* for more information about the mediation policy. See the *5620 SAM Optical Parameter Reference* for more information about configuring the parameters.

Warning — Scripts that are not correctly created or applied can cause serious damage to the network. Alcatel-Lucent recommends that the system administrators clearly define user responsibilities for CLI script usage, and ensure that the scripts are verified and validated before they are run on devices in a live network.

Table 6-1 Device CLI session references

Topics	Chapter	Document
Device CLI sessions overview	Device CLI sessions	*5620 SAM User Guide*
To configure the 5620 SAM CLI console preferences	Device CLI sessions	*5620 SAM User Guide*
To open and close a 5620 SAM device CLI session	Device CLI sessions	*5620 SAM User Guide*
All topics	All chapters	*1830 Photonic Service Switch (PSS-1) Command Line Interface Guide*

Procedure 6-1 To create, run and schedule an 1830 PSS CLI script

1 Choose Tools→Scripts from the 5620 SAM main menu. The Scripts form opens.

2 Choose CLI Script (Scripting) from the object drop-down menu and click Create. The CLI Script (Create) form opens.

3 Configure the required parameters.

Enable the Use Latest Version parameter to associate all of the targets of the script with the latest version of the CLI script.

You can set the Content Type parameter to one of the following:

- CLI
- Velocity

Note — If you choose Velocity, you can import a script by clicking on the Import button in the right panel of the Script Manager form.

4 Click the Add icon to add the NE types and click Apply.

5 Click on the Versions tab and click Create to create a script. The Script Editor *script_name* form opens

6 Create a version for a set of commands that must be run on the 1830 PSS. The following commands can be created:

- show version—displays the device software release information
- show xc brief —lists the cross-connects on the NE
- whoami—lists the user logged in to the NE

7 Click on the Targets tab and click Create. The Target Configuration form opens.

8 Click on the Add icon to add the target on which the created script must be run. The Select Network Elements form opens.

9 Choose the target and click OK. The specific target appears on the Target Configuration form.

10 Click OK. The target is created and the CLI Script (Edit) form opens.

11 Perform one of the following in the right panel to run the script:

a Click Execute to execute the script. Go to step 13.

b Click Schedule. The Script Scheduled Task (Create) form opens.

12 Schedule a script:

i Configure the required parameters.

ii From the Schedule panel, click Select. The Select Schedule - Script Scheduled Task form opens.

iii Click Create. The SAM Schedule (Create) form opens.

iv Configure the required parameters in the Information, Time Settings, Schedule Settings, and Frequency Settings panel.

v Click OK. The Select Schedule - Script Scheduled Task form opens.

vi Choose the schedule task and click Properties. The Script Scheduled Task (Create) form opens.

vii Click Apply. The schedule is created and runs at the scheduled time.

viii After the schedule is created, the Schedule tab appears on the CLI Script (Edit) form, which displays the schedule information.

13 Click Show Results to view the results of the executed script or the scheduled script.

Note — The Schedule column displays the executed script as N/A. The scheduled script displays information about the Schedule manager and the script.

14 Close the forms.

1830 PSS device management

7 — 1830 PSS discovery

7.1 Device discovery overview

The 5620 SAM discovers the 1830 PSS devices and reconciles their properties with the contents of the database.

WDM device discovery

The 5620 SAM discovers the WDM devices using SNMP. The 1830 PSS WDM device must be commissioned and preconfigured before the 5620 SAM can manage the device. When the preconfiguration is complete, the 5620 SAM can discover the device.

During the discovery process, the IP address that is used to discover an 1830 PSS device is the Loopback IP address (also called the system ID) of the 1830 PSS device. When the system ID is used to discover a device, the management is in-band. When the management IP address of the device management port is used to discover a device, the management is out-of-band. See section 7.3 for more information about in-band and out-of-band management.

Note 1 — Before device discovery, ensure that the SNMP Source parameter of the 1830 PSS device is set to Loopback IP only using the WebUI or CLI.

Note 2 — If you need to change the system name and system ID of a device, you must unmanage and delete the device from the 5620 SAM before you change the system ID, and then rediscover the device. See Procedures “To manage, suspend, or unmanage a device” and “To delete a device” in the *5620 SAM User Guide* for information about unmanaging and deleting devices.

OCS device discovery

The 5620 SAM discovers the OCS devices using TL1. The 1830 PSS OCS device must be pre-provisioned before it can be manged by the 5620 SAM. When the pre-provisioning is complete, the 5620 SAM can discover the device. See the *Alcatel-Lucent 1830 PSS-64 Installation and System Turn-up Guide* for more information about pre-provisioning the device.

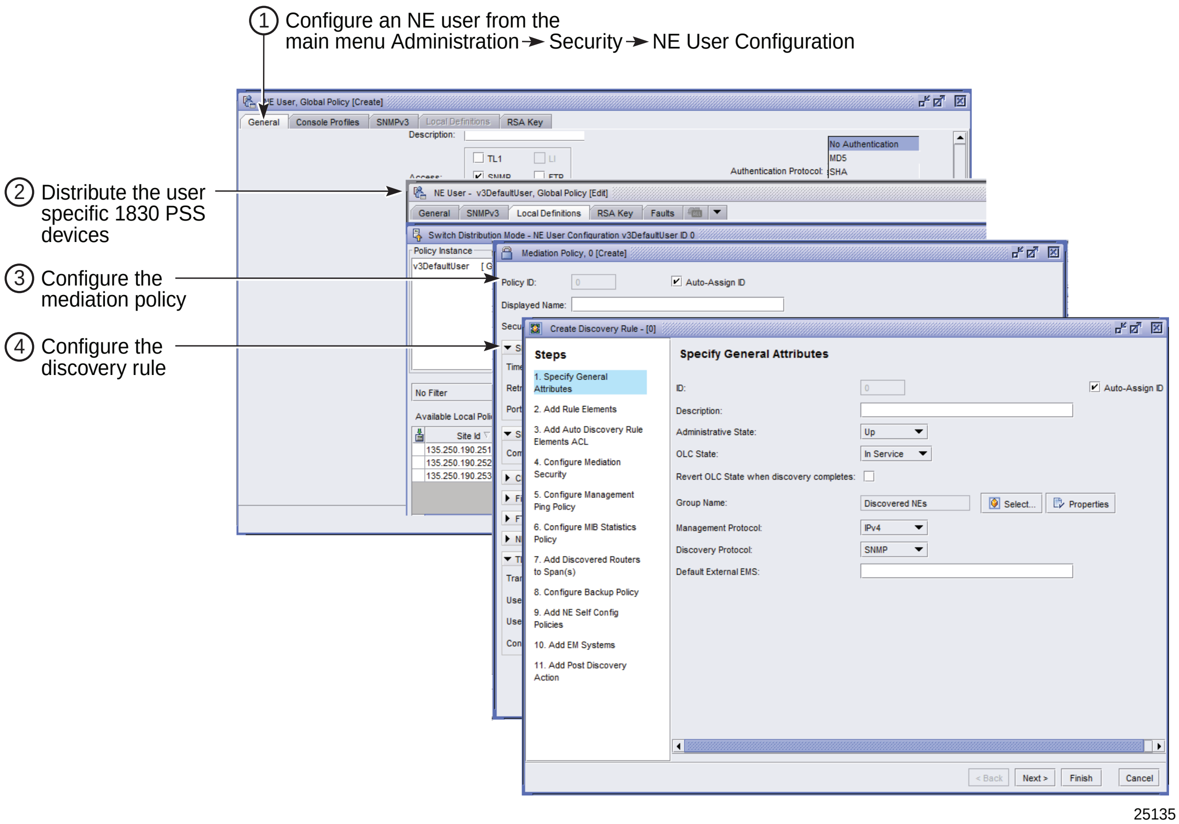
Manage or unmanage devices

You can manage or unmanage an NE. Unmanaged NEs are displayed on the topology map of the 5620 SAM GUI as an unmanaged NE icon.

Note — If you unmanage an NE, all associated optical transport services are unmanaged. If the service is rediscovered, the name of the service reverts to the default name.

7.2 Workflow to discover 1830 PSS devices

Figure 7-1 1830 PSS device discovery workflow



The following workflow describes the sequence of high-level tasks required to discover 1830 PSS devices with the 5620 SAM. Prior to discovering network devices, ensure that:

- the SNMP Source parameter of the 1830 PSS WDM device is set to Loopback IP only using the WebUI or CLI
- the 1830 PSS OCS device is pre-provisioned. See the *Alcatel-Lucent 1830 PSS-64 Installation and System Turn-up Guide* for more information about pre-provisioning the device.

From the WebUI

1 If required, configure SNMPv3 on the 1830 PSS WDM device from the WebUI. See Procedure 7-1.

From the 5620 SAM

2 Configure a user account as SNMPv2 (console) or SNMPv3 for 1830 PSS WDM or TL1 for an OCS device. See Procedure 7-2.

3 Distribute the user to specific 1830 PSS devices. See Procedure 7-3.

i If required, delete the user configuration. See Procedure 7-4.

ii If required, identify the differences between local and global users. See Procedure 7-5.

4 Configure the NE mediation policy. See Procedure 7-6.

5 Configure the discovery rule. See Procedure 7-7.

7.3 Out-of-band and in-band management

The 5620 SAM supports in-band and out-of-band management of devices for the 1830 PSS.

Out-of-band management

When you configure a device for out-of-band management only, management traffic between the 5620 SAM and the 1830 PSS device is transmitted through the management port of the device. The 5620 SAM sends management traffic to the management IP address of the 1830 PSS device.

When you configure a device for in-band and out-of-band management, one method provides redundancy for the other method. If the IP addresses are the same, redundancy is not supported. The out-of-band connection is called the primary connection and the in-band connection is called the secondary connection.

See "Device commissioning and management" of the *5620 SAM User Guide* for out-of-band management information.

In-band management

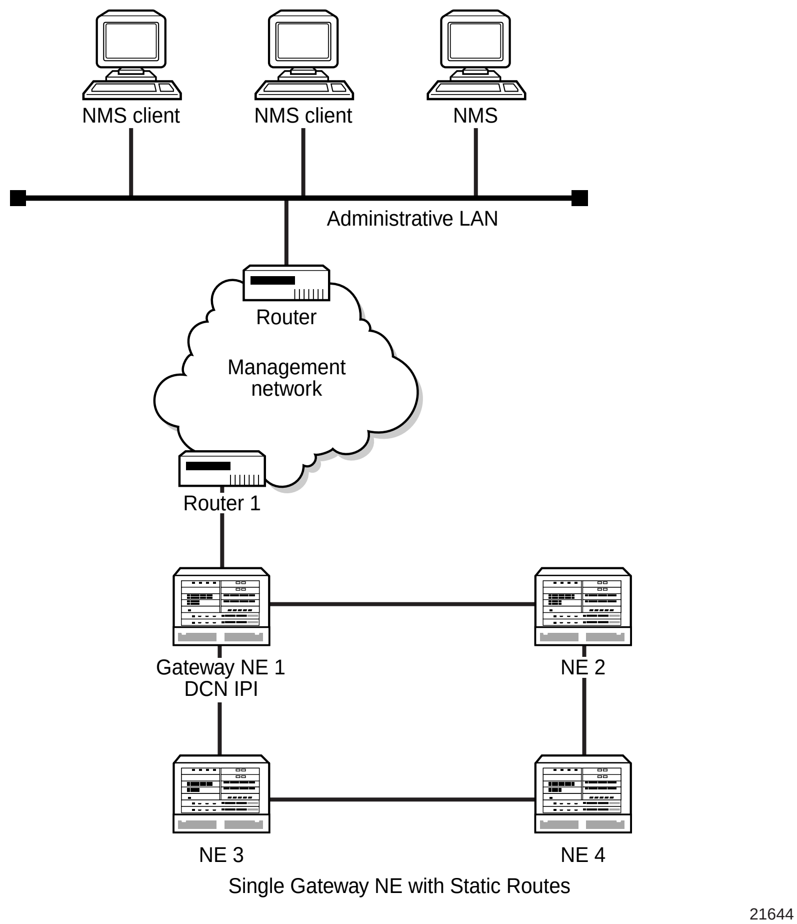
The network management system can manage an 1830 PSS-32 network by connecting to a single 1830 PSS-32 NE called a GNE. The GNE provides management connectivity to the other 1830 PSS-32 NEs in the network. The GNE communicates externally using an IP address. Non-GNE nodes are only in-band to each other. The network system does not specifically manage or configure the GNE.

The SONET, SDH, and OTN architectures support DCC and GCC, which are in-band channels that can be used for management. IP over DCC/GCC is an in-band management channel which can be used if a device is connected to a TRX-24000 client port.

Figure 7-2 shows NE 1 as the gateway NE for the ring that interconnects the cards which support OSC ports between the NEs providing inter-NE communication for network management.

See the *Alcatel-Lucent 1830 Photonic Service Switch 32/16 (PSS-32/PSS-16) Installation and System Turn-Up Guide* for more information.

Figure 7-2 In-band management



Prerequisites

You must configure the following on the 1830 PSS for a gateway NE with static routes:

- OAMP IP address
- OAMP IP address subnet mask
- Default route gateway IP address (which is redistributed)
- NE loopback IP address and subnet mask

You must configure the following for non-gateway:

- NE loopback IP address and mask

Although the 1830 PSS NEs do not exchange routing information with operating organization routers, an operating organization router that is attached to the gateway NE requires the following:

- The operating company router must have auto-negotiation enabled, or must be running in 10Mpbs half-duplex mode
- static route for the NE loopback IP address subnet

To configure the 1830 PSS to use in-band, out-of-band, or in-band and out-of-band polling at the intervals specified in a mediation policy, see the chapter Device commissioning and management of the *5620 SAM User Guide*. See the chapter Device discovery of the *5620 SAM User Guide* for information about configuring mediation policies.

Table 7-1 Out-of-band and in-band management references

Topics	Chapter	Document
In-band and out-of-band management	Device commissioning and management	*5620 SAM User Guide*
Configure GNE for management system access	S1t1and-alone node set-up	Alcatel-Lucent 1830 Photonic Service Switch 32/16 (PSS-32/PSS-16) Installation and System Turn-Up Guide

7.4 Switching modes between SONET and SDH

The 1830 PSS can be set to SONET or SDH mode using the CLI command. You cannot change the SONET or SDH mode using the 5620 SAM GUI. If you switch modes between SONET and SDH, and the mode value is changed, you would need to perform a full manual resynchronization of the NE using the 5620 SAM GUI.

When the mode is changed using a tnSysSonetSdhMode CLI command, the 5620 SAM recognizes the NE mode change and generates an alarm. The alarm must be cleared by the user. See “Alarm management” in the *5620 SAM User Guide* for more information about clearing alarms.

Caution — If the NE mode is changed to SONET or SDH, the configurations on the shelf, card, and port NE are lost. After the NE is restarted, the new mode must be reconfigured.

7.5 Device discovery procedures

Procedure 7-1 To configure SNMPv3 on an 1830 PSS devices from the WebUI

Note — This procedure is performed in the WebUI.

1 Connect to the 1830 PSS device using admin credentials. The WebUI opens with the System Properties form displayed.

2 Choose Administration→Security→Encryption→SSH Key. The SSH KEY form opens.

3 Click Generate and click OK. The SSH key is generated.

4 Click Close. The SSH KEY form closes and the System Properties form reappears.

5 Configure the UI Mode parameter as Encrypted or Fips and click Submit.

Note 1 — Configure the UI mode parameter as Normal or Encrypted for the authentication protocol MD5 and privacy protocol AES128.

Note 2 — Configure the UI mode parameter as Fips for the authentication protocol SHA and the privacy protocol AES256.

Note 3 — Configuration of the UI mode parameter as Fips is only allowed if the existing mode is Normal.

Note 4 — You cannot switch directly between Encrypted and Fips, or vice versa.

6 Click OK. The 1830 PSS device reboots.

Note — The 1830 PSS devices support the creation of a default SNMP user at initial startup with a known password. This known password permits 5620 SAM to perform auto-discovery of NEs. The default SNMP user cannot be deleted. It can only be disabled.

7 Connect to the 1830 PSS device using admin credentials. The WebUI opens with the System Properties form displayed.

8 Choose Administration→Security→SNMP v3 Users. The SNMP v3 Users form opens.

9 Click Create. The Create SNMP v3 Users form opens.

10 Configure the required parameters, save your changes and close the forms.

Procedure 7-2 To configure a user account on an 1830 PSS device

1 Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens.

2 Click Create. The NE User Global Policy (Create) form opens.

3 Configure the parameters.

4 Perform one of the following:

a SNMPv2 (Console) user:

i Select Console in the Access panel.

ii Configure the parameters for SNMPv2 (Console) user in the following panels:

- Set New Password (Console and/or FTP)
- File System Permissions
- Console Login Permissions
- PSS Specific Attributes

b SNMPv3 user:

i Select SNMP in the Access panel.

ii Click on the SNMPv3 tab.

iii Configure the required parameters.

Note 1 — When the Authentication Protocol parameter is set to MD5, set the Privacy Protocol parameter to AES-128.

Note 2 — When the Authentication Protocol parameter is set to SHA, set the Privacy Protocol parameter to AES-256.

Note 3 — Provide the same user name and password that was provided during the SNMPv3 user creation in the Procedure 7-1.

iv Configure the parameters in the Set New Authentication Password panel.

v Configure the parameters in the Set New Privacy Password panel.

vi Configure the parameters in the PSS Specific Attributes panel.

Note 1 — Configure the Access Privilege parameter to NMS or Admin to obtain complete privileges.

Note 2 — Configuring the Access Privilege parameter to Provisioner, Observer, or Crypto will restrict access to certain functions.

c TL1 user:

i Select TL1 in the Access panel.

ii Click on the TL1 tab.

iii Configure the required parameters.

5 Save your changes and close the forms.

6 If required, distribute the global users to specific devices. See Procedure 7-3.

7 If required, perform an audit to identify the differences between two local users or a global and a local user. See Procedure 7-5.

Procedure 7-3 To distribute a user account to 1830 PSS devices

1 Create the user as described in Procedure 7-2.

2 Choose Administration→Security→NE User Configuration. The NE User Configuration form opens.

3 Choose a user and click Properties. The NE User - Global Policy (Edit) form opens.

4 When the Configuration Mode parameter is Draft, the Distribute button or the Distribute option under the More Actions button, is disabled and the policy cannot be distributed to the 1830 PSS devices. You must first release the policy for distribution. If the Configuration Mode parameter is Released, go to step 5.

i Click Switch Mode and a dialog box appears.

ii Click Yes and the configuration mode of the policy is changed to Released. The Release - SR Local User form opens with a list of available nodes.

iii Go to step 6.

5 Click Distribute. The Distribute - SR Local User form opens.

6 Choose the 1830 PSS devices from the Available Nodes list and click on the right arrow icon. The devices move to the Selected Nodes list on the right side of the form.

7 Click Distribute. The policy is distributed to the devices.

8 Close the Distribute - SR Local User form. The NE User - Global Policy (Edit) form reappears.

9 Configure the distribution mode of the local definitions.

i Click Distribution Mode. The Distribution Mode - SR Local User form opens.

ii Configure the Distribution Mode parameter. The local definitions that are configured with the specified distribution mode are listed.

iii Choose one ore more rows from the Available Nodes list.

iv Click on the right arrow icon. The devices move to the Selected Nodes list on the right side of the form.

v Click Sync With Global or Local Edit, depending on the distribution mode of the specified devices.

vi Close the Distribution Mode - SR Local User form. The NE User - Global (Edit) form reappears.

10 Close the forms.

Note — The SNMPv3 users cannot be distributed on 1830 PSS devices discovered using SNMPv2.

Procedure 7-4 To delete an 1830 PSS user configuration

1 Choose Administration→Security→NE User Configuration. The NE User Configuration form opens with a list of NE Users displayed.

2 Perform one of the following:

a Choose the user that needs to be deleted and click Delete.

Note — If you delete a global policy, all of the local instances are deleted.

b To delete a local user:

i Choose the global user containing the local user that needs to be deleted and click Properties. The NE User Global Policy (Edit) form opens.

ii Click on the Local Definitions tab. The 1830 PSS devices are listed.

iii Choose an entry and click Delete.

Procedure 7-5 To identify differences between a global and local 1830 PSS user or two local 1830 PSS users

1 Choose Administration→Security→NE User Configuration. The NE User Configuration form opens.

2 Choose the NE user local or global policy that you want to compare with another policy.

3 Click Properties. The NE User (Edit) form opens.

4 Click Local Audit On. The Local Audit form opens.

> **Note —** You can cancel the local audit at any time by clicking on Local Audit Off on the NE User (Edit) form.

5 Perform one of the following from the Policy scope drop-down menu:

- **a** Choose Global and click OK. The local user is compared with the global user.
- **b** Choose Local and perform the following:
  - **i** Click Select to choose an NE. The Select a Network Element form opens.
  - **ii** Select the required NE from the list and click OK. The local users are compared.

6 View the differences between the policies by clicking on the tabs that are highlighted with an arrow icon, which indicates that differences exist between the forms. A purple arrow indicates that an attribute is set differently between the two audited forms.

Procedure 7-6 To configure NE mediation

Perform this procedure to configure the mediation policy for 1830 PSS devices.

1 Choose Administration→Mediation from the 5620 SAM main menu. The Mediation (Edit) form opens.

2 Click on the Mediation Security tab.

3 Click Create to create a new mediation security policy, or choose an existing policy and click Properties. The Mediation Policy form opens.

4 Configure the parameters.

5 Configure the Security Model parameter depending on the type of user.

a For SNMPv1 or SNMPv2c user:

i Configure the Security Model parameter as SNMP v1 or SNMP v2c.

ii Configure the Community String parameter in the SNMPv1/v2c panel.

b For SNMPv3 user:

i Configure the Security Model parameter as SNMP v3 (USM).

ii Select the v3DefaultUser or the specific SNMPv3 user configured as per Procedure 7-2.

6 Configure the required parameters in the TL1 panel for OCS devices.

7 Retain the default values for all other parameters in the Mediation Policy (Edit) form.

8 Save your changes and close the form.

Procedure 7-7 To configure a discovery rule

1 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager form opens.

2 Click Create. The Specify General Attributes step form opens.

3 Configure the required parameters.

4 Select a equipment group.

Note — If the selected equipment group reaches the maximum element limit, any additional discovered NEs are automatically added to the Discovered NEs group.

5 Configure the Discovery Protocol parameter to SNMP for WDM devices and TL1 for OCS devices.

6 Click Next. The Add Rule Elements form opens.

7 Click Create to add a new rule element. The Topology Discovery Rule Element (Create) form opens.

8 Configure the required parameters and click OK.

9 Repeat steps 7 to 8 to create an additional rule element, if required.

10 Click Next. The Add Auto Discovery Rule Elements ACL form opens.

11 Retain the default values and click Next. The Configure Mediation Security form opens.

12 Perform one of the following:

a Select the specific mediation security policy in the following panels and click Next.

- Read Access Mediation Policy
- Write Access Mediation Policy
- Trap Access Mediation Policy
- Security Access Mediation Policy

Note — The OCS NE mediation requires only the Read Access Mediation Policy for connection establishment. The other policies can retain the default values.

b Overwrite the default policy or create a copy of the mediation policy.

i Click Properties in the Read Access Mediation Policy panel. The Mediation Policy (Edit) form opens.

ii Configure the parameters depending on the Security Model parameter value.

iii For SNMPv1 or SNMPv2c, configure the Community String parameter.

iv For SNMPv3, select the v3Default user or a specific user.

Note — It is recommended that SNMPv3 user with NMS or Admin access privilege should be used in discovery rule to discover the 1830 PSS device in the 5620 SAM.

v Click Next.

13 Retain the default values for all other parameters in the remaining step forms.

14 Click Finish.

15 Save your changes and close the forms.

8 — 1830 PSS backup and upgrade

8.1 Backing up and restoring files on the 1830 PSS NEs

The WDM devices support SFTP and TFTP data transfer. The OCS devices support SFTP data transfer.

Encrypted file transfer

During the SFTP data transfer, the NE communicates with an external SSH server that runs on the database backup and software repository machine. The 5620 SAM runs on the same machine.

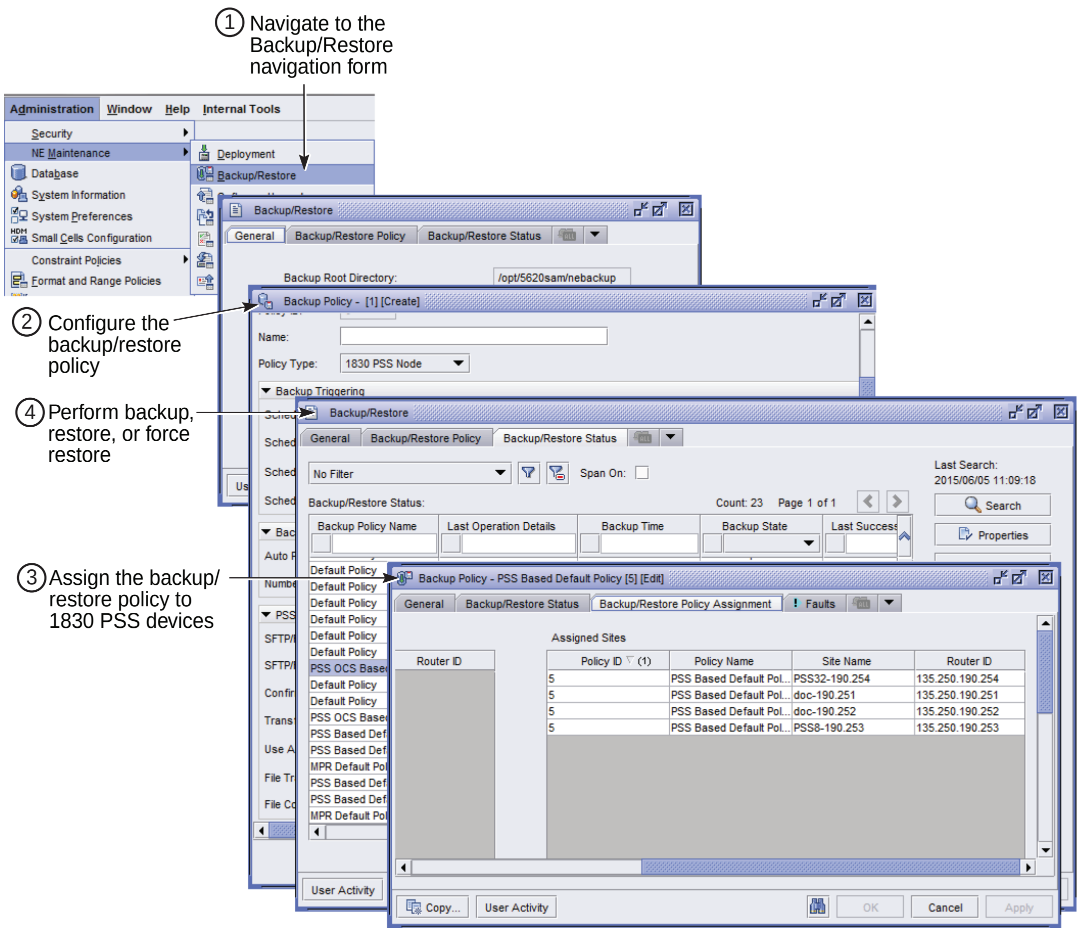
Previous configurations supported in the CLI are valid for software configuration or database configuration. The option is available in the transfer protocol field, and must be used to initiate an SFTP-based transfer.

For software and database downloads, the applications that run on the NE are SSH or SFTP clients which connect to an external SSH server. Authentication is password-based only. Public key-based authentication is not supported. As a result, you can initiate SFTP-based database and software download operations even when an encryption key is not generated.

For more information about backup and restore, see “5620 SAM database management” in the *5620 SAM System Administrator Guide*.

8.2 Workflow to backup and restore an 1830 PSS device

Figure 8-1 Backup and restore workflow



25130

1. Configure a backup/restore policy. See Procedures 8-1 and 8-2 for more information about how to configure backup/restore policies for WDM and OCS devices.

2. Assign a backup/restore policy to the 1830 PSS devices. See Procedure 8-4.

3. Perform an on-demand 1830 PSS device backup. See Procedure 8-4 for more information about how to configure on-demand 1830 PSS device backup for WDM and OCS devices.

4. If required, import specific 1830 PSS device backup files from a file system to the 5620 SAM. See Procedure 8-5.

5. If required, export specific 1830 PSS device backup files from the 5620 SAM to a client file system. See Procedure 8-6.

6 If required, restore a backed up 1830 PSS device configuration. See Procedures 8-7 and 8-8 for WDM and OCS devices respectively.

7 If required, force restore an 1830 PSS device configuration. See Procedure 8-9.

8.3 Procedures to backup and restore 1830 PSS devices

Procedure 8-1 To configure an 1830 PSS WDM backup/restore policy and assign the policy to NEs

Note — The default backup policy is automatically assigned to 5620 SAM-managed NEs that do not have an assigned backup policy.

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens.

2 Click on the Backup/Restore Policy tab and click Create. The Backup Policy (Create) form opens.

3 Perform one of the following to specify whether backup functionality is enabled:

a Select the Enable Backup check box.

b Deselect the Enable Backup check box. Go to step 9.

4 Set the Policy Type parameter to 1830 PSS Node.

5 Configure the required parameters in the Backup Triggering and Backup Purging panels.

6 Configure the required parameters in the PSS Backup/Restore Settings panel.

Note — If the Transfer Protocol parameter is set to SFTP, the SFTP User ID, SFTP Password, and the Server IP parameter values must be authenticated.

7 Perform one of the following to configure the server to save the backup files:

a Select the Use Active Server check box.

b Deselect the Use Active Server check box and configure the Server IP parameter.

8 Save your changes and close the form.

9 Assign the policy to the 1830 PSS devices, as required.

i Choose Administration→NE Maintenance→Backup/Restore, choose the new policy in the list and click Properties. The Backup Policy (Edit) form opens.

ii Click on the Backup/Restore Policy Assignment tab. The Backup Policy (Edit) Filter form opens.

iii Configure the policy filter criteria, as required and click OK. The Backup Policy (Edit) Filter form closes.

iv Choose one or more 1830 PSS devices in the Unassigned Sites list and click on the right arrow key to move 1830 PSS devices to the Assigned Sites list.

v Save your changes and close the form.

Procedure 8-2 To configure an 1830 PSS OCS backup/restore policy and assign the policy to NEs

Note — The default backup policy is automatically assigned to 5620 SAM-managed NEs that do not have an assigned backup policy.

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens.

2 Configure the general backup policy parameters.

3 Click on the Backup/Restore Policy tab.

4 Click Create. The Backup Policy (Create) form opens.

5 Enable or disable the backup functionality:

a Select the Enable Backup check box.

b Deselect the Enable Backup check box. Go to step 8.

6 Configure the general backup policy parameters.

Note — Configure the Policy Type parameter as 1830 PSS OCS Node.

7 Configure the required parameters in the Backup Triggering and Backup Purging panels.

8 Configure the SFTP parameters in the PSS Backup/Restore Settings panel.

9 Configure the backup server:

a Select the Use Active Server parameter.

b Deselect the Use Active Server parameter and configure the Server IP and File Transfer Server Directory parameters.

Note 1 — The 5620 SAM appends the site name to the file transfer server directory configured in the PSS Backup/Restore Settings panel. Before performing the backup, you must ensure that the directory exists on the remote server.

- For example, if the File Transfer Server Directory parameter is configured as **/user/ocs_backup**, and you are performing a backup of the site with Site Name as SITE_123, then you must ensure that **/usr/ocs_backup/SITE_123** directory exists in the remote server.
- If the File Transfer Server Directory parameter is not configured in the PSS Backup/Restore Settings panel, the default directory for the backup of the site with Site Name as SITE_123 is **/opt/5620sam/server/nms/samNodeBackup/1830OCS/SITE_123**.

Note 2 — In case of remote server backup, the 5620 SAM does not compress the backup file.

Note 3 — If a backup exists for an OCS device, then you must move the existing backup to another location, before performing the next backup for a particular OCS device.

10 Save your changes and close the form.

11 Assign the policy to the 1830 PSS OCS devices.

i Choose the new policy from the list in the Backup/Restore form and click Properties. The Backup Policy (Edit) form opens.

ii Click on the Backup/Restore Policy Assignment tab. The Backup Policy (Edit) Filter opens.

iii Apply the filter criteria as required.

iv Choose one or more OCS devices from the Unassigned Sites list and click on the right arrow button to move OCS devices to the Assigned Sites list.

v Save your changes and close the forms.

Procedure 8-3 To assign a backup policy to 1830 PSS devices

Note — The default backup policy is automatically assigned to 5620 SAM-managed NEs that do not have an assigned backup policy.

1 Choose Administration→NE Maintenance→Backup/Restore, choose the new policy in the list and click Properties. The Backup Policy (Edit) form opens.

2 Click on the Backup/Restore Policy Assignment tab. The Backup Policy (Edit) Filter form opens.

3 Configure the policy filter criteria, as required and click OK. The Backup Policy (Edit) Filter form closes.

4 Choose one or more 1830 PSS devices in the Unassigned Sites list and click on the right arrow key to move 1830 PSS devices to the Assigned Sites list.

5 Save your changes and close the form.

Procedure 8-4 To perform an on-demand 1830 PSS backup

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens.

2 Perform one of the following.

a For OCS devices:

i Click on the Backup/Restore Policy tab.

ii Choose the OCS backup policy and click Properties. The Backup Policy (Edit) form opens.

iii Configure the required parameters in the PSS Backup/Restore Settings panel.

iv Click OK to confirm. The Backup/Restore form reappears.

b Go to step 3 for WDM devices.

3 Click on the Backup/Restore Status tab, choose an OCS or a WDM device, and click Backup.

4 Confirm the changes to start the backup and close the form after successful backup.

Note — The status of the backup is displayed in the Last Operation Details column of the Backup/Restore form.

Procedure 8-5 To import an 1830 PSS device backup from a file system to the 5620 SAM database

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 Import. If the Import button is not visible, click on the More Actions button and choose Import. A file navigator form opens.

5 Use the form to specify the directory that contains the device backup and click OK.

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, and the import fails. Click OK to close the dialog box.

6 Save your changes and close the forms.

Procedure 8-6 To export device backup files from the 5620 SAM to file system

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. A list of backups for the selected device appears, ordered from the oldest to the most recent.

5 Choose a specific backup in the list and click Export. A file navigator form opens.

6 Use the form to specify the directory that is to contain the exported device backup and click OK. The NE configuration backup is saved to the specified directory.

7 Save your changes and close the forms.

Procedure 8-7 To restore a WDM 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 8-4 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. A list of configuration backups for the selected device appears, ordered from the oldest to the most recent.

5 Choose a backup in the list and click Restore. A dialog box appears.

6 Click Yes.

7 Right-click on the device on the navigation tree and choose Resync and ensure that the latest network information is available.

Note — The status of the restore is displayed in the Last Operation Details column of the Backup/Restore form.

8 Save your changes and close the forms.

Procedure 8-8 To restore an OCS 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 8-4 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 Policy tab.

3 Choose the OCS backup policy and click Properties. The Backup Policy (Edit) form opens.

4 Configure the required parameters in the PSS Backup/Restore Settings panel.

5 Click on the Backup/Restore Status tab. The managed devices are listed.

6 Double-click on a device from the list. The NE Backup/Restore Status form for the selected device opens.

7 Click on the Backups tab to list the configuration backups for the selected device, sorted from the oldest to the most recent.

8 Choose the specific backup in the list and click Restore.

9 Save your changes and close the forms.

10 Right-click on the device on the equipment tree and choose Resync and ensure that the latest network information is available.

Note — The status of the restore is displayed in the Last Operation Details column of the Backup/Restore form.

Procedure 8-9 To force restore a device configuration

You can choose to restore a device configuration using the configuration of another 1830 PSS OCS or WDM (1830 PSS-32) device to meet special network requirements by importing that device configuration and performing a forced restore. The default restore rejects the OCS device configuration if the loopback IP address and region parameter values do not match. You can perform a force restore where the 5620 SAM requests the NE to override the following validations and restores the device configuration despite the existence of failure conditions.

- Software release identifier mismatch
- SID mismatch
- Time stamp mismatch
- Region mismatch

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 8-4 before you proceed.

1 Import the device configuration from a specific node. See Procedure 8-5.

2 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM menu. The Backup/Restore form opens.

3 Click on the Backup/Restore Status tab. The managed devices are listed.

4 Double-click on a device from the list. The NE Backup/Restore Status form for the selected device opens.

5 Click on the Backups tab. A list of configuration backups for the selected device appears, ordered from the oldest to the most recent.

6 Choose the specific backup in the list and click Force Restore.

7 Save your changes and close the forms.

8 Right-click on the device on the navigation tree and choose Resync and ensure that the latest network information is available.

Note — The status of the restore is displayed in the Last Operation Details column of the Backup/Restore form.

8.4 Managing 1830 PSS software upgrades

When an 1830 PSS device needs a software upgrade to another software version, you can use the 5620 SAM to perform an on-demand or scheduled NE software upgrade 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:

- whether to activate the software after the software is transferred to the NE
- whether to reinitialize the NE after the upgrade

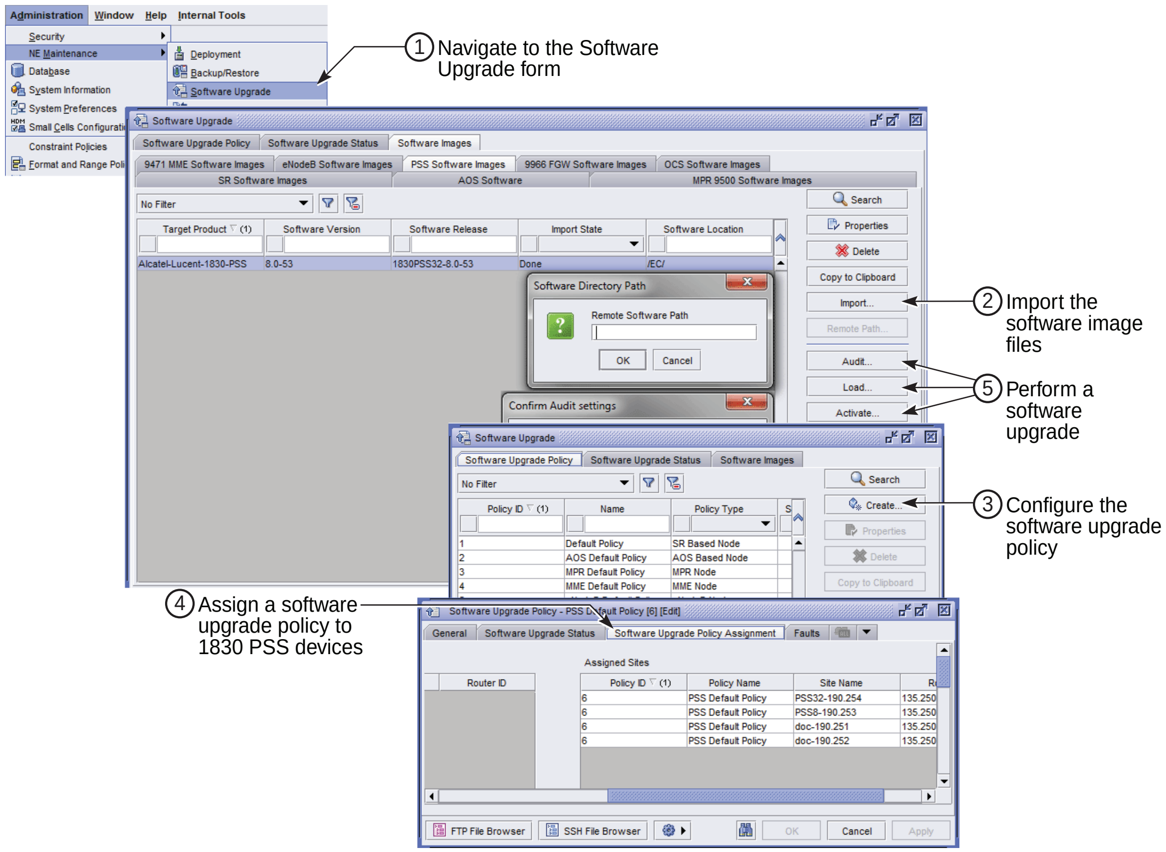
During a software upgrade, the 5620 SAM performs checks to ensure that the new software is compatible with the device type and that the required files are present. The 5620 SAM initiates a device software upgrade only when the required conditions exist. You can use the 5620 SAM to roll back a software upgrade to the previous version if an upgrade fails.

For more information about the error descriptions, see the following guides:

- *Alcatel-Lucent 1830 Photonic Service Switch 36 Installation and System Turn-up Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch 64 Installation and System Turn-up Guide*
- *5620 SAM System Administrator Guide*
- *Alcatel-Lucent 1830 Photonic Service Switch 36/32/16 (PSS-36/PSS-32/PSS-16) User Provisioning Guide*

8.5 Workflow to configure an 1830 PSS software upgrade

Figure 8-2 Software upgrade workflow



1. Import 1830 PSS device software image files to the 5620 SAM database.

   See Procedures 8-10 and 8-11 for more information about how to import WDM and OCS software images respectively.

2. Configure a software upgrade policy. See Procedure 8-12.
3. Assign a software upgrade policy to an 1830 PSS device. See Procedure 8-13.
4. Perform an immediate software upgrade. See Procedure 8-14.
5. If required, schedule an automatic software upgrade. See Procedure 8-15.
6. If required, view the status of the software upgrade. See Procedure 8-16.

8.6 Procedures to manage NE software upgrades

Use the following procedures to perform 1830 PSS software upgrades.

Procedure 8-10 To import 1830 PSS WDM device software image files to the 5620 SAM database

1 Copy or move the device software to a directory that is accessible to the 5620 SAM. The directory can be on the local server or an accessible remote server.

> **Note —** The directory must contain a valid and complete set of device software files. See the *1830 PSS Release Notes* for a complete list of files.

2 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

3 Click on the Software Images tab and then on the PSS Software Images tab.

4 Perform one of the following:

a Import image files from the 5620 SAM directory on the local server:

i Click Import. The Select import PSS Software window appears.

ii Navigate to the directory that contains the software image file and select the image directory.

> **Note —** Ensure that the image directory name is in the following format:
>
> `<1830PSSxx-software version/>`
>
> where xx can be: 4, 16, or 32, depending on the device variant that you are upgrading. For example: 1830PSS4-6.0-37/. In this example, the device is a 1830 PSS-4 and the software version is 6.0-37.

iii Click Open. The Import Image dialog box appears.

iv Click Yes. When the import is complete, an entry for the image file appears in the list.

b Import 1830 PSS software from a remote location with FTP support:

> **Note 1 —** The remote system address is the server IP address that is configured in the policy of the associated NE. See Procedure 8-12 for more information about creating a software upgrade policy.
>
> **Note 2 —** When using FTP, the default user login directory is typically "/var/ftp".

i Click Remote Path. A Remote Path notification box appears.

ii Click Yes. The Software Directory Path form opens.

iii Enter the Remote Software Path. The software upgrade files must have the last directory specified in the path described in the Table 8-1.

Table 8-1 Remote path

Device	Default login directory	Format	Example
1830 PSS-4	/var/ftp	</EC/1830PSS4-software version>	/EC/1830PSS4-8.0-62 where the device is 1830 PSS-4 and the software version is 8.0-62
1830 PSS-8	/var/ftp	</EC/1830PSS8-software version>	/EC/1830PSS8-8.0-12 where the device is 1830 PSS-8 and the software version is 8.0-12
1830 PSS-16	/var/ftp	</EC/1830PSS16-software version>	/EC/1830PSS16-7.0-57 where the device is 1830 PSS-16 and the software version is 7.0-57
1830 PSS-32	/var/ftp	</EC/1830PSS32-software version>	/EC/1830PSS32-6.0-43 where the device is 1830 PSS-32 and the software version is 6.0-43

When the remote path import is complete, an entry for the image file appears in the list.

5 Save your changes and close the forms.

Procedure 8-11 To import 1830 PSS OCS device software image files to the 5620 SAM database

1 Copy or move the device software to a directory that is accessible to the 5620 SAM. The directory can be on the local server or an accessible remote server.

Note — The directory must contain a valid and complete set of device software files. See the 1830 PSS 36/64 Release Notes for a complete file listing.

2 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

3 Click on the Software Images tab and then on the OCS Software Images tab.

4 Perform one of the following:

a To import image files from the 5620 SAM directory on the local server:

i Click Import. The Select Import PSS Software window appears.

ii Navigate to the directory that contains the software image file and select the image directory.

Note — Ensure that the image directory name is in the following format:

`<software version/>`

iii Click Open. The Import Image dialog box appears.

iv Click Yes. When the import is complete, an entry for the image file appears in the list.

b To provide a remote path for the 1830 PSS OCS software:

Note — Ensure that the server IP address is configured in the software upgrade policy of the associated NE. See Procedure 8-12 for information about creating a software upgrade policy.

i Click Remote Path. A Remote Path notification box appears.

ii Click Yes to continue. The Software Directory Path dialog box appears.

iii Enter the Remote Software Path. The software upgrade files must have the last directory specified in the path, as follows:

`</root/FLC/software version/>`

For example: /root/FLC/08.08.12

Note 1 — Ensure that the format of the software version is “xx.xx.xx”.

Note 2 — See the current *5620 SAM Network Element Compatibility Guide* for more information about the load that you need to upgrade or downgrade.

5 Close the Software Upgrade form.

Procedure 8-12 To create a software upgrade policy

The 5620 SAM uses an 1830 PSS-specific software upgrade policy to download 1830 PSS software. A default 1830 PSS software upgrade policy is created when the 5620 SAM initializes.

Use the following procedure to create a policy that you can use to perform an on-demand or scheduled device software image upgrade. Contact your Alcatel-Lucent technical support representative for information about downgrades.

Ensure that:

- you validate the default user directory at login to determine the appropriate path for WDM devices. When using FTP, you can run pwd to display the default login directory. A typical return example would be "/var/ftp"
- appropriate FTP accounts are configured and available on the devices to which you intend to apply the policy for WDM devices
- device configuration files are backed up for OCS and WDM devices

1 Perform Procedure 8-10 to import the 1830 PSS OCS device software image file or Procedure 8-11 for 1830 PSS WDM device.

2 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

3 Click Create. The Software Upgrade Policy (Create) form opens.

4 Configure the 1830 PSS Node for the Policy Type parameter, if your are configuring a WDM device, and 1830 PSS OCS Node for an OCS device.

5 Configure the required parameters in the PSS Based Setting panel.

6 If you deselect the Use Active Server parameter in step 5, configure the Server IP parameter.

7 Configure the required parameters in the PSS Audit Setting panel, for a WDM device.

Note — If you want to use the Revert function, ensure that you select the Node Backup check box in the PSS Audit Setting panel.

8 Save your changes and close the forms.

Procedure 8-13 To assign a software upgrade policy to an 1830 PSS

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

2 Choose a software upgrade policy from the list and click Properties. The Software Upgrade Policy (Edit) form opens.

3 Click on the Software Upgrade Policy Assignment tab, configure the filter parameters, as required and click OK.

4 Choose one or more NEs in the Unassigned Sites list and click on the right arrow to move the NEs to the Assigned Sites list.

5 Save your changes and close the forms.

Procedure 8-14 To perform an immediate software upgrade

Before you perform the steps, ensure that:

- the required software image files are imported to the 5620 SAM database. See Procedure 8-10 to import the 1830 PSS OCS device software image file or Procedure 8-11 for 1830 PSS WDM device.
- the node is assigned to the appropriate software upgrade policy. See Procedure 8-13.

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 are configuring an OCS device:

i Choose the OCS upgrade policy and click Properties. The Software Upgrade Policy (Edit) form opens.

ii Configure the required parameters in the PSS Based Setting panel.

iii Click OK to confirm the changes and the Software Upgrade form reappears.

iv Click on the Software Images tab, then on the OCS Software Images tab.

b If you are configuring a WDM device, click on the Software Images tab, then on the PSS Software Images tab.

3 Perform one of the following node level upgrades:

a separate audit, load, and activate tasks. Go to step 4.

b single task. Go to step 5.

c scheduled task. See Procedure 8-15.

4 Perform the audit, load, and activate as separate tasks. See the *1830 PSS User Provisioning Guide* for more information about the audit, load, and activate tasks.

Audit the 1830 PSS software image file to verify the software load on the 5620 SAM local server or remote server.

i Choose the appropriate 1830 PSS software image file from list, click Audit, configure the Audit Settings parameter, and select the 1830 PSS device.

Note 1 — If you choose the Default Audit Settings option, the policy level settings are used.

Note 2 — Click on the Software Upgrade Status tab to view the progress of the audit.

Note 3 — Verify that the software is successfully audited before you go to step ii.

ii Click Load and select the 1830 PSS device.

Note 1 — The load operation may take considerable time to complete.

Note 2 — Click on the Software Upgrade Status tab to view the progress of the audit.

Note 3 — Verify that the audited software is successfully loaded before you go to step iii.

iii Click Activate, and select the 1830 PSS device.

Note — The activate operation may take considerable time to complete.

iv Go to step 6.

5 Choose the appropriate 1830 PSS software image file from list, click Auto Upgrade, and select an 1830 PSS device.

Note 1 — If you choose the Default Audit Settings option, the policy level settings are used.

Note 2 — Click on the Software Upgrade Status tab to view the progress.

6 Perform one of the following:

a Click Commit and select an 1830 PSS device.

> **Note —** You can commit the active release at any time after the software release has been activated.

b Click Revert and select an 1830 PSS device.

> **Note —** You can revert to a previously committed software release at any time during the software upgrade process.

7 Save your changes and close the forms.

Procedure 8-15 To schedule an automatic software upgrade

See "5620 SAM-based schedule procedures" in the *5620 SAM User Guide* for information about creating schedules. Before you perform the procedure, ensure that the required software image files are imported to the 5620 SAM database (see Procedure 8-10 to import the 1830 PSS OCS device software image file or Procedure 8-11 for 1830 PSS WDM device), and that the node is assigned to the appropriate software upgrade policy (see Procedure 8-13).

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 and click on the Software Images tab.

> **Note —** The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

3 Choose a software image in the list and click Schedule. The Confirm Audit Settings dialog box appears.

4 Choose an option from the Audit Settings and click OK. The AutoUpgrade - Select Sites form opens.

> **Note —** If you choose the Default Audit Settings option, the policy level settings are used.

5 Select the node that you need to upgrade and click OK. The Select Schedule - Select Schedule form opens.

6 Choose a schedule in the list and click OK. The Schedule Upgrades dialog box appears. See the *5620 SAM User Guide* for information about creating schedules.

7 Click Yes. The 5620 SAM schedules the upgrade.

8 Perform one of the following:

a Commit the activated software release to the node.

i Click Commit. The Commit - Select Sites form opens with a list of nodes that have activated software displayed.

ii Select the node where you need to commit the activated software release and click OK. The Commit dialog box appears.

iii Click Yes.

b Revert the node to the previously committed software release.

i Click Revert. The Revert - Select Sites form opens with a list of nodes that have activated software displayed.

ii Select the node where you need to revert the software release and click OK. The Revert dialog box appears.

iii Click Yes.

9 Save your changes and close the forms.

Procedure 8-16 To view the status of a software upgrade

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

2 Click on the Software Upgrade Status tab.

3 Choose the node from the list and click Properties. The Software Upgrade Status (View) form opens.

4 Click on the Software Upgrade tab. The values of the Last Operation Status and Last Operation Percentage Completed parameters represent the status of the software upgrade.

5 Close the forms.

---

9 — 1830 PSS equipment management

9.1 Equipment management overview

The 5620 SAM equipment management interface consists of:

- a main menu
- contextual menus
- a navigation tree
- managed objects
- property forms to configure object parameters

The 5620 SAM is used to create, configure, and manage a device with the child objects that must be part of a network. Equipment, for example, the routers, which are at the top of the hierarchy, have properties that are configured using the CLI and are 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. See the *5620 SAM User Guide* for more information about equipment management.

9.2 Workflow to manage the 1830 PSS equipment

The workflow is used to manage the 1830 PSS. See the ***5620 SAM User Guide*** for more information about managing devices.

1 To manage the 1830 PSS equipment using the navigation tree:

  i Use the 5620 SAM to discover the 1830 PSS.

  ii Right-click on the Discovered NEs equipment group in the Equipment view of the navigation tree and choose List. You can also double-click on the Discovered NEs icon on the topology map to open the Discovered NEs form.

  iii Drag the 1830 PSS to the network icon in the Equipment view of the navigation tree or to the topology map.

  iv Right-click on the 1830 PSS device in the navigation tree and choose an option. See the ***5620 SAM User Guide*** for a list of contextual menu options.

  v Use the Properties option in the Equipment view to perform any of the following, as required:

  - Modify the device parameters
  - Create card objects in the shelf. See section 9.5 for more information.
  - View the parameters of the port objects that were created automatically with the card object. See section 9.6 for more information.
  - Modify the parameters of the created objects.

2 Verify that the 1830 PSS devices are configured before they are discovered by the 5620 SAM.

3 Access the 1830 PSS device and start the configuration and management.

From the 5620 SAM, choose Manage→Equipment→Equipment. The Manage Equipment form opens. The network administrators and operators can:

- filter views and information for the managed devices
- view and use a graphical representation of the shelf to configure equipment
- view objects and get statistical information about the NEs 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 that has at least one physical shelf
    - internal and external storage devices (flash memory)
    - physical links
    - current OLC state
- configure network and access policies for network objects; for example, ingress buffer policies for a port
- view and manage APS groups
- manage hardware fault conditions

9.3 Working with objects

Objects in the 5620 SAM 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 parameters for each object are configured for a specific function. The parameters can be managed to meet the needs of the service. Objects are created and managed using the properties forms of the Equipment view.

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 child objects are created automatically in the navigation tree after the device is discovered.

Resynchronization of objects

The Resync option of the contextual menu specifies that SNMP MIB and CLI information bases are reread to synchronize them with the 5620 SAM, which also synchronizes the network management settings with the device. The changes in the values for some of the read-only parameters from the 1830 PSS are not updated automatically. The parameters are identified by the resync icon that is beside each parameter. Click on the resync icon to display the updated parameter values.

Note — The port operational state is updated automatically.

11DPM12 card and port objects

The 11DPM12 card and port objects of 1830 PSS devices Release 5.5 and later appear differently than the other 1830 PSS cards on the navigation tree of the 5620 SAM. When you expand the 11DPM12 card object, the following objects appear on the navigation tree:

- eight ODU1PTFs
- two line ports
- 12 client ports
- two VA ports

Line port objects

The 5620 SAM supports the creation of two 11DPM12 line ports with OTU2 as the Assigned Rate parameter option on the General tab under the Port Specifics tab of the Physical Port (Edit) form. Each OTU2 line port contains an ODU2 object below the OTU2 line port on the navigation tree. The ODU2 object allows you to configure multiple low-order ODU objects below the ODU2 objects by clicking on the Configure Timeslots button on the General tab under the Port Specifics tab of the Physical Port (Edit) form. The timeslots are numbered from 1 to 8. The number of low-order ODU objects that can be created depends on the container type.

ODU1PTF objects

The 5620 SAM displays the ODU1PTF objects on the navigation tree after the 11DPM12 card is configured. The eight ODU1PTF objects are mapped to 12 client ports. An 11DPM12 card is divided into four client port groups with three client ports per group. Each port group can use two ODU1PTFs to map to the OPTSG client ports. Table 9-1 lists the client ports and the assigned ODU1PTFs.

Table 9-1 ODU1PTF mapping

Port groups	Client ports	ODU1PTF
1	C1, C2, and C3	ODU1PTF1 and ODU1PTF2
2	C4, C5, and C6	ODU1PTF3 and ODU1PTF4
3	C7, C8, and C9	ODU1PTF5 and ODU1PTF6
4	C10, C11, and C12	ODU1PTF7 and ODU1PTF8

The OPTSG objects are either configured manually or created automatically by the 5620 SAM.

To manually configure the OPTSG objects, configure the timeslots for ODU1 container type as described in Procedure 16-13. Associate the line-side LO-ODUk facility as described in Procedure 16-14. Right-click on the ODU1PTF object and choose the Configure ODU1PTF Timeslots option to configure ODU1PTF timeslots which appear as OPTSG objects under the ODU1PTF object.

During optical transport service creation, the 5620 SAM automatically creates ODU1 container on the line-side, configures the appropriate ODU1PTF objects, associates with the line-side, creates OPTSG objects, and creates the cross connect between the client port and the OPTSG object. The cascading cross connects between ODU1PTF objects across port groups are also created as required. The OPTSG objects are created when you choose OC3 or OC12 for the Rate parameter on the General tab of the Optical Transport Service (Create) form. The Assigned Rate parameter option of the client port must be set to OC3 or OC12 on the General tab under the Port Specifics tab of the Physical Port (Edit) form which automatically configures the container type as OPTSG.

The timeslots are numbered from 1 to 16. The OC3 requires one timeslot and OC12 requires four timeslots. The number of OPTSG objects created depends on the Rate parameter value.

Client port objects

The twelve client ports support the following signal rates:

- 1GbE
- 3GSDI
- FC100
- FC200
- FC400
- FE
- HDSDI
- OC3
- OC12
- OC48
- OTU1
- SDSDI

The ODU0, ODU1, ODUflex, and OPTSG containers are mapped to the signal rate as follows:

- ODU0—1GbE, FE, FC100, SDSDI, OC3 or OC12
- ODU1—FC200, HDSDI, OC48, or OTU1
- ODUflex—3GSDI, or FC400
- OPTSG—OC3, or OC12

Depending on the Assigned Rate parameter option that is specified on the General tab under the Port Specifics tab of the Physical Port (Edit) form, the corresponding client port objects appear on the navigation tree with the container type displayed.

VA port objects

The 11DPM12 cards contain two eVOA ports that are used for wavelength tracking and power adjustment. The eVOA ports appear as VA objects on the navigation tree.

9.4 Managing shelves

The 1830 PSS-32 and 1830 PSS-16 shelves provide the framework for the configuration of the 1830 PSS-32 / 1830 PSS-16 NEs. A universal shelf provides card slots, fiber management trays, backplane, power distribution, and cooling for the NE. The NEs can be deployed in a shelf or expanded to multiple interconnected universal shelves.

The first universal shelf of an NE becomes the master shelf, which provides the management and control connections to the operations systems for the cluster of shelves in a multi-shelf NE. Expansion shelves connect to the master shelf using a protected internal LAN communication link. The shelves provide extended slot capacity managed by the database that resides in the master shelf.

The universal shelf is the basic building block for the 1830 PSS-32 NE. The shelf provides a framework for the active modules in a system, for example, the controller and interface cards.

Each universal shelf has a shelf ID that can be configured using a physical mechanism (for example, a rotary dial) on the backplane. Up to eight bits of information can be set. The shelf ID determines the identity of each universal shelf in the cluster. The most significant bit of the rotary dial determines whether the shelf is the main shelf or an extension shelf.

Each shelf is equipped with mandatory modules. Some of the shelves are equipped with optional modules.

The mandatory equipment must be automatically provisioned regardless of whether the equipment is present. Each shelf includes the following mandatory equipment:

- one shelf controller (EC) in slot 1 or 18
- two power modules (PF)
- a fan module (FAN)

The user interface panel (USRPNL) is mandatory and can only reside on the main shelf. Mandatory equipment is provisioned without an AINS state. The AINS allows newly provisioned entities to be inserted later without generating alarms. Therefore, if a mandatory equipment (without AINS) is inserted later, alarms are generated.

A DCM enclosure can hold up to 16 DCMs. The system manages each DCM as a separate shelf.

See the Alcatel-Lucent *1830 Photonic Service Switch Product Information and Planning Guide* and the Alcatel-Lucent *1830 Photonic Service Switch User Provisioning Guide* for more information. See the *5620 SAM Optical Parameter Reference* for more information about parameters.

The 1830 PSS-36 and 1830 PSS-64 shelves provide the framework for the configuration of the 1830 PSS-36 and 1830 PSS-64 devices. The main shelf provides card slots, fiber management trays, backplane, power distribution, and cooling for the devices.

The 1830 PSS-36 and 1830 PSS-64 are composed of a main shelf and expansion shelves. Expansion shelves connect to the main shelf using a protected internal LAN communication link. The main shelf provides a framework for the active modules in a system, for example, the controller and interface cards. Switching can be performed until the matrix card capacity is reached.

See the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide* and the *Alcatel-Lucent 1830 Photonic Service Switch User Provisioning Guide* for more information.

1830 PSS-36 shelves

The 1830 PSS-36 has one high-speed backplane with 16 I/O card slots. The dedicated card slots on the 1830 PSS-36 support the following cards:

- MT1T9C—matrix cards
- FLC36EA—first-level controller cards
- BT36—bus termination cards
- PSFC—power supply, filter, and clock interface cards
- FAN3T8—fan unit

See the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide* and the *Alcatel-Lucent 1830 Photonic Service Switch User Provisioning Guide* for more information.

1830 PSS-64 shelves

The 1830 PSS-64 has one high-speed and two low-speed backplanes with 32 I/O card slots. The dedicated card slots on the 1830 PSS-64 support the following cards:

- MT1T9—matrix cards
- FLC64—first-level controller cards
- BT3T8/BTC3T8—bus termination cards
- PSF3T8—power supply, filter, and clock interface cards
- FAN3T8—fan units

See the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide* and the *Alcatel-Lucent 1830 Photonic Service Switch User Provisioning Guide* for more information.

1830 PSS-32 shelves

The 1830 PSS-32 system supports the following types of shelves: Universal, DCM, ITLB, and ITLU. The 1830 PSS-32 universal shelf contains 32 replaceable slots.

The SFD44 (44-channel DWDM static filter) is modelled as an OMD shelf with an SFD44 card. Other shelves that can be configured from the 5620 SAM are: SFD40, SFD40B, SFD44B, and ITLB.

The DCM and OMD shelves are passive module shelves that can contain DCMs and SFD44 modules. The modules provide dispersion compensation and the optical mux/demux function that is associated with core optics modules that is, line drivers and CWR8, respectively that are installed in the universal shelf. Each 1830 PSS-32 includes up to 8 universal shelves, and up to 24 DCM and OMD shelves.

Each 1830 PSS-32 universal shelf contains 32 slots for function cards. Two additional slots are reserved for controller cards that are configured for redundant control. Two more slots are reserved for the power filter cards. The top of the shelf contains a fan tray for cooling, a customer interface panel, and two timing interface cards that provide a redundant connection to synchronization references. See the Alcatel-Lucent *1830 Photonic Service Switch Product Information and Planning Guide* and the Alcatel-Lucent *1830 Photonic Service Switch User Provisioning Guide* for more information.

1830 PSS-16 shelves

In addition to the slots for the two power filters and two controller cards, the 1830 PSS-16 shelf contains 16 function card slots. The 1830 PSS-16 supports the following types of shelves: PSS 16, DCM, ITLB, and ITLU. The slots at the top of the shelf can hold two function cards or the user interface panel on units that are used as main shelves. A fan tray for cooling is located at the bottom of the shelf. The 5620 SAM supports up to eight extension shelves. See the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide* and the *Alcatel-Lucent 1830 Photonic Service Switch User Provisioning Guide* for more information.

1830 PSS-8 shelves

The 1830 PSS-8 shelf has an overall depth of 325 mm. The shelf is 33 mm high and 439 mm wide.

The 1830 PSS-8 shelf has slots 1 and 7 dedicated to power filter modules, and slots 6 and 12 dedicated to integrated shelf controllers. Slot 12 can also be used for user panel card when the protection EC is not installed in the master shelf. The electrical shelf-ID for user panel is 40.

There are eight half-slots (2 to 5, 8 to 11) capable of supporting universal I/O cards. Two half-slots (left and right) can be combined into a single full-height slot by removing the divider that separates the left slot from the right slot. Slot 13 is for the user panel and slot 14 is for the fan unit.

See Procedure 9-2 for more information about configuring the 1830 PSS shelves.

Fan unit

The Fan units used in *Alcatel-Lucent* 1830 PSS-8 shelf are controlled by the active EC through backplane links. The EC determines the speed of the fan motors on the fan unit. A local microcontroller control and monitor each associated fan motor.

Power filter cards

The 1830 PSS-8 shelf supports AC and DC power filter (PF) cards. The PF-AC card, 8AC7, accepts AC input and provides power supply to other parts of the shelf. The PF-DC card, F8DC30, accepts DC input and provides power supply to other parts of the shelf.

The 5620 SAM supports the configuration of the AC and DC power filter cards in slot 1 by setting the PFA Expected parameter value to AC7 or DC30 on the Shelf (Edit) form. The card object in slot 1 changes to PFAC or PFDC on the equipment tree, depending on the PFA Expected parameter setting.

The 5620 SAM supports the configuration of the AC and DC power filter cards in slot 7 by setting the PFB Expected parameter value to AC7 or DC30 on the Shelf (Edit) form. The card object in slot 7 changes to PFAC or PFDC on the equipment tree, depending on the PFB Expected parameter setting.

See Procedure 9-7 for more information about configuring a card.

Equipment controller

Each 1830 PSS-8 shelf contains at least one active EC. A standby EC can be configured and equipped to provide controller redundancy. An1830 PSS-8 can operate normally, without alarms, with a single EC in each 1830 PSS-8 shelf. EC protection provides both automatic and user-initiated switch capability.

User panel

The User panel is an optional card that is installed in the protection EC slot in 1830 PSS-8 master shelf.

VWM-CW and VWM-DW shelves

The 1830 PSS-8 shelf supports CWDM and DWDM clip-on shelves. The 5620 SAM supports the configuration of the VWM-CW (the CWDM clip-on shelf) and the VWM-DW (the DWDM clip-on shelf). See Procedure 9-2 for more information about configuring the 1830 PSS shelves. Both CWDM and DWDM clip-on shelves are managed and powered by a USB interface on the 1830 PSS-8 EC faceplate.

A single 1830 PSS-8 EC can subtend up to three VWM-CW clip-on shelves through USB interfaces. The 5620 SAM supports the configuration of the following EC and SFC cards in the VWM-CW shelves:

- EC-CW—slot 1
- SFC4A—slot 2 and 3
- SFC4B—slot 2 and 3
- SFC8—slot 2 and 3

A partially protected 1830 PSS-8 EC can subtend up to two VWM-DW clip-on shelves through a USB interface. An unprotected 1830 PSS-8 EC can subtend up to three VWM-DW clip-on shelves through a USB interface. The 5620 SAM supports the configuration of the following EC and SFD cards in the VWM-DW shelves:

- EC-DW
- SFD2A
- SFD2B
- SFD2C
- SFD2D
- SFD2E
- SFD2F
- SFD2G
- SFD2H
- SFD2I
- SFD2L
- SFD2M
- SFD2N
- SFD2O
- SFD2P
- SFD2Q
- SFD2R
- SFD4A
- SFD4B
- SFD4C
- SFD4D
- SFD4E
- SFD4F
- SFD4G
- SFD4H
- SFD8A
- SFD8B
- SFD8C
- SFD8D

The 5620 SAM supports the association of the 1830 PSS-8 EC with the clip-on shelves. See Procedure 9-1 for more information.

Procedure 9-1 To associate an 1830 PSS-8 EC with a clip-on shelf

1. On the equipment tree, expand Network→1830 PSS-8 object→VWM-CW or VWM-DW Shelf.
2. Right-click on the EC-CW or EC-DW card and choose Properties. The Card Slot (Edit) form opens.
3. Click on the Card Specifics tab and select an EC card to associate with the clip-on shelf on the Card Details panel.
4. Configure the Clip-On Shelf ID parameter.
5. Save the changes and close the forms.

SFC and SFD cards on clip-on shelves

The SFC and SFD cards on the clip-on shelves can be used as replacement or extensions of the SFC and SFD cards on the 1830 PSS-8 shelf. The 5620 SAM supports the configuration of the SFC and SFD cards. See Procedure 9-7 for more information about configuring a card.

1830 PSS-4 shelves

The 1830 PSS-4 provides a modular platform with four universal slots that can be used for cards that support ILAs, and various FOADM and terminal configurations. The 1830 PSS-4 supports DCM shelves. The 1830 PSS-4 shelf is two RU high and can be mounted in EIA, ETSI, or WECO racks. See the *Alcatel-Lucent 1830 Photonic Service Switch 4 (PSS-4) User Guide* for more information.

1830 PSS-1 AHP shelves

The 1830 PSS-1 AHP system supports the following types of shelves: Universal and DCM.

MSH8-FSM shelf

The Mesh 8 degrees Fiber Shuffle Module is a rack mounted, 3 RU, passive shelf. All of the front plate optical connectors are Multi-Push On fiber connectors with 12 fibers. The MSH8-FSM card is used to provide fiber shuffle between degrees, to and from the multicast switch add-drop blocks, and to the expansion layer of the CDC-F configuration. The 5620 SAM supports the configuration of the MSH8-FSM shelf on the 1830 PSS-32 devices.

The MSH8-FSM card, the MPO ports, and the LC ports are automatically configured during the shelf configuration.

The 5620 SAM supports modifying and viewing the following MPO port attributes on the MSH8-FSM card:

- WSS(1-8)ADD1OUT
- WSS(1-8)DROP1IN
- WSS(1-8)ADD2OUT
- WSS(1-8)DROP2IN
- WSS1TO4AD(1-12)
- WSS5TO8AD(1-12)

The eight LC ports are dimmed and not available for configuration.

Working with shelves on the 1830 PSS

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 following information about the shelf:

- general information
- fan tray state and speed
- power supply tray statuses
- LED statuses
- card slots
- hardware environment
- timing
- statistics
- dry contacts
- faults
- port segregation
- software control module
- software bank
- cross-connects

Procedure 9-2 To configure a WDM shelf

1 On the equipment tree, expand Network→1830 PSS.

2 Right-click on the 1830 PSS device object and choose Configure Shelf. The Shelf, Configure Shelf, (Create) form opens.

3 Configure the required parameters in the Shelf Details panel.

Note — During the creation of an ITLB shelf, one ITLB card slot is automatically provisioned.

4 Save your changes and close the form.

Procedure 9-3 To configure an OCS shelf

1 On the equipment tree, expand Network→1830 PSS.

2 Right-click on an 1830 PSS device object and choose Configure Shelf. The Shelf, Configure Shelf (Create) form opens.

3 Configure the required parameters in the Shelf Details panel.

4 If the Shelf Type parameter is configured as 1830 PSS 36 Shelf in step 3, configure the Air Flow parameter, then go to step 6.

5 If the Shelf Type parameter is configured as 1830 PSS 64 Shelf in step 3, configure the required parameters:

- TRU Type
- TRU Shelf ID

Note — The TRU Shelf ID parameter can be configured as a value between 128 to 255, if the TRU Type parameter is not None.

When an 1830 PSS-64 device is configured with TRU shelf, the HPCFAP card is configured automatically under the 1830 PSS TRU Shelf on the navigation tree. See the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide* for more information about the HPCFAP card.

6 Select an Alarm Profile.

7 Configure the Matrix Size (Gbps) parameter in the Switching Capacity panel.

8 Save your changes and close the form.

Procedure 9-4 To remove a shelf

1 On the equipment tree, expand Network→1830 PSS.

2 Right-click on the shelf and choose Remove Shelf. A dialog box appears.

3 Click on View Dependencies. An Information form displays the dependencies that affect the removal of the shelf.

4 Select “I understand the implications of this action” check box and click Yes. The shelf is removed from the network object.

9.5 Managing cards

This section describes the procedures for slot and card level provisioning. The 5620 SAM GUI supports view, modify, create, and delete card level functions, and the pre-provisioning of a card in an empty slot. See Table 18-1 for transmission cards supported on the universal shelf. See Table 18-2 for dedicated cards required to boot the 1830 PSS. See the *5620 SAM Optical Parameter Reference* for more information about parameters.

Note 1 — You must use filler blanks in slots that are not used for the required airflow and cooling.

Note 2 — To provision two-slot height cards and two-slot width cards, the adjacent slots must be empty.

OCS cards

This section describes the procedures for card slot provisioning. The 5620 SAM GUI supports viewing, modifying, creating, and deleting card slot level functions, and configuring a card in an empty slot.

The following dedicated cards can be viewed on the 5620 SAM GUI for the OCS shelves:

- agnostic matrix
- first-level controller
- power supply filter
- fan unit
- bus termination card

Agnostic matrix cards

The matrix cards on the 1830 PSS-36 and 1830 PSS-64 OCS shelves can operate as a 1+1 redundant pair. One of the matrix cards is active and the other is standby. The following parameters are selected by default in the Secondary State information under the States panel of the Card Specifics tab of the card properties form:

- Working—for the active matrix card
- Standby Hot—for the standby matrix card

In the navigation tree of the 5620 SAM, two MT1T9C cards are configured by default in card slots 11 and 15 on the 1830 PSS-36 device and two MT1T9 cards in card slots 71 and 72 on the 1830 PSS-64 device.

First-level controller cards

In the navigation tree of the 5620 SAM, two FLC36EA cards are configured by default in card slots 23 and 40 on the 1830 PSS-36 device and two FLC64 cards in card slots 73 and 75 on the 1830 PSS-64 device.

Bus termination cards

In the navigation tree of the 5620 SAM, two BT36 cards are configured by default in card slots 42 and 43 on the 1830 PSS-36 device, four BT3T8 cards in card slots 81, 82, 85, and 86 on the 1830 PSS-64 device, and two BTC3T8 cards in card slots 83 and 84 on the 1830 PSS-64 device.

Power supply filter cards

In the navigation tree of the 5620 SAM, two PSFC cards are configured by default in card slots 44 and 45 on the 1830 PSS-36 device and two PSF3T8 cards in card slots 91 and 94 on the 1830 PSS-64 device.

Fan units

In the navigation tree of the 5620 SAM, one FAN3T8 card is configured by default in card slot 41 on the 1830 PSS-36 device and two FAN3T8 cards in card slots 92 and 93 on the 1830 PSS-64 device.

I/O cards

The I/O cards signal and transport varying data formats and rates across the network. The I/O cards that can be configured using the 5620 SAM on the 1830 PSS-36 and 1830 PSS-64 devices include:

- 1AN100G
- 2AN40G
- 4AN10G
- 8ET1GB
- 10AN10G
- 10AN10GC
- 10ET10G
- 10ET10GC
- 10OTH10G
- 24ANM
- 24ET1GB
- 24ET1G

The 1AN100G card can be configured on the 1830 PSS-36 or 1830 PSS-64, Release 7.0.1 or later. The 10AN10GC and 10ET10GC cards can be configured on the 1830 PSS-36 or 1830 PSS-64, Release 8.0 or later

Uplink cards

The uplink cards are used for connecting and interworking with the WDM systems. On the 1830 PSS-64, the uplink cards are configured on the lower row by default, that is, from card slot 33 to card slot 64. You can also configure the uplink cards on the upper row, that is, from card slot 1 to 16, by configuring the Environmental Conditions Restricted parameter. See Procedure 9-9 for more information about configuring uplink cards on the upper row of the 1830 PSS-64 device.

The following uplink cards are supported on the 1830 PSS-36 and 1830 PSS-64 devices:

- 11QCUP
- 11QCUPC
- 43SCUP
- 130SCUP
- 130SCUPB
- 130SCUPC

The 130SCUPC card is similar to the 130SCUP and 130SCUPB cards, but has a faster payload restructuring. The 130SCUPC can interwork with the following OTs and uplink cards in the L0 control plane:

- 112SCA1(AFEC only with asymmetric flag set)
- 112SCX10 (AFEC only with asymmetric flag set)
- 112SNA1 (AFEC only with asymmetric flag set)
- 112SNX10 (AFEC only with asymmetric flag set)
- 130SCUP,130SCUPB (SDFEC only)
- 130SCUPC (SDFEC only)
- 130SCX10 (SDFEC only)
- 130SNX10 (SDFEC only)
- 260SCX2 in 130G mode (SDFEC only)

Filter card

The SFC8 filter card can be configured in any I/O card slot on the 1830 PSS-36 and 1830 PSS-64.

For more information about the cards supported on the 1830 PSS-36 and 1830 PSS-64 devices, see the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide*.

Amplifier and associated cards

ASWG and A4WSG cards

The 5620 SAM supports viewing and modifying the ASWG and A4PWSG ports that function as unidirectional LD ports with the following additional functions:

- The EDFA module monitors both low and medium power gain ranges.
- The OTDRRX and OTDRTX ports provide connections to an OTDR card. OTDR monitoring is used for characterization of the fiber plant, and for locating fiber cuts.

The following ports are automatically configured during the card configuration:

- LINEIN
- OTDRRX
- OTDRTX
- LINEOUT
- OSCSFP
- OSC

The received optical power of the OSC is displayed for the OSCSFP port. If the OSCSFP port on the ASWG or A4PWSG card is assigned, the LINEIN port can only be connected as an external connection. The A4PWSG is a Raman amplifier with four Raman pumps unlike the AWSG card, which is not a Raman amplifier.

OTDR cards

The 5620 SAM supports configuration of the Connected LD OTDR Port parameter on OTDR P (1-8) ports. The P (1-8) ports are automatically created and deleted with the card. The OTDR card is used with the LD cards that has OTDR ports. The supported card and port types include:

- OTDRRX ports for the LD card types: A4PSWG and ASWG
- OTDRTX ports for the LD card types: A4PSWG and ASWG

AAR-8A card

The AAR-8A card is connected between the MSH8-FSM and the MCS8-16 to provide add-drop direction amplification in the CDC-F ROADM configuration. The AAR-8A card provides four drop paths and four add paths. On each path, a nominal fixed-gain EDFA optical amplifier amplifies the signal.

The 5620 SAM supports modifying and viewing the following ports:

- AAR-8A AMPIN(1-8) ports
- AAR-8A AMPOUT(1-8) ports
- AAR-8A FSM port
- AAR-8A MCS port

The 1-4 AMPIN and AMPOUT ports are used for drop amplification, and the 5-8 ports are used for add amplification. The ASE Mode parameter on the Port Specifics tab of the AMPOUT Physical Port (Edit) form can be configured to Yes to provide constant power. If you set the ASE Mode to Yes, the Operating Mode parameter is automatically set to Power. If you set the ASE Mode parameter to No, the Operating Mode parameter is automatically set to Gain. The Power Setting parameter can be configured only when the ASE Mode is set to Yes.

The FSM port connects to the AD ports on the MSH8-FSM. The MCS port connects to the MCS8-16 at the AAR1 or AAR2 port in its MCS add-drop block.

MON-OCM cards

The 5620 SAM supports MON-OCM card configuration. The MON-OCM card is used to provide signals to the WTOCMx cards and to the associated external optical monitoring device (for example, to an optical spectrum analyzer). The MON-OCM card splits the monitored DWDM optical signal from the MON port of an LD into two paths: one to the WTOCMx card for optical channel monitoring and the other to the customer monitoring equipment. The MON-OCM is configured between the WTOCMx and the amplifier cards. Supported amplifier cards include:

- AM2125A
- AM2125B
- AM2318A
- A2P2125
- AM2032A
- AM2625A
- ASWG
- A4PSWG

Optical transponder cards

MVAC cards

The 5620 SAM supports configuring the VOA Mode parameter to either Power or Attenuation on the Port Specifics→General tab of the Physical Port (Edit) form for the G1 to G8 ports on the MVAC card. When the VOA Mode parameter is configured to Power, the Attenuation (dB) parameter cannot be configured. When the VOA Mode parameter is configured to Attenuation, you can configure the Attenuation (dB) parameter from 0 to 10 dB, allowing you to increase the optical power at the receiving end of the fiber link. The default value is 0 dB.

You can also connect the supported ingress LD ports to the MVAC G ports by selecting the ports on the Connected to Port panel of the Port Specifics→General tab of the Physical Port (Edit) form.

You can configure the VOA Mode parameter when:

- there are no internal optical links to or from the port
- the port Administrative State parameter value is Down or Maintenance

You can configure the Attenuation (dB) parameter when:

- the VOA Mode parameter is set to Attenuation
- port Administrative State parameter value is Up or Maintenance

Note — When the port Administrative State parameter value changes from Up to Down or Maintenance, the configured attenuation value is retained.

When the VOA Mode parameter is set to Attenuation:

- ensure that the Pluggable Module Type parameter is configured to sVOA on the Physical Port (Edit) form
- receive power and transmit power are not applicable
- connection information attributes are not applicable
- opposite direction port is not applicable
- wave key encoder attributes are not applicable
- performance monitoring is not supported

OPSA and OPSB cards

Procedure 9-5 To configure an OPSA card

1 On the equipment tree, expand Network→NE→Shelf→Card Slot (OPSA: Enhanced Optical Protection Switch Card).

2 Right-click on the card slot and choose Properties. The Card Slot OPSA: Enhanced Optical Protection Switch Card (Edit) form opens.

3 Click on the Card Specifics tab and choose OMSP or OLP from the Protection Mode drop-down menu, as applicable.

Note — The default value for the Protection Mode parameter is OCHP.

4 Click Apply to save the changes and close the form.

Procedure 9-6 To configure an OPSB card

1 Configure the OPSB card. See Procedure 9-7 for information about configuring a card.

Note — The A, B, and SIG ports are automatically created when the OPSB card is configured.

2 Configure an optical link from either the OPSB A port or OPSB B port to the OT. See Procedure 9-18 for information about creating an optical link.

Note — The following configuration rules apply for the client ports when creating an optical link.

- Set the Assigned Rate, Transmit Frequency, Pluggable Module Type, and OPR mode to be same at the client ports of the working and protection OTs.
- Set the LOS Propagation to LASER OFF.
- Encapsulation Mode can be the same or different at the client ports of the working and protection OTs.
- Set the Transmit Frequency to either 1310 or 1550.

3 Create an APS group. See Procedure 16-29 for information about creating an APS group.

Wavelength router cards

MCS8-16 card

The MCS8-16 card is a multicast switch card used with the AAR-8A card to provide MCS add-drop blocks for the colorless, directionless, and contentionless flexible grid ROADM configuration.

The 5620 SAM supports modifying and viewing the following ports:

- MCS8-16 AD (1-16) ports
- MCS8-16 SIG (1-8) ports
- MCS8-16 AAR1 port
- MCS8-16 AAR2 port

The AD ports direct the signals to SIG ports in the add direction and receive signals from SIG ports in the drop direction. The Force Routing Add/Drop parameter on the Port Specifics→General tab of the Physical Port (Edit) form is configured to route the signal to a specific SIG port.

The SIG ports combine signals from the AD ports and direct the signals to AAR-8A cards. The SIG ports also receive signals from an AAR-8A packs and split the signals to the AD ports for selection.

The MPO ports AAR1 and AAR2 amplify signals to and from the MCS add/drop blocks.

WR20-TFM card

The WR20-TFM card is a twin 1x20 WSS flex capable card with MPO connectors.

The 5620 SAM supports modifying and viewing the following ports of the WR20-TFM card:

- SIG port
- two 1x20 wavelength selective switches in a single optical module, called twin WSS. Eight ports are used for add, drop, or through paths and the remaining 12 ports are used for add-drop paths.
    - ADT(1-8) ports
    - AD(9-20) ports

  The 20 ports are connected to the four MPO ports.
- MPO ports

  The MPO port is known as a multi-port and supports 12 positions where the underlying ports connect. Some of the positions are not used on a specific multi-port.
    - DROP1OUT
    - DROP2OUT
    - ADD1IN
    - ADD2IN

TDM cards

The 5620 SAM supports the configuration of the following TDM cards on an 1830 PSS-36 or 1830 PSS-64 device:

- 10SD10G
- 24SDM

These cards help in providing a gateway from and to SDH to OTN using VC timeslots at a device level. See chapter 12 for more information.

Procedure 9-7 To configure a card on a WDM shelf

1 On the equipment tree, expand Network→1830 PSS→Shelf.

2 Right-click on an empty Card Slot object and choose Configure Card. The Card Slot (Create) form opens.

3 Configure the required parameters on the General tab.

4 Click Apply to save the changes. The form name changes to Card Slot (Edit) form.

5 Click on the Card Specifics tab.

6 Configure the required parameters in the Card Details panel.

7 Configure the Card Rate Mode parameter for the 11DPE12 card.

8 Configure the required parameters in the Ethernet Loopback panel for the 11DPE12A cards.

9 Configure the Optical Intrusion Detection parameters for the AM2318A and AM2125B cards. An external topological link must be configured on a line port.

10 Configure the required parameters on the Temperature panel.

11 Configure the Card Mode parameter for 4DPA4, 112SCA1, 112SNA1, and 1DPP24M cards. The 1DPP24M card is configured only on the 1830 PSS-4 device.

The 1DPP24M card supports the card modes, Master and Slave. The Master mode provides 21 E1 access points and one line port (STM-1). The Master mode can support 42 E1 access points (21 E1 from Master mode and 21 E1 from Slave mode 1DPP24M). The Slave mode provides 21 E1 access points. The Line port of the Slave mode is always set to the unassigned state and is connected to the Master mode through the backplane.

12 Save your changes and close the form.

Procedure 9-8 To configure a card on an OCS shelf

Full-slot I/O cards can be configured in the following card slots:

- 2 to 9, 12, 13, and 16 to 21 on the 1830 PSS-36 device
- 1 to 16 and 33 to 48 on the 1830 PSS-64 device

The uplink cards can be configured in card slots 33 to 48 on the 1830 PSS-64. See Procedure 9-9 to configure the uplink cards in card slots 1 to 16 of the 1830 PSS-64.

The dedicated cards, such as the matrix cards, power supply filter cards, bus termination cards, fan units, and first-level controller cards are configured in the default card slots automatically when a shelf is configured.

1 On the equipment tree, expand Network→1830 PSS→Shelf.

2 Right-click on an empty Card Slot object and choose Configure Card. The Card Slot (Create) form opens.

3 Configure the required parameters on the General tab.

4 Click Apply to save the changes.

5 Click on the Card Specifics tab.

6 Configure the required parameters on the Card Details panel.

7 Click on the IO Card tab and configure the Administrative State parameter, if required.

8 To view more information about the configured card:

- Click on the Port Group tab to view the port groups. For more information about port groups, see section 9.6.
- Click on the Ports tab to view the ports on the card.
- Click on the Statistics tab to view the statistics policies associated with the card.
- Click on the Faults tab to view the alarms on the card.

9 Save your changes and close the form.

See the *ENT-EQPT State Mismatches* subsection in the *Alcatel-Lucent 1830 Photonic Service Switch TL1 Commands and Messages Guide (Switching Applications) Guide* for more information about the card slot restrictions.

Procedure 9-9 To configure uplink cards on the upper row of the 1830 PSS-64

By default, you cannot configure uplink cards on the upper row, that is, in card slots 1 to 16 of the 1830 PSS-64 device.

1 On the equipment tree, expand Network→1830 PSS-64.

2 Right-click on the 1830 PSS-64 device and choose Properties. The Network Element (Edit) form opens.

3 Click on the NE Specifics tab.

4 Select the Environmental Conditions Restricted check box.

5 Click OK to confirm and close the form.

6 On the equipment tree, expand Network→1830 PSS-64→Shelf→Card Slot. Right-click on the empty upper row card slot and choose Properties. The Card Slot (Create) form opens.

7 Perform steps 3 to 9 of Procedure 9-8 to configure the required uplink card.

See the ENT-EQPT State Mismatches subsection in the *Alcatel-Lucent 1830 Photonic Service Switch TL1 Commands and Messages Guide (Switching Applications) Guide* for more information about the card slot restrictions.

Procedure 9-10 To remove a card

1 On the equipment tree, expand Network→1830 PSS→Shelf→Card.

2 Right-click on the card object and choose Remove Card. A dialog box appears.

3 Select the "I understand the implications of this action" check box and click Yes. The card is removed from the navigation tree.

Procedure 9-11 To configure card firmware

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose Card Firmware (Physical Equipment) from the Object drop-down menu and click Search. A list of cards managed appears.

3 Choose an entry and click Properties. The Card firmware form opens.

4 Select the provisioned release for the equipped card.

5 Click Properties beside the Slot parameter. The Card Slot (Edit) form opens.

6 Click on the IO Card tab and set the Administrative State parameter to Down.

7 Click Apply to save the changes and close the Card Slot (Edit) form. The Card firmware Slot form reappears.

8 Click Apply to save the changes and close the Card firmware Slot form. The list of card reappears.

9 Choose the specific card from the list and click Reboot. After the card is rebooted successfully, the Provisioned Release parameter is updated with the firmware profile.

Procedure 9-12 To configure the card mode for the 260SCX2 card

The 260SCX2 card operates in the following modes:

- 100GbE
- OTU4

When the card is configured in 100GbE mode, the card capacity can be set to either 100GbE or 200GbE, based on the line rate. If the line rate is configured as the OTU4 rate, only the C1 client port that is set to the 100GbE rate is available. If the line rate is configured as the OTU4x2 rate, both the C1 and the C2 client ports that are set to 100GbE rates are available.

When the card is configured in OTU4 mode, the card capacity is 100GbE and the line rate is OTU4. Only the C1 client port set to the OTU4 rate is available.

Note — The following configurations are not supported on the 260SCX2 card:

- 260GbE mode with two OTU4 clients at the same time
- 260GbE mode with one OTU4 client and one 100GbE client at the same time
- 260GbE mode with one OTU4 client

To configure the card mode by assigning the rate on the line port of the 260SCX2 card, perform the procedure.

1 On the equipment tree, expand Network→1830 PSS→Shelf.

2 Configure the 260SCX2-100GEth or 260SCX2-OTU4 card on the required card slot. See Procedure 9-7.

3 Expand the card slot object to view the ports of the card.

4 Right-click on the line port and choose Properties. The Physical Port (Edit) form opens.

5 Click on the Port Specifics tab.

6 Configure the Assigned Rate parameter to one of the following, depending on the card that is configured:

- OTU4
- OTU4x2

7 Click Apply.

8 Expand the L1 line port object on the navigation tree to view the port objects.

- If the value for the Assigned Rate parameter is configured as OTU4 in step 6, the CH1-OTU4 object appears below the line port.
- If the value for the Assigned Rate parameter is configured as OTU4x2 in step 6, the CH1-OTU4 and CH2-OTU4 objects appear below the line port.

9 Change the mode of the 260SCX2 card:

- **i** On the equipment tree, expand Network→1830 PSS→Shelf→260SCX2-100GEth or 260SCX2-OTU4 card.
- **ii** Right-click on the card object and choose Properties. The Card Slot (Edit) form opens.
- **iii** Click on the Card Specifics tab and configure the Card Mode parameter.

10 Save your changes and close the form.

Dry contacts

A dry contact is a contact of a relay that does not make or break a current. Usually another relay or device starts or stops the current. For example, a reed relay matrix switch is usually switched with all contacts dry. After the contacts are connected, a wire spring relay connects a supervisory scan point through which the current flows.

Procedure 9-13 To configure 1830 PSS dry contact sensors

1 On the equipment tree, expand Network→NE→Shelf→Card Slot (USRPNL - User Interface Panel)

2 Right-click on the card slot and choose Properties. The Card Slot (User Interface Panel) (Edit) form opens.

3 Click on the External Control tab. The dry contacts are listed.

4 Choose an entry and click Properties. The DryContact (Edit) form opens.

5 Configure the required parameters.

6 Click Apply to save the changes and close the form.

9.6 Managing ports

The 5620 SAM supports a physical topology view that allows you to create a fiber connection by selecting two ports on the displayed shelves. The connection can be between two ports on the same shelf or different shelves.

Note — You can create a fiber connection only with ports that are not already part of a fiber connection.

For an interface (that is, a shelf, slot, or port), you can specify that the interface is:

- connected to another interface on the network element
- connected to an external interface within or outside of the 1830 PSS network
- unconnected

To define the network topology, you first configure the fiber topology on each network element in the network. You can then connect the external interfaces on each of the network elements to create the network.

OCS ports

The 5620 SAM supports the following for a port on 1830 PSS-36 and 1830 PSS-64 devices:

- configure port group
- configure the pluggable module type
- assign a rate
- configure TCA and alarm profiles
- view ODUk cross-connects, optical transport services, and APG groups associated with a port

Port groups

Port groups are automatically configured when cards are configured on the OCS shelves, with PWRSV or UNIVTRM as the default port group mode. Each port group is identified by the first port in the group, and each group has a specific mode that is mapped to a specific signal type.

The value of the port group mode must be changed before any port in the group is configured. The mapping of port group modes to signal types is as follows:

- OTH—OTU2, OTU2e, OTU3, OTU3e2, and OTU4
- ETHSTH—10GbE LAN, STM64, and STM256
- STH—STM1, STM4, STM16, and STM64
- UNIVTRM—100 GbE LAN and OTU4
- PWRSV—power save mode does not have a rate associated with it. It is used to change the port mode, if required.

Table 9-2 lists the cards and the corresponding port groups.

Table 9-2 Port groups

Card name	Port group modes	Port group ID	Ports in the group
1AN100G	UNIVTRM	1	1
2AN40G	ETHSTH OTH PWRSV	1	1
		2	1

(1 of 3)

Card name	Port group modes	Port group ID	Ports in the group
4AN10G	ETHSTH OTH PWRSV	1	1, 2
		3	3, 4
8ET1GB	ETHSTH PWRSV	1	1 to 8
10AN10G	ETHSTH OTH PWRSV	1	1, 2
		3	3, 4
		5	5, 6
		7	7, 8
		9	9, 10
10ET10G	ETHSTH PWRSV	1	1, 2
		3	3, 4
		5	5, 6
		7	7, 8
		9	9, 10
10OTH10G	ETHSTH OTH PWRSV	1	1, 2
		3	3, 4
		5	5, 6
		7	7, 8
		9	9, 10
10SD10G	STH PWRSV	1	1,2
		3	3,4
		5	5,6
		7	7,8
		9	9,10
11QCUP	OTH PWRSV	1	1, 2
		3	3, 4
11QCUPC	OTH PWRSV	1	1, 2
		3	3, 4
24ANM	ETHSTH PWRSV STH	1	1 to 8
		9	9 to 16
		17	17 to 24
24ET1GB	ETHSTH PWRSV	1	1 to 8
		9	9 to 16
		17	17 to 24
24ET1G	ETHSTH PWRSV	1	1 to 8
		9	9 to 16
		17	17 to 24

(2 of 3)

Card name	Port group modes	Port group ID	Ports in the group
24SDM	STH PWRSV	1	1 to 8
		9	9 to 16
		17	17 to 24
43SCUP	OTH PWRSV	1	1
130SCUP	OTH	1	1
130SCUPB	OTH	1	1
130SCUPC	OTH	1	1

(3 of 3)

LAN ports

LAN ports are used for management network connections and debug purposes. The 1830 PSS OCS devices have the following LAN ports:

- CIT port on the FLC card
- OAMP port on the FLC card
- ES1 and ES2 ports on the matrix cards

See the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide* for more information about external communication through LAN port interfaces.

Procedure 9-14 To configure a port on a WDM device

1 On the equipment tree, expand Network→NE→Shelf→Card→Port.

2 Right-click on the port object and choose Properties. The Physical Port (Edit) form opens.

3 Configure the required parameters on the General and Port Specifics tabs. Configure the Transmit Frequency parameter as required in the OT panel. Ensure that the administrative state of the port is down before configuring the transmit frequency.

Note — If the transmit frequencies are already configured on the ports, the Receive Frequency parameter is updated automatically, when a bidirectional service is created between two devices.

4 Click on the States tab and configure the Administrative State parameter.

5 Save your changes and close the form.

Procedure 9-15 To configure a port on an OCS device

1 On the equipment tree, expand Network→1830 PSS→Shelf→Card→Port.

2 Right-click on the port you want to configure, and choose Properties. The Physical Port (Edit) form opens.

3 Click on the Port Specifics tab.

4 Click Properties beside the Port Group Mode parameter. The Port Group (Edit) form opens.

5 Configure the Mode parameter as required.

6 Save your changes and close the form.

7 Configure the required parameters in the Physical Port (Edit) form.

Note 1 — The Assigned Rate parameter can only be configured after configuring the Pluggable Module Type parameter.

Note 2 — The Pluggable Module Type parameter is not applicable for uplink cards.

8 Click on the States tab and configure the Administrative State parameter, if required.

9 Save your changes and close the form.

Procedure 9-16 To enable interworking between different generations of coherent 100G OTU4 cards

Perform the following procedure to enable interworking between second-generation 100G OTU4 cards such as the 130SCA1, 130SCX10 and legacy 100G OTU4 cards such as the 112SCX10 and 112SNX10 cards. You can create an optical trail or service between these cards only when the second-generation cards are in the AFEC mode and asymmetric interworking is enabled on all the cards.

1 On the equipment tree, expand to the required line port level of the 130SCA1 or 130SCX10 card.

2 Right-click on the line port and choose Properties. The Physical Port (Edit) form opens.

3 Click on the Port Specifics tab.

4 Configure the FEC Mode parameter as AFEC.

Note — By default, the value of the FEC Mode parameter is AFEC for the legacy 100G cards, such as 112SX10 and 112SNX10.

5 Select the Asymmetric Interworking Enabled check box.

6 Save your changes and close the form.

Procedure 9-17 To auto-disable a CIT port on an EC card

The CIT port can be set to auto-disabled after the 1830 PSS is installed. See the *Alcatel-Lucent 1830 Photonic Service Switch User Provisioning Guide* for more information.

1 On the equipment tree, expand Network→NE→Shelf→Card Slot (EC: Equipment Controller Card)→Port CIT (Local Ethernet Port).

2 Right-click on the CIT port and choose Properties. The Physical Port (Edit) form opens.

3 Click on the Port Specifics tab.

4 Configure the 5620 SAM server IP in the Source IP field in the Auto-Disable port Status panel and click Apply. The Disable Port Automatically check box is enabled.

5 Save your changes and close the form.

Note — As long as the 1830 PSS can reach the 5620 SAM server, the CIT port remains in the disabled state. The 1830 PSS checks the communication link between the 5620 SAM server every 30 s. If the server is unreachable, the NE waits for 300 s before the CIT port is enabled for local access.

9.7 Managing optical links

WDM topological links

The 5620 SAM supports configuration of the following topological links for WDM devices:

- bidirectional internal topological link
- bidirectional external topological link
- unidirectional internal topological link
- unidirectional external topological link

See Procedure 9-18 for more information about configuring WDM topological links.

OCS topological links

The 5620 SAM supports configuration of the following topological links for OCS devices:

- bidirectional internal topological link
- bidirectional external topological link
- bidirectional compound topological link

See Procedure 9-21 for more information about configuring an OCS topological link.

Bidirectional internal topological link

The bidirectional internal topological link is configured between the ports within an OCS device. The ports that are not already part of an optical link are available for creating a new link. The link is configured between two ports on the same shelf or on different shelves.

Note — Unidirectional internal topological links are not supported in the 5620 SAM for OCS devices.

Bidirectional external topological link

The bidirectional external topological link is configured from a port within an OCS device to a port in another OCS or WDM device. The ports that are not already part of an optical link are available for creating a new link.

Inter-compound topological link

The inter-compound topological link is configured from an OCH port of the WDM device to a port in an OCS uplink card.

Note — Inter-compound topological links are always bidirectional.

The OCS and WDM devices interwork as partners where the OCS uplink ports and optical channels are integrated into the WDM domain using virtual OCONNs and PXCs. The WDM-OCS partner pairing is configured in the 5620 SAM as follows:

- On the OCS device—configure the Partner NE parameter, that is, the IP address of the participating WDM device, before configuring the inter-compound topological link. The parameter can be viewed on the NE Specifics tab of the Network Element (Edit) form.
- On the WDM device—configure the OCS IP parameter, that is, the IP address of the participating OCS device, before configuring the inter-compound topological link. The parameter can be viewed on the NE Specifics tab of the Network Element (Edit) form.

The 5620 SAM automatically creates a compound node object named Compound_OCS node name on the navigation tree and on the physical topology map after the WDM-OCS partner pair is configured. The characteristics of the compound node object are:

- created automatically after WDM-OCS partner pair configuration
- consists of the participating OCS and WDM nodes
- only the compound node object can have the prefix Compound_. The 5620 SAM does not allow the configuration of a new group in the equipment view of the navigation tree and on the appropriate topology maps with the object name prefixed by Compound_.
- you cannot delete the compound node object and it is automatically deleted when the WDM-OCS partner pairing is de-provisioned or modified
- you cannot move the elements out of the compound node object or add elements into the compound node object

The WDM-OCS partner pairing is de-provisioned by deleting the inter-compound topological link and configuring the Partner NE and OCS IP parameters with the value 0.0.0.0 or any other IP address. The WDM-OCS partner pairing can also be configured using the WebUI. See the *Alcatel-Lucent Photonic Service Switch User Provisioning Guide* for more information about connecting an OCS application to WDM application from the WebUI.

Note — Ensure that the inter-compound topological link is deleted before modifying the partner IP from the node.

The UCM is the WDM module responsible for WDM to OCS communication, and for integrating OCS uplink data into the WDM system. The WDM UCM interface supports the following OCS uplink cards:

- 11QCUP
- 11QCUPC
- 43SCUP
- 130SCUP
- 130SCUPB
- 130SCUPC

Table 9-3 lists the cards and ports that support inter-compound topological links between a WDM compound and an OCS uplink card. See Procedure 9-21 for more information about configuring OCS topological links.

Table 9-3 Supported cards and ports

Card type	Ports
CWR8	CLS 1 to 8
CWR8-88	CLS 1 to 8
OPSA	SIG
PSC1-6	A to E (1 to 6)
SFD5x	channel ports
SFD8x	channel ports

(1 of 2)

Card type	Ports
SFD40	channel ports
SFD40B	channel ports
SFD44	channel ports
SFD44B	channel ports

(2 of 2)

The cross-connect provisioned for the configuration terminates on the SFD or CWR port, because the uplink card is not managed by the WDM device.

1830 PSS and generic NE optical links

The 5620 SAM supports establishing an optical link between an 1830 PSS WDM or OCS device and a non-Alcatel-Lucent transport device or generic NE. See Procedure 9-22 for more information about how to configure an optical link between an 1830 PSS device and a generic NE.

Procedure 9-18 To configure an optical link between ports

1 Perform one of the following to create an optical link between two ports on the same shelf:

a From the 5620 SAM main menu.

i Choose Create→OTN→Optical Link (OTS/OS) from the 5620 SAM main menu. The Optical Link (Create) form opens.

ii Configure the Endpoint A Type or Endpoint B Type parameters as Unmanaged NE, if required.

b On the equipment tree, expand Network→NE→Shelf→Card.

i Choose two ports, one from each device.

ii Right-click on the selected ports and choose Create Optical Link. The Optical Link (Create) form opens.

Note — When you choose two ports from the equipment tree, the port properties are automatically populated for endpoint A and B.

2 Perform the following steps if the value of Endpoint A Type and Endpoint B Type parameters are configured to Port:

i Select a port in the Endpoint A - Port panel.

ii If a rate is not assigned to the endpoint A port, click Properties on the Endpoint A - Port panel. The Physical Port (Edit) form opens.

iii Click on the Port Specifics→General tab and configure the Assigned Rate parameter.

iv Perform steps i to iii for Endpoint B - Port panel.

3 Perform one of the following if either Endpoint A Type or Endpoint B Type parameter is configured to Unmanaged NE:

a Configure Unmanaged NE Identifier in the Endpoint A - UnManaged NE panel.

b Configure Unmanaged NE Identifier in the Endpoint B - UnManaged NE panel.

Note — The Unmanaged NE Identifier parameter can be configured as **Site ID Shelf/Slot/Port** or **Site Name Shelf/Slot/Port**. For example, 123.45.56.78 1/2/3 or SiteA 1/2/3.

4 Save your changes and close the form.

Note — You can set the transmit frequency on the ports, even after you create an optical link, if the administrative state of the port is down. See Procedure 9-14 for more information.

Procedure 9-19 To delete an optical link

1 Perform one of the following to list the optical links:

a List the optical links to be deleted from the 5620 SAM main menu:

i Choose Manage→Equipment→Equipment. The Manage Equipment form opens.

ii Choose Optical Link (Optical Management) from the object type drop-down menu.

iii Go to Step 2.

b Double-click on an optical link in the Physical Topology - Network view. The Physical Link Group List form opens

2 Choose the optical link to be deleted and click Delete.

3 Close the form.

Procedure 9-20 To view an invalid or stale optical link

1 Double-click on the optical link that links to the Unmanaged NEs icon on the Physical Topology map. The Physical Link Group List form opens with a list of invalid or stale optical link; for example, optical links from a managed NE to an Unmanaged NE in the 5620 SAM

2 Choose an invalid or stale optical link and click Properties. The Optical Link (Edit) form opens. Information about the Managed and Unmanaged NE is displayed. The Unmanaged NE Identifier parameter displays the link that leads to the unmanaged NE.

Procedure 9-21 To configure an OCS topological link

Ensure that the following parameters are configured before configuring the inter-compound topological link:

- the Partner NE parameter, that is, the IP address of the participating WDM device, is configured on the NE Specifics tab of the Network Element (Edit) form of the OCS compound
- the OCS IP parameter, that is, the IP address of the participating OCS device, is configured on the NE Specifics tab of the Network Element (Edit) form of the WDM compound

1 Perform one of the following:

a From the 5620 SAM main menu:

i Choose Create→OTN→Optical Link (OTS/OS). The Optical Link (Create) form opens.

ii Configure the required parameters.

iii Select a port in the Endpoint A - Port panel.

iv If a rate is not assigned to the endpoint A port, click Properties on the Endpoint A - Port panel. The Physical Port (Edit) form opens.

v Click on the Port Specifics→General tab and configure the Assigned Rate parameter.

vi Perform steps i to v for the Endpoint B - Port panel.

b From the equipment tree:

i Choose a port and press CTRL to choose the second port. The two participating ports are selected.

ii Right-click and choose Create Optical Link. The Optical Link (Create) form opens with the parameters automatically populated.

2 Save your changes and close the form.

The Notes Parameter on the Optical Link (Edit) form displays the type of topological link.

The inter-compound topological link configuration results in the creation of a compound node object named as Compound_OCS node name, on the equipment tree and consists of the participating WMD and OCS device objects.

Procedure 9-22 To create a physical link between an 1830 PSS device and a GNE

1 Right-click on the Physical Topology map and choose Equipment→Create Optical Link. The Optical Link (Create) form opens.

2 Configure the required parameters.

3 Configure the Endpoint A Type parameter as Port.

4 Configure the Endpoint B Type parameter as Generic NE Interface.

5 Select a port in the Endpoint A - Port panel.

6 Select a GNE in the Endpoint B - Generic NE Interface panel.

7 Save your changes and close the form.

9.8 Managing LAGs

Link aggregation aggregates one or more links to form a Link Aggregation Group (LAG), such that a MAC client can consider the LAG as if it were a single link. The 5620 SAM supports LAG through LACP on the following supported ports and cards, where all the member ports have the same signal rate.

Table 9-4 Supported cards and ports

Card	Ports
11DPE12A	C(1-12)
11OPE8	X(1-6), C(1-2), M(1-4)
11QCE12X	X(1-4), C(1-12), M(1-4)
11QPE24	X(1-4), C(1-22)

LAGs are used for link protection of Ethernet services on UNIs, specifically with a signal rate of 10 GbE. The LAGs can also be used as a form of linear protection for NNI ports. A maximum of four ports can be aggregated to form one LAG.

Procedure 9-23 To configure LAG on 11OPE8, 11QCE12X, and 11QPE24 cards

1 On the equipment tree, expand Network→NE→Shelf→Card Slot→LAGs.

2 Right-click on the LAGs object and choose Create LAG. The Create LAG step form appears.

3 Configure the required parameters:

- LAG ID
- Auto Assign ID
- Description
- Configured Address
- L2Uplink
- Encap Type
- Administrative State

4 Select a split horizon group, if required. See Procedure 15-2 for more information about configuring a split horizon group

5 Click Next. The Configure LAG Parameters step appears.

6 Configure the Port Threshold parameter.

7 Click Next. The Configure LACP step appears.

8 Configure the required parameters:

- LACP Enabled
- LACP Transmit Interval
- LACP Transmit Standby
- Hold Time Down (100s of milliseconds)

9 Configure the required parameters in the Selection Criteria panel:

- Active Sub-Group Selection Criteria
- Slave to Partner

10 Click Next. The Configure LAG Members step appears.

11 Click Create to add client ports to the LAG. The Create LAG Member step form with the Only show compatible ports step appears.

12 Configure the required parameters:

- Show only Compatible Ports
- Class

13 Click Next. The Select Ports step appears with the list of ports.

Note — If you configure the Show only Compatible Ports and Class parameters in step 12, only the ports that are compatible with the selected class appear in the Select Ports form. Only those LAGs with compatible ports can be used during service configuration.

14 Choose the compatible ports from the list and click Next. The Specify the Member Properties step appears.

15 Configure the required parameters:

- Priority
- Sub-Group ID

16 Click Finish. A list of the selected ports appears in the Configure LAG members step of the Create LAG step form.

The Specify Member Properties form closes and the Configure LAG Members form reappears. A dialog box appears.

17 Click OK.

18 Click Finish. The Configure LAG Members form closes and the Create LAG form reappears.

19 Click Close.

20 On the equipment tree, expand Network→NE→Shelf→Card Slot→LAGs→LAG. Right-click on the created LAG object and choose Properties to view information about the created LAG or to modify LAG parameters.

- The General tab displays the LAG ID, description, and the configured MAC address.
- The Link Aggregation Group tab displays the parameters selected during LAG creation, Number of selected ports, Number of attached ports, and size.
- The States tab displays the administrative state, which is the LAG enabled or disabled state on the node.
- The LACP tab displays the LACP parameters, such as LACP mode, Actor Administration Key, Actor Operational Key, Partner Operational Key, Actor System ID, Partner System ID, Actor System Priority, and Partner System Priority.
- The LAG Members tab allows you to add the LAG member ports.
- Statistics, terminations, and fault information is available from the appropriate tabs.

21 Expand the LAG object in the equipment tree to view the created LAG and the LAG members.

Procedure 9-24 To create a LAG on an 11DPE12A card

1 On the equipment tree, expand Network→NE→Shelf→Card Slot→LAGs.

2 Right-click on the LAGs object and choose Create LAG. The Create LAG step form appears.

3 Configure the required parameters:

- LAG ID
- Auto Assign ID
- Description
- Administrative State
- MTU (bytes)

4 Click Next. The Configure LAG Parameters step appears.

5 Configure the required parameters:

- Size
- SVLAN Tag Protocol ID
- LOS Propagation
- LPT Consequent Action

6 Click Next. The Configure LACP step appears.

7 Configure the required parameters:

- Actor Administration Key
- Actor System Priority

8 Click Next. The Configure LAG Members step appears.

9 Click Create to add client ports to the LAG. The Create LAG Member step form with Select Ports step appears.

10 Choose the ports from the list and click Next. The Specify the Member Properties step appears.

11 Configure the required parameters:

- Priority
- Admin State

12 Click Finish. A list of the selected ports appears in the Configure LAG members panel of the Create LAG step form.

The Specify Member Properties form closes and the Configure LAG Members form reappears. A dialog box appears.

13 Click OK.

14 Click Finish. The Configure LAG Members form closes and the Create LAG form reappears.

15 Click Close.

16 Choose Network→NE→Shelf→Card Slot→LAGs→LAG. Right-click on the newly created LAG and choose Properties to view information about the created LAG or to modify LAG parameters.

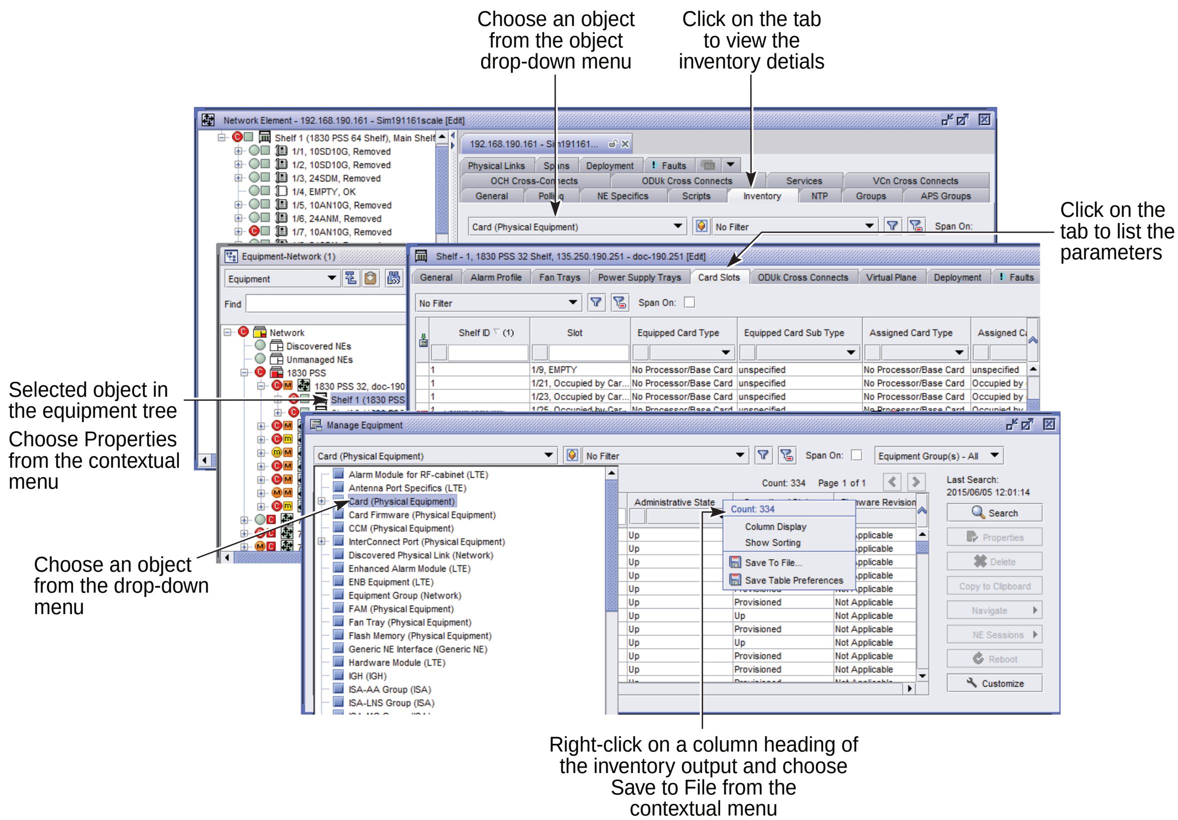
- The General tab displays the LAG ID, description, and the configured MAC address.
- The Link Aggregation Group tab displays the parameters selected during LAG creation, including Number of selected ports, Number of attached ports, size, SVLAN Protocol ID, LOS propagation, LPT Consequent action and Bandwidth Attributes.
- The States tab displays the administrative state, which is the LAG enabled or disabled state on the node.
- The LACP tab displays the LACP parameters such as LACP mode, Actor Administration Key, Actor Operational Key, Partner Operational Key, Actor System ID, Partner System ID, Actor System Priority and Partner System Priority.
- The LAG Members tab allows you to add the LAG member ports.
- The VTS map tab displays the VTS map parameters such as VTS Map Number, VTS Direction, Classification Mode, CE-VLAN ID, and SVLAN ID.
- Statistics, terminations, and fault information is available from the appropriate tabs.

17 Expand the LAG object in the equipment tree to display the created LAG and LAG members.

9.9 Managing inventory

You can use a 5620 SAM GUI to inventory the managed network equipment. The inventory information is available to GUI clients on equipment list, properties, and management forms. For information about performing inventory management, see the *5620 SAM User Guide*.

Figure 9-1 Inventory data



9.10 Managing ROADM OADM and mesh connections (degree 2+)

The ROADM OADM (degree 2) faces the east and west directions. Some traffic from the optical lines may be added or dropped and at least one single wavelength passes through transparently. The configuration can be used as an optical add or drop multiplexer in linear networks.

The WR8-88A supports up to degree 5 mesh connections without the need for additional mesh cards. For the connectivity, the mesh output port (MESHOUT(1-3)) of a WR8-88A card is connected directly to the add input port (ADDIN(1-8)) of another WR8-88A. Three mesh outputs are required for degree 5 connectivity. See Table 9-5 for more information.

The ROADM OADM mesh (degree 3 to 8) faces more than two line directions. Individual channels enter from one line and may be added or dropped or transit transparently to any one of the other lines.

Note — If the 1830 PSS-32 network contains WR8-88A and CWR cards, use the Exclusion option in the Path Constraints tab to accelerate the path search and transport service creation. See Procedure 16-1 for more information.

See the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide* for more information.

Table 9-5 ROADM-2 Degree 8 ROADM connectivity

From port	To port	From	To
WR1 DROPOUT	–	–	ITLU+SFD
WR1 THRU Out	–	–	WR2 THRU In
WR1 MESHOUT1	–	–	WR3 ADDIN3
WR1 MESHOUT2	–	–	WR4 ADDIN3
WR1 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT1	WR5 ADDIN3
WR1 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT2	WR6 ADDIN3
WR1 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT3	WR7 ADDIN3
WR1 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT4	WR8 ADDIN3
WR2 DROPOUT	–	–	ITLU+SFD
WR2 THRU Out	–	–	WR1 THRU In
WR2 MESHOUT1	–	–	WR3 ADDIN4
WR2 MESHOUT2	–	–	WR4 ADDIN4
WR2 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT1	WR5 ADDIN4
WR2 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT2	WR6 ADDIN4
WR2 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT3	WR7 ADDIN4
WR2 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT4	WR8 ADDIN4
WR3 DROPOUT	–	–	ITLU+SFD
WR3 THRU Out	–	–	WR4 THRU In
WR3 MESHOUT1	–	–	WR1 ADDIN3
WR3 MESHOUT2	–	–	WR2 ADDIN3
WR3 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT1	WR5 ADDIN5
WR3 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT2	WR6 ADDIN5
WR3 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT3	WR7 ADDIN5
WR3 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT4	WR8 ADDIN5
WR4 DROPOUT	–	–	ITLU+SFD
WR4 THRU Out	–	–	WR3 THRU In
WR4 MESHOUT1	–	–	WR1 ADDIN4
WR4 MESHOUT2	–	–	WR2 ADDIN4
WR4 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT1	WR5 ADDIN6
WR4 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT2	WR6 ADDIN6
WR4 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT3	WR7 ADDIN6
WR4 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT4	WR8 ADDIN6
WR5 DROPOUT	–	–	ITLU+SFD

(1 of 2)

From port	To port	From	To
WR5 THRU Out	–	–	WR6 THRU In
WR5 MESHOUT1	–	–	WR1 ADDIN5
WR5 MESHOUT2	–	–	WR2 ADDIN5
WR5 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT1	WR3 ADDIN5
WR5 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT2	WR4 ADDIN5
WR5 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT3	WR7 ADDIN7
WR5 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT4	WR8 ADDIN7
WR6 DROPOUT	–	–	ITLU+SFD
WR6 THRU Out	–	–	WR5 THRU In
WR6 MESHOUT1	–	–	WR1 ADDIN6
WR6 MESHOUT2	–	–	WR2 ADDIN6
WR6 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT1	WR3 ADDIN6
WR6 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT2	WR4 ADDIN6
WR6 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT3	WR7 ADDIN8
WR6 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT4	WR8 ADDIN8
WR7 DROPOUT	–	–	ITLU+SFD
WR7 THRU Out	–	–	WR8 THRU In
WR7 MESHOUT1	–	–	WR1 ADDIN7
WR7 MESHOUT2	–	–	WR2 ADDIN7
WR7 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT1	WR3 ADDIN7
WR7 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT2	WR4 ADDIN7
WR7 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT3	WR5 ADDIN7
WR7 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT4	WR6 ADDIN7
WR8 DROPOUT	–	–	ITLU+SFD
WR8 THRU Out	–	–	WR7 THRU In
WR8 MESHOUT1	–	–	WR1 ADDIN8
WR8 MESHOUT2	–	–	WR2 ADDIN8
WR8 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT1	WR3 ADDIN8
WR8 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT2	WR4 ADDIN8
WR8 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT3	WR5 ADDIN8
WR8 MESHOUT3	MESH4 SIGIN	MESH4 SIGOUT4	WR6 ADDIN8

(2 of 2)

9.11 Managing One-device Anydirection and Two-device Anydirection configuration connections

You can manage the following configuration connections:

- One-device Anydirection
- Two device Anydirection

Note — Service provisioning, discovery and topological views are supported for protected and unprotected services for One-device Anydirection and Two-device Anydirection configurations. See Procedure 16-1 for more information.

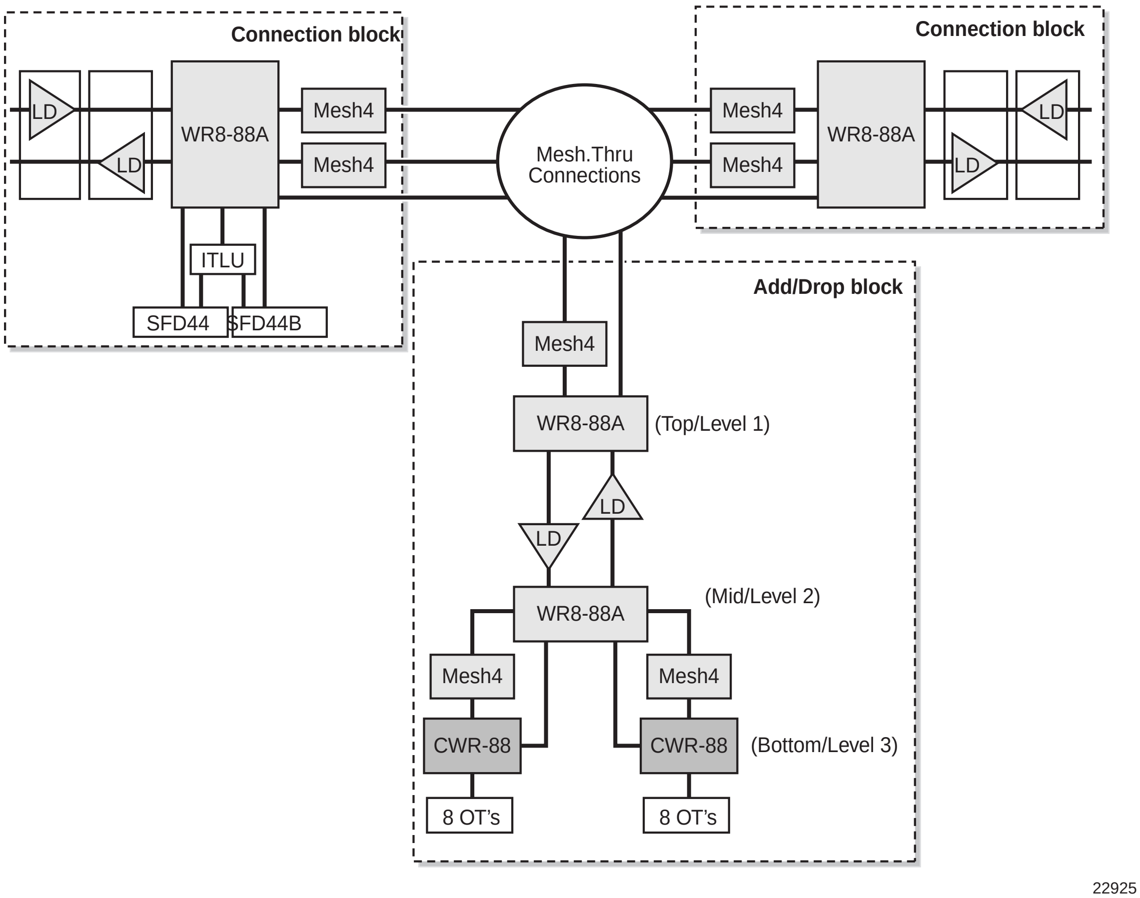
One-device Anydirection configuration

For one-device anydirection configuration, the Add drop block and the connection block are on the same device. The configuration that can be used is the Mesh card (optional) with WR8, WR8-88A and CWR8-88 cards.

Two-device Anydirection configuration

Two-device Anydirection configuration is supported on two devices for Add and Drop blocks at the terminal on one device and connection blocks on the other device. The following configurations are supported in the Add and Drop blocks and the connection blocks. Figure 9-2 shows the Two-device Anydirection configuration.

Figure 9-2 Two-device Anydirection connectivity



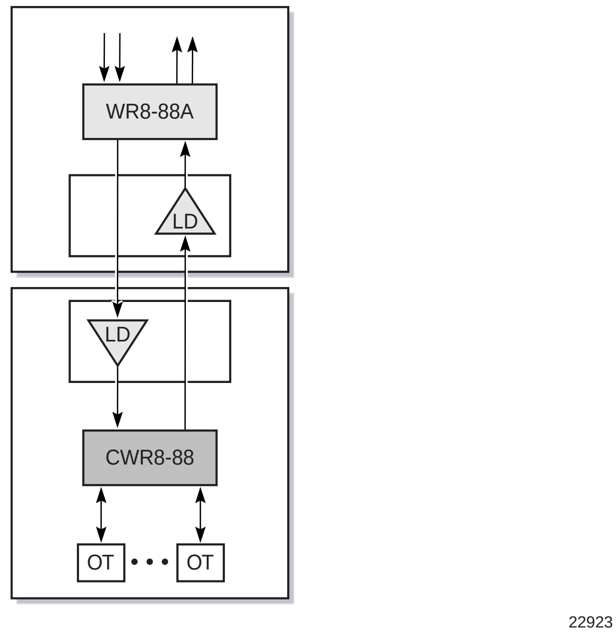
Note — Regeneration is possible inside the Add and Drop blocks.

Two devices with no MESH4 card in Add path

Figure 9-3 shows two devices with no MESH4 card in Add path. With this configuration, the limitations in degrees are:

- N<=5 with configuration not allowing in–service upgrade to higher degrees
- N<=4 with configuration allowing in–service upgrade to higher degrees

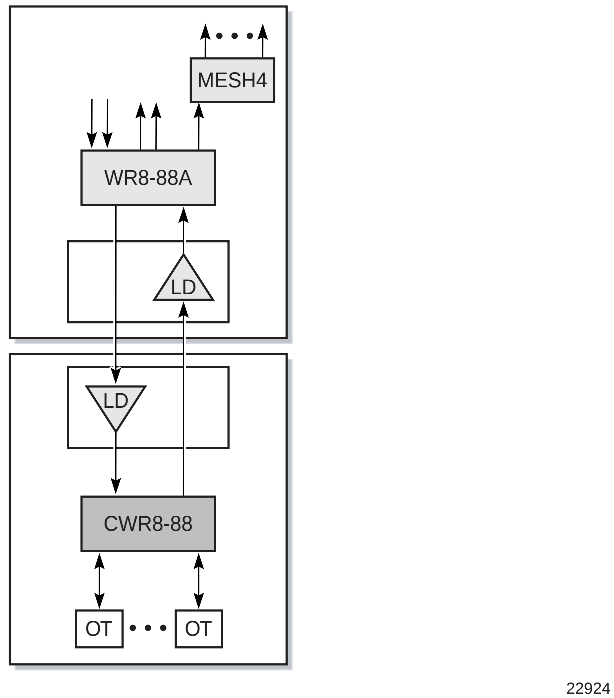
Figure 9-3 Two devices with no MESH4 card support



Two devices with one MESH4 card in Add path

The Add and Drop block allows a configuration up to degree 8+2 as shown in Figure 9-4.

Figure 9-4 Two devices with one MESH4 card support



9.12 Managing an NTP server

The 5620 SAM provides a list of NTP servers configured on the 1830 PSS. The NTP servers are used for time of day synchronization when the NTP is enabled. The 5620 SAM supports the creation and deletion of an NTP server. Up to three NTP servers are supported on the 1830 PSS.

Procedures to manage an NTP server

Procedure 9-25 To configure an NTP server

1 On the equipment tree, expand Network→1830 PSS.

2 Right-click on the 1830 PSS device object and choose Properties. The Network Element (Edit) form opens.

3 Click on the NTP tab and on the Server sub-tab.

4 Click Create. The NTP Server (Create) form opens.

5 Configure the required parameters and click OK.

> **Note —** The options for the Index parameter are 1, 2, and 3. The value represents the number of NTP servers that can be added.

6 Click on the General tab and select the NTP Enabled check box for WDM devices.

> **Note —** There must be at least one NTP server added to select the NTP Enabled check box.

7 To request the WDM devices to authenticate NTP packets arriving from an NTP server:

- **i** Click on the Authentication tab and click Create.
- **ii** Configure the required parameters.
- **iii** Click OK.

8 Save your changes and close the form.

Procedure 9-26 To delete an NTP server

1 On the equipment tree, expand Network→1830 PSS.

2 Right-click on an 1830 PSS and choose Properties. The Network Element (Edit) form opens.

3 Click on the NTP tab and on the Server tab. The configured NTP servers are listed.

4 Choose the NTP server to be deleted and click Delete.

> **Note —** If all of the NTP servers are deleted, the NTP Enabled check box in the General tab is automatically deselected, which means the NTP is automatically disabled.

5 Close the form.

9.13 Precision time protocol

PTP is used to distribute time of day and a common epoch or frequency. PTP maintains synchronization between master and slave clocks, distributes the time to slaves using multicast.

The 5620 SAM supports IEEE 1588 PTP clocks for packet-based timing synchronization from a master clock to one or more slave clocks in a network. You can configure IEEE 1588 PTP clocks on the 1830 PSS device with an ordinary master, an ordinary slave, or a boundary clock.

The following cards support PTP on the 1830 PSS:

- PTPCTL, which implements the physical layer clock (syncE) to distribute frequency and the PTP clock to distribute time or phase across the network
- PTPIO, which provides adaptation for transport of PTP over WDM links
- IEEE 1588 PTP-capable OTs (currently only 11DPE12A)

Procedures to manage PTP

Procedure 9-27 To configure TOD on the PTPCTL cards

1. On the equipment tree, expand Network→1830 PSS→Shelf→PTPCTL→TOD port.
2. Right-click on the TOD port and choose Properties. The Physical Port (Edit) form opens.
3. Click on the Port Specifics tab configure the required parameters in the TOD Attributes panel.
4. Save your changes and close the form.

Procedure 9-28 To configure an IEEE 1588 PTP clock

1. On the equipment tree, expand Network→1830 PSS→Shelf→PTPCTL or 11DPE12A card.
2. Right-click on the card object and choose Properties. The Card Slot (Edit) form opens.
3. Click on the PTP tab. The General tab appears.
4. Configure the required parameters and click OK to save the changes.
5. Click on the Clock tab, choose an entry, and click Properties. The IEEE 1588 PTP Clock (Edit) form opens.

Note — A PTP clock is automatically created when the Clock Mode is changed from PTP Disabled to any other mode.

6. Configure the required parameters in the General tab.
7. Click on the Port tab and click Create. The IEEE 1588 PTP Port (Create) form opens.

8 Select an associated physical port.

9 Select a PTP IO timing port.

> **Note 1 —** For an 11DPE12A card, if the Clock Mode is Ordinary Clock – Master or Ordinary Clock – Slave, only one PTP port can be configured. If the Clock Mode is Boundary Clock, up to 14 PTP ports can be configured.
>
> **Note 2 —** For a PTPCTL card, if the Clock Mode is Boundary Clock, up to 6 PTP ports can be created.

10 Configure the Associated VLAN ID parameter.

11 Save your changes and close the forms.

9.14 BITS

The BITS input and output ports provide external input and output station clock interfaces.

WDM BITS

The 5620 SAM provides BITS input and output ports on the PTPCTL and 11DPE12A cards. The BITS ports are automatically created and deleted with the card. See Procedure 9-29 for more information about configuring the BITS attributes.

Procedure 9-29 To configure BITS attributes on an 1830 PSS WDM device

1 On the equipment tree, expand Network→1830 PSS→Shelf→PTPCTL or 11DPE12A card→ BITS1 or BITS2 port.

2 Right-click on the BITS1 or BITS2 port object and choose Properties. The Physical Port (Edit) form opens.

3 Click on the Port Specifics tab and configure the required parameters in the BITS Attributes panel.

The Signal Type parameter is configured to 2 MHz for the PTPCTL card and cannot be configured if the SONET/SDH Mode parameter is configured to SONET on the 1830 PSS device. For the 11DPE12A card, if the SONET/SDH Mode parameter is configured to SONET on the 1830 PSS device, the Signal Type parameter can be configured as DS1 SF or DS1 ESF.

If the SONET/SDH Mode parameter is configured to SDH on the 1830 PSS device, the Signal Type parameter can be configured as follows for the PTPCTL and the 11DPE12A cards:

- 2 MHz
- Unframed E1
- Framed E1
- Framed E1 with SSM

The Line Impedance parameter can be configured as 75 ohms or 120 ohms for the PTPCTL card in SONET or SDH mode.

For the 11DPE12A card, the Line Impedance parameter is configured to 100 ohms and cannot be configured in SONET mode. The parameter can be configured as 75 ohms or 120 ohms in SDH mode.

The SA Bit parameter can be configured when the Signal Type parameter is configured to Framed E1 with SSM in SDH mode.

The Transmitted SSM and AIS Mode parameters can be configured on the BITS1 port of the PTPCTL card when the Signal Type parameter is set to Framed E1 with SSM in SDH mode.

The Transmitted SSM and AIS Mode parameters can be configured on the BITS1 port of the 11DPE12A card, when the Signal Type parameter is configured to DS1 ESF in SONET mode or Framed E1 with SSM in SDH mode.

The Line Code parameter can be configured only for the 11DPE12A card when the Signal Type parameter is configured to DS1 ESF or DS1 SF in SONET mode.

The LBO parameter can be configured only on the BITS1 port of the 11DPE12A card when the Signal Type parameter is configured to DS1 ESF or DS1 SF in SONET mode.

4 Save your changes and close the form.

OCS BITS

The 5620 SAM provides two BITS ports on the PSFC card on the 1830 PSS-36 device and the PSF3T8 card on the 1830 PSS-64 device. The BITS ports can be viewed and configured on these cards only on the main shelf of the 1830 PSS OCS devices.

Procedure 9-30 To configure BITS attributes on an 1830 PSS OCS device

The two BITS ports supported on the 1830 PSS OCS devices are:

- BITS 0—PSFC card in card slot 44 of the 1830 PSS-36 shelf and PSF3T8 card in card slot 91 of the 1830 PSS-64 shelf
- BITS 1—PSFC card in card slot 45 of the 1830 PSS-36 shelf and PSF3T8 card in card slot 94 of the 1830 PSS-64 shelf

You can view BITS ports only on the main shelf and not on the extension shelves.

1 On the equipment tree, expand Network→NE→Shelf→PSFC or PSF3T8 card→PSFC or PSF3T8 BITS port.

2 Right-click on the PSFC or PSF3T8 BITS port and choose Properties. The Physical Port (Edit) form opens.

3 Click on the Port Specifics tab and perform one of the following:

a Configure the required parameters on the BITS Attributes panel for the 1830 PSS OCS device in SDH mode:

Note — The SA Bit parameter can be configured when the Signal Type parameter is set as 2MBIT SSM.

b Configure the required parameters on the BITS Attributes panel for the 1830 PSS OCS device in SONET mode:

Note — The Line Code parameter can be configured when the Signal Type parameter is set as DS1 ESF or DS1 ESF no SSM.

4 Save your changes and close the forms.

9.15 Synchronization

An 1830 PSS device synchronizes various signals using a single timing source. The synchronization can be performed using external line references. See section 12.6 for more information about external line timing and SDH line timing reference synchronization on an 1830 PSS OCS device.

WDM synchronization

You can configure synchronization on the following cards installed on the 1830 PSS-4, 1830 PSS-16, or 1830 PSS-32 devices:

- 11DPE12A
- 11DPE12E
- 11QPE24
- 11OPE8
- 11QCE12X

Procedure 9-31 To configure synchronization on an 1830 PSS WDM device

1 On the equipment tree, expand Network→1830 PSS→Shelf→Card.

2 Right-click on the card and choose Properties. The Card Slot (Edit) form opens.

3 Click on the Card Specifics tab and configure the SyncE Support parameter as Enable. The Line Timing, Sync Alarm Profile, and Performance sub-tabs appear.

Assign a port to the line references

4 Click on the Line Timing tab.

5 Choose a Line Reference, and click Properties. The LineReference (Edit) form opens.

6 Configure the Assigned Port parameter and other line timing parameters as required. Table 9-6 lists the ports and line references for the cards supporting synchronization.

Table 9-6 Line references and ports

Cards	Ports	Line reference
11DPE12A	C(1-12)	Line Ref 0
	C(1-12)	Line Ref 1
	L1	Line Ref 2
	L2	Line Ref 3
11DPE12E	C(1-4, 9-12)	Line Ref 0
	C(5-8)	Line Ref 1
	L1	Line Ref 2
	L2	Line Ref 3
11QPE24	X(1-4) and C(1-22)	Line Ref 0
	X(1-6), C(1-2), and M(1-4)	Line Ref 1
11OPE8	X(1-6), C(1-2), and M(1-4)	Line Ref 0 and Line Ref 1
11QCE12X	X(1-4), C(1-12), and M(1-4)	Line Ref 0 and Line Ref 1

7 Click OK to save the changes. The LineReference (Edit) form closes.

Switch timing reference

8 Click on the General tab and configure the Switch To Timing Reference and Switch Request parameters as required in the Sync0 Settings panel.

9 Click Apply to save the changes and close the form.

10 — 1830 PSS applications

10.1 1830 PSS equipment view

The equipment view is a 5620 SAM application that provides a graphical representation of the 1830 PSS shelves, cards, ports and the interconnections.

You can launch the 5620 SAM equipment view from the 5620 SAM GUI. See Procedure 10-1 for information about launching the 5620 SAM equipment view from the 5620 SAM GUI.

10.2 1830 PSS optical service view

The optical service view is a 5620 SAM application that provides a three dimensional graphical representation of an optical transport service and the underlying OTN layers.

You can launch the 5620 SAM optical service view from the 5620 SAM GUI. See Procedure 10-2 for information about launching the 5620 SAM optical service view from the 5620 SAM GUI.

10.3 Procedures to start the applications from the 5620 SAM

Procedure 10-1 To start the equipment view application on a specific web browser

1 To specify the web browser for equipment view:

- **i** Choose Application→User Preferences. The User Preferences form opens.
- **ii** Click Browse beside the Browser Path parameter. The Browser Path form opens.
- **iii** Choose the **exe** file from the appropriate folder and click Open.
- **iv** Close the forms.

Note 1 — Perform step 1 to set the web browser path when the client is used for the first time.

Note 2 — The 5620 SAM applications are supported on the latest version of Mozilla Firefox and Google Chrome, and the latest release of Internet Explorer.

2 Perform one of the following.

a Choose equipment from the 5620 SAM navigation tree view selector. The navigation tree displays the navigation tree objects.

b Choose an 1830 PSS object in the Physical topology map.

3 Right-click on the 1830 PSS object and choose Equipment View. The 5620 SAM equipment view appears in the specified web browser.

Procedure 10-2 To start the optical service view application on a specific web browser

1 To specify the web browser for equipment view:

i Choose Application→User Preferences. The User Preferences form opens.

ii Click Browse beside the Browser Path parameter. The Browser Path form opens.

iii Choose the **exe** file from the appropriate folder and click Open.

iv Close the forms.

Note 1 — Perform step 1 to set the web browser path when the client is used for the first time.

Note 2 — The 5620 SAM applications are supported on the latest version of Mozilla Firefox and Google Chrome, and the latest release of Internet Explorer.

2 On the 5620 SAM main menu, navigate to Manage→Service→Services. The Manage Services form opens.

3 Choose the Optical transport Service (Optical Management) option from the object contextual menu. The optical transports services are listed.

4 Perform one of the following.

a Choose an entry and click Optical Transport Service→Multi-Layer Service Map. The Optical Service View application opens in the specified browser.

b From the Optical transport Service (Edit) form.

i Choose an entry and click Properties. The Optical Transport Service (Edit) form opens.

ii Click Multi-Layer Service Map. The Optical Service View application opens in the specified browser.

5 Choose a service from the Service drop-down menu. The three dimensional view of the optical transport service and the underlying OTN layers appear.

1830 PSS control plane management

11 — 1830 PSS GMRE control plane management

11.1 Overview

The evolution of data applications and the increasing need for on-demand network bandwidth services has put networks under pressure, challenging operators with service provisioning and management simplification. The challenge is to manage all of the different transport layers: circuit, packet, and photonic layers. An intelligent control plane using ASON and GMPLS technologies increases network availability, while protecting services against failures.

The ASON and GMPLS control plane coordinates the operations and provisioning of multilayer networks that provide the capacity and scale to support innovative services while optimizing network resources. The ASON and GMPLS control plane gives service providers the ability to build and manage networks efficiently, control operating costs, and support emerging traffic demands.

GMPLS

GMPLS is a set of protocols that extends MPLS to provide the control plane (signaling and routing) for devices that switch in different domains, including wavelength and fiber. The common control plane simplifies network operation and management by automating end-to-end provisioning of connections, managing network resources, and providing the level of QoS.

ASON

An Automatically Switched Optical Network (ASON) is a an architecture that enables the automatic delivery of transport services. In an ASON architecture, each device should be equipped with a control plane. The control plane sets up and releases connections and may restore a connection in case of a failure.

The ASON relies on the GMPLS protocol to reroute traffic dynamically around a failure. When the failure in the network is repaired, the connection is returned to its original route automatically or upon demand, depending on the connection settings.

Layer 1 GMRE control plane support

The Alcatel-Lucent GMPLS Routing Engine (GMRE) is a software package which contains the GMPLS control plane application. The software package is installed on the First Level Controller (FLC) card of an OCS device and activated on each node in the network using CLI commands.

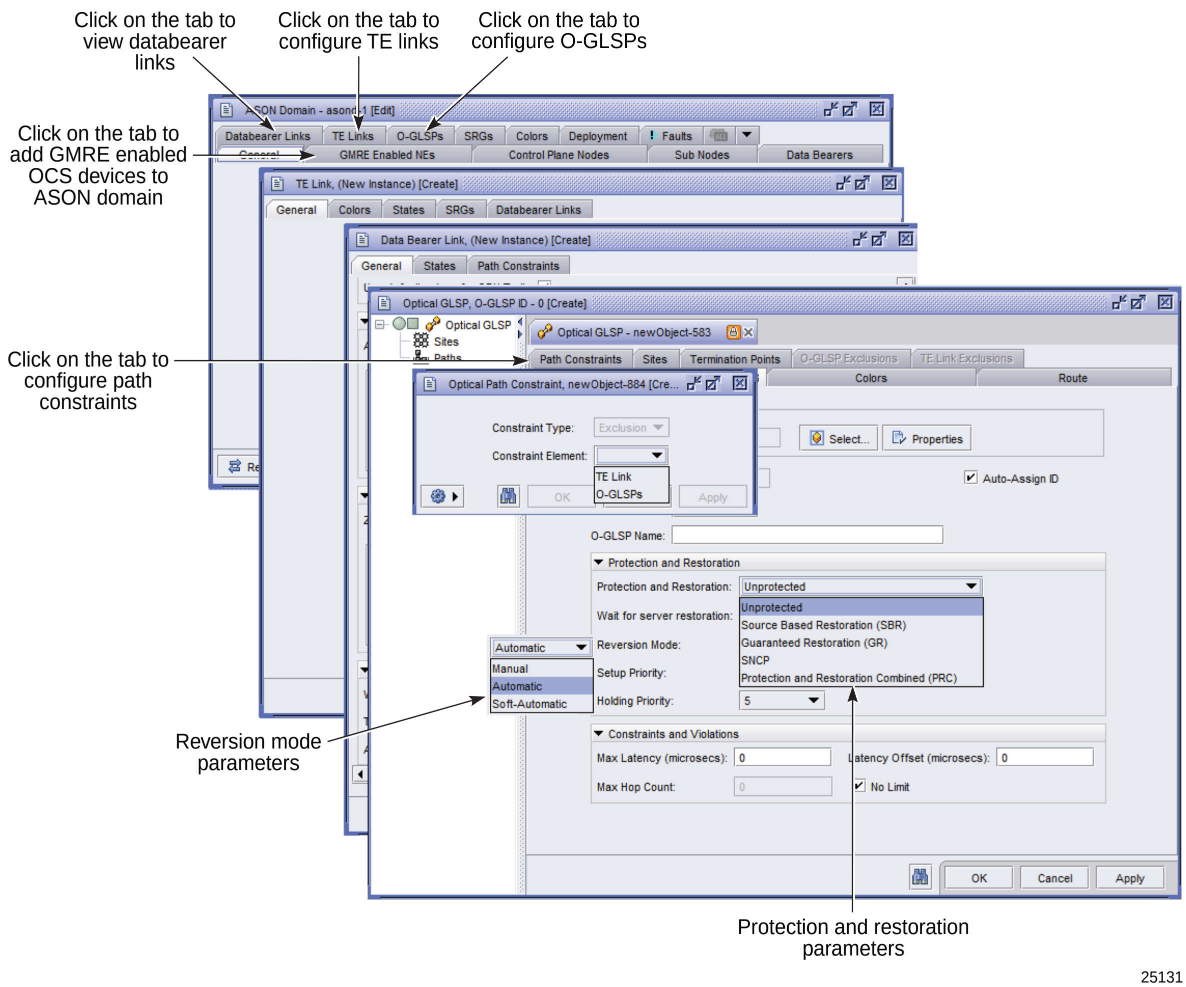
The GMRE-enabled OCS device functions as the control plane and executes the GMPLS protocol suite. The resources of the GMRE-enabled OCS devices are stored in a topology database, and used for routing, link, and alarm administration.

The 5620 SAM supports the configuration of the layer 1 GMRE network for 1830 PSS OCS devices. The 5620 SAM supports the configuration and management of:

- control plane connections—originate and terminate in the ASON network
- managed plane connections—provisioned outside of the ASON network, which is the traditional method of managing connections within a network.

11.2 Workflow to manage the 1830 PSS layer 1 GMRE

Figure 11-1 GMRE management workflow



The following workflow describes the sequence of high-level tasks required to manage and configure the 1830 PSS layer 1 GMRE.

1. Install the GMRE software on 1830 PSS OCS devices. See the *Alcatel-Lucent 1830 PSS GMPLS/GMRE Guide* for more information about GMRE configuration on the 1830 PSS OCS devices.
2. Configure the ASON domain; see Section 11.3.
3. Discover the GMRE-enabled OCS nodes by the 5620 SAM; see Section 11.4.
4. Add the GMRE-enabled OCS nodes to the ASON domain; see Section 11.5.

5 Set up the layer 1 ASON domain infrastructure:

i Configure the data bearers; see Section 11.6.

ii Configure the TE links and data bearer links; see Section 11.7.

iii Configure the SRGs; see Section 11.8.

6 Configure the O-GLSPs; see Section 11.9.

7 As required, configure the GMRE protection; see Section 11.10.

8 As required, configure the color for the GMRE entities; see Section 11.11.

9 As required, update the software version of the CP nodes; see Section 11.12.

11.3 ASON domain management

The 5620 SAM supports the configuration of the ASON domain. See Procedure 11-1 for more information about how to configure the ASON domain. The default ASON domain is configured when you configure the GMRE for the first time. The default ASON domain cannot be deleted.

The 5620 SAM allows you to manage all of the ASON domain objects from the default ASON domain. See Procedure 11-2 for more information about how to navigate to the default ASON domain. You can perform the following functions from the ASON Domain (Edit) form:

- view control plane node properties
- view sub-node properties
- configure data bearers; see Section 11.6
- manage TE links and data bearer links; see Section 11.7
- configure SRGs; see Section 11.8
- configure O-GLSPs; see section 11.9
- color management; see Section 11.11

Procedure 11-1 To configure an ASON domain

1 Perform one of the following:

a Configure the ASON domain from the Manage menu:

i Choose Manage→GMPLS→ASON GMPLS Topology from the 5620 SAM main menu. The ASON GMPLS Topology form opens.

ii Click Create→Create ASON Domain. The ASON Domain (Create) form opens.

b Choose Create→ASON GMPLS Topology→ASON Domain from the 5620 SAM main menu. The ASON Domain (Create) form opens.

2 Configure the required parameters, save your changes, and close the form.

Procedure 11-2 To view the default ASON domain

1 Choose Manage→GMPLS→ASON GMPLS Topology from the 5620 SAM main menu. The ASON GMPLS Topology form opens.

2 Click Search to view the default ASON domain.

3 Choose the default ASON domain entry and click Properties. The ASON Domain (Edit) form opens.

4 View the GMRE entities and close the forms.

11.4 GMRE configuration and 1830 PSS OCS device discovery

GMRE software package configuration

The GMRE software package is installed on the controller card, that is, the First-Level Controller (FLC) of the 1830 PSS OCS device software. See the *Alcatel-Lucent 1830 PSS GMPLS/GMRE Guide* for more information about GMRE configuration on the 1830 PSS OCS devices.

A CP node is an OCS node with GMRE installed. The CP node has an IP address and a node ID called the control plane node ID (CPNodeId). The IP address and node ID must be unique in the network. The node ID and IP address can be assigned with the same value, but they are independently used by the GMRE.

A CP node is divided into logical sub-nodes. The sub-nodes are each of the OCS shelves. Each sub-node is identified in the network by a data plane node ID (DPNodeId).

CP node discovery by the 5620 SAM

The CP node is discovered by the 5620 SAM and the procedure is similar to the OCS device discovery procedure. See Procedure 11-3 for more information about how to discover the CP node.

Procedure 11-3 To discover a CP node

1 Install the GMRE software package on the controller card. See the *Alcatel-Lucent 1830 PSS GMPLS/GMRE Guide* for more information about GMRE installation on the 1830 PSS OCS devices.

2 Configure the mediation policy. See Procedure 7-6.

3 Configure the discovery rule. See Procedure 7-7.

The GMRE-enabled OCS device appears on the physical topology map and on the equipment tree.

Note — The GMRE is not discovered until the CP node is added to the ASON domain.

4 Add the GMRE-enabled OCS node to the ASON domain. See Procedure 11-5.

The CP node is synchronized.

The CP node object display the “G” character on the physical topology map and “GMPLS” label on the equipment tree.

CP node discovery of an already managed OCS device

If the 1830 PSS OCS device is already managed by the 5620 SAM, the GMRE configuration is carried out from the GMRE CLI cut-through and the OCS device is resynchronized on the 5620 SAM. See Procedure 11-4 for more information about how to configure the GMRE on the OCS device that is managed by the 5620 SAM.

Procedure 11-4 To configure GMRE software on an OCS device managed by the 5620 SAM

1 Right-click on the OCS device in the topology map and choose NE Sessions→SSH Session. The SSH Session form and a dialog box opens.

2 Enter the login credentials in the dialog box.

3 Enter the Port parameter value as 22 and click OK. The dialog box closes and the SSH Session form appears.

4 Enter the following at the command prompt:

`cli` ↵

5 Install the GMRE software package. See the *Alcatel-Lucent 1830 PSS GMPLS/GMRE Guide* for more information about GMRE installation on the 1830 PSS OCS devices.

6 Right-click on the 1830 PSS OCS device object on the equipment tree or in the physical topology map, and choose Resync→Customized Resync. The Resync Site(s) step form opens.

7 Select Choose MIB Entries and click Next. The Choose MIB Entries form opens.

8 Enter *optical.CpMgrDataTableEntry* in the MIB Entry field and click Search. The MIB entry is listed.

9 Choose the MIB entry, click Finish to resynchronize the MIB, and close the form.

10 Add the GMRE-enabled OCS nodes to the ASON domain. See Procedure 11-5.

The CP node is synchronized.

The CP node object displays the "G" character on the physical topology map and "GMPLS" label on the equipment tree.

11.5 ASON licensing and adding the GMRE-enabled OCS nodes to the ASON domain

The 5620 SAM supports the licensing of the CP nodes. A 5620 SAM NE-level license is required before the 5620 SAM enables the control plane part of the node that has GMRE installed.

The license information is displayed on the Devices and Quantities Licensed tab of the Help→5620 SAM License Information→5620 SAM License (Edit) form. If the Remaining table entry count for the 1830 GMPLS Node table entry is less than one, the CP node is not discovered by the 5620 SAM.

The GMRE entities are synchronized after the GMRE-enabled OCS nodes are added to the ASON domain. See Procedure 11-5 for more information about adding the GMRE-enabled OCS nodes to the ASON domain. One NE-level license is used for each OCS node that is added to the ASON domain. The count of the licenses used is also displayed in the Manage→GMPLS→ASON GMPLS Topology→ASON GMPLS Topology form.

After adding the GMRE-enabled OCS nodes to the ASON domain:

- the GMRE entities are populated in the ASON Domain (Edit) form
- the "GMPLS" label appears against the device object in the equipment tree
- the "G" character appears on the device icon in physical topology map

Procedure 11-5 To add the GMRE-enabled OCS nodes to ASON domain

1 Perform Procedure 11-2 to open the ASON Domain (Edit) form.

2 Click on the GMRE-enabled NEs tab and click ADD.

3 Choose the GMRE-enabled OCS nodes that need to be added to the ASON domain.

11.6 Data bearers

The 5620 SAM supports the configuration of the following data bearers:

- Drop
  - L1 OTU drop data bearers
  - L1 client transparent drop data bearers
- I-NNI

L1 drop data bearers assign a client port to the control plane and L1 drop data bearers provide end-points for SPC services. Therefore, L1 drop data bearers are also called SPC endpoints. Signaling and routing protocols are not run on L1 drop data bearers. See Procedure 11-6 for more information about how to configure L1 drop data bearers.

I-NNI data bearers assign a line port to the control plane. When I-NNI data bearers are discovered, a data bearer link is configured between the OTU ports of the OCS uplink or I/O cards of two 1830 PSS OCS sub-nodes that point to each other. See Procedure 11-7 for more information about how to configure the data bearer links.

L1 OTU drop data bearers

Configure the L1 OTU drop data bearer on an OTU port of an I/O card in an 1830 PSS OCS GMRE device.

Procedure 11-6 To configure an L1 OTU drop data bearer

1 Perform one of the following:

a Configure an L1 OTU drop data bearer from the equipment tree:

i On the equipment tree, expand Network→1830 PSS OCS (GMPLS)→Shelf→I/O card→OTU port.

ii Right-click on the port object and choose Create DROP data Bearer. The Data Bearer (Create) form opens with all the parameters configured.

b Configure an L1 OTU drop data bearer from the ASON default domain:

i Perform Procedure 11-2 to open the ASON Domain (Edit) form.

ii Click on the Data Bearers tab and click Create. The Data Bearer (Create) form opens.

iii Select a sub-node in the ASON SubNode DP Node ID panel and a port in the Local Port Pointer panel.

c Configure an L1 OTU drop data bearer from the 5620 SAM main menu:

i Choose Create→ASON GMPLS Topology→DROP data Bearer from the 5620 SAM main menu. The Data Bearer (Create) form opens.

ii Select a sub-node in the ASON SubNode DP Node ID panel and a port in the Local Port Pointer panel.

2 Save your changes and close the forms.

L1 client transparent drop data bearers

The L1 client transparent drop data bearer is configured on a non-OTU port, for example, SONET, SDH, or GbE port, of an I/O card in an 1830 PSS OCS GMRE device. Perform Procedure 11-6 to configure an L1 client transparent drop data bearer by choosing the non-OTU port.

11.7 TE links

A traffic engineering link is a GMRE entity that is configured by grouping the other GMRE entities like data bearer link, SRGs, or metrics. The grouping reduces the amount of information sent through the network.

The 5620 SAM supports the configuration of TE links. You can configure metric (cost), color, data bearer link, and assign SRGs for a TE link.

See Procedure 11-7 for more information about how to configure the TE links and data bearer links.

Data bearer links

The 5620 SAM supports the configuration of data bearer links between the OTU line ports of the OCS uplink or I/O cards. A physical or logical link needs to be configured between the OTU ports of the OCS uplink or I/O cards before the configuration of the data bearer links.

A physical link is established when you configure an optical link between OTU ports. See Procedure 9-18 for more information about how to configure optical links.

A logical link is established when you configure OTU trails between OTU ports. See Procedure 13-6 for more information about how to configure OTU trails.

See Procedure 11-7 for more information about how to configure the TE links and data bearer links.

If a physical link is established between two OCS I-NNI ports, the corresponding OTU trails and ODUk cross-connects are auto-configured during the data bearer link configuration. The 5620 SAM performs a path search and if there is a path between the two ports, an Unterm ODU trail is auto-configured. If no path is found, the data bearer link configuration fails.

The data bearer links need to be assigned to a TE link, so that the data bearer link is made available for a service. You can add the data bearer links to an existing or a new TE link. See Procedure 11-7 for more information about how to configure data bearer links.

Unterm ODU trail

The 5620 SAM automatically configures the underlying HO Unterm ODU trail, when the data bearer link is configured between the I-NNI ports. See Procedure 11-7 for more information about how to configure the data bearer links and TE links.

The 5620 SAM supports the configuration of the missing Unterm ODU trails, for the data bearer links that do not have associated Unterm ODU trails. See Procedure 11-8 for more information about how to configure the missing Unterm ODU trails.

The 5620 SAM supports the discovery of Unterm ODU trails for the data bearer links when the CP nodes are discovered or the Unterm ODU trail is unmanaged. See Procedure 11-9 for more information about how to discover the Unterm ODU trails.

Note — Ensure that the Unterm ODU trail discovery is performed every time the CP nodes are added to the ASON domain,

The 5620 SAM allows you to modify the attributes of the Unterm ODU trails. See Procedure 11-10 for more information about how to modify the attributes of an Unterm ODU trail.

Procedure 11-7 To configure a TE link, a data bearer link, and assign SRGs with the TE links

1 Perform one of the following:

- **a** Configure TE links from the ASON default domain:
  - **i** Perform Procedure 11-2 to open the ASON Domain (Edit) form.
  - **ii** Click on the TE Links tab and click Create. The TE Link (Create) form opens.
- **b** Choose Create→ASON GMPLS Topology→TE Link from the 5620 SAM main menu. The TE Link (Create) form opens.

Configure cost and latency

2 Configure the required parameters.

3 Select the sites in the Endpoint A - TE Link Endpoint and Endpoint Z - TE Link Endpoint panels.

4 Configure the parameters in the Traffic Engineering Parameters panel to manage cost and latency.

Assign colors

5 Click on the Colors tab and assign a color ID to the TE link to identify the TE link in the network.

6 Click on the States tab and configure the Administrative State parameter.

Assign SRGs

7 Click on the SRGs tab and click Add. The Select SRG form opens.

8 Choose SRGs and click OK to assign the SRGs to the TE link.

Configure a data bearer link

9 Click on the Databearer Links tab and click Create. The Data Bearer Link (Create) form opens.

10 Configure the required parameters and the parameters in the Unterm ODU Trail panel.

11 Select the ports in the Endpoint A and Endpoint Z panels.

> **Note —** Ensure that a physical connectivity exists between the ports. See Procedure 9-18 for more information about how to configure an optical link.

12 If a path constraint needs to be configured, click on the Path Constraints tab and click Create. The Optical Path Constraint (Create) form opens.

13 Configure the required parameters and select the port, site, trail, ODUk timeslot, or optical link, depending on the constraint element

14 Save your changes and close the forms.

Procedure 11-8 To configure the missing Unterm ODU trails

1 Perform Procedure 11-2 to open the ASON Domain (Edit) form.

2 Click on the Databearer Links tab.

3 Choose the data bearer link with the missing Unterm ODU trail and click Properties.

4 Click Create Unterm ODU Trail.

The Create Unterm ODU Trail button is dimmed for the data bearer links that have an associated Unterm ODU trail.

5 Choose an entry and click Properties. The Unterm ODU Trail (Edit) form opens.

6 Save your changes and close the forms.

Procedure 11-9 To discover the Unterm ODU trails

1 Perform Procedure 11-7 to configure the data bearer links between the I-NNI ports.

2 Choose Manage→OTN→OTN Trails. The Manage OTN trails form opens.

3 Choose Unterm ODU Trail (Optical Management) from the object contextual menu and click Discover Optical Trails. The Discover Optical Trails form opens.

4 Choose the equipment group and click OK. The Unterm ODU trails are listed.

One Unterm ODU trail is auto-configured for each data bearer link that is configured.

Procedure 11-10 To modify the properties on an Unterm ODU trail

1 Perform Procedure 11-7 to configure the data bearer links between the I-NNI ports.

2 Choose Manage→OTN→OTN Trails. The Manage OTN trails form opens.

3 Choose Unterm ODU Trail (Optical Management) from the object contextual menu. The Unterm ODU trails are listed.

4 Choose an entry and click Properties. The Unterm ODU Trail (Edit) form opens.

5 If a path constraint needs to be configured, click on the Path Constraints tab and click Create. The Optical Path Constraint (Create) form opens.

6 Configure the required parameters and select the port, site, trail, ODUk timeslot, or optical link depending on the constraint element

7 Save your changes, wait for the changes to be populated in the forms, and close the forms.

11.8 Shared risk groups

An SRG is a set of physical connections and objects that share a common risk. The failure of one of the objects can cause the failure of all the elements in the group. The SRGs provide a redundant route through the network for an existing route, avoiding the same problem; for example, a link failure that disturbs both the routes.

SRGs are identified by SRG IDs, which need to be unique in a GMRE domain. The 5620 SAM supports the configuration of the SRGs with unique IDs.

See Procedure 11-11 for more information about how to configure SRGs, and Procedure 11-7 for more information about how to assign SRGs to a TE link.

Procedure 11-11 To configure SRGs

1 Perform Procedure 11-2 to open the ASON Domain (Edit) form.

2 Click on the SRGs tab and click Create.The SRG (Create) form opens.

3 Configure the required parameters.

4 Save your changes and close the forms.

Note — The SRGs are deployed when they are assigned to a TE link. One or more SRGs have to be assigned to the TE links in the ASON network that share at least one risk.

11.9 O-GLSP

O-GLSP is a layer 1 service between two GMRE nodes in a subnetwork. See Procedure 11-12 for information about configuration of an O-GLSP.

A nominal path is established when an O-GLSP is configured. According to the GMRE, the nominal path is the best path available under ideal network conditions. When a failure occurs in the nominal path, a backup path is created by the GMRE. The backup path is not the best path. The GMRE finds a backup path to keep the traffic flow up, until the nominal path is fixed.

Soft-permanent connection type

The 5620 SAM supports the configuration of the soft-permanent connection. A soft-permanent connection is an end to end service between a source node and destination node which may or may not go through intermediate nodes. See Procedure 11-12 for information about configuration of an O-GLSP.

Protection and restoration

You can configure one of the following O-GLSP protection and restoration methods with the 5620 SAM.

Unprotected

There is no backup path available if a failure occurs in the nominal path.

Source based restoration (SBR)

If a failure occurs in the nominal path, a backup path is created. If the backup path fails, another backup path is created until no more backups can be found. After the nominal path failure is fixed, one of the following occurs to switch the traffic to nominal path:

- If the reversion mode is set as automatic, the GMRE switches the traffic to the nominal path.
- If the reversion mode is set as manual, you need to choose Switch Route→Nominal on the Optical O-GLSP (Edit) form to switch the traffic to the nominal path. See Procedure 11-12 for information about configuration of an O-GLSP.

Guaranteed restoration (GR)

If a failure occurs in the nominal path, the pre-calculated backup path is activated as the backup path, and another backup is calculated by the GMRE. The pre-calculated backup path is always different from the nominal path. After the nominal path failure is fixed, the GMRE switches the traffic to the nominal path.

Sub-network connection protection (SNCP)

The two paths of a protected service in a GMRE domain are referred to as main and spare paths. If a failure occurs in the nominal main path, the traffic is switched to the nominal spare path. However, no restoration is supported. The traffic path is automatically switched through the control plane APS group.

Note — Internal SNCP

In a GMRE domain, internal SNCP is a service of protection type SNCP between GMRE domain-boundary nodes.

In a unidirectional operation, traffic is bridged in the source node, also known as the head-end node. In the destination node, also known as the tail-end node, a selector switch is implemented. The selector switch selects the traffic received through either of the two paths, the main or spare path.

In a bidirectional operation, each of the end nodes of the SNCP works as a bridge for one direction and as a selector switch for the opposite direction.

Protection and restoration combined (PRC)

If a failure occurs in the nominal main path or the nominal spare path, main and spare backup paths are created. After the failure in the nominal main or spare paths is fixed, the GMRE switches the traffic to the nominal main or spare paths. The path is switched through the control plane APS group.

Restore O-GLSP nominal paths

You can configure the following Reversion Mode parameter options to switch traffic to the nominal path when the failure is fixed.

- Manual—The reversion process involves manual intervention to reroute the carried services, before switching to the nominal path. Choose Switch Route→Nominal or Registered Backup at the bottom of the Optical O-GLSP (Edit) form to perform this task. See Procedure 11-12 for information about configuration of an O-GLSP.
- Automatic—Within five minutes of nominal path restoration, the 5620 SAM automatically switches to the nominal path. By default, the 5620 SAM sets the path reversion to automatic mode.
- Soft-Automatic—The reversion process involves triggering the carried services to reroute. The rerouting is monitored for timeout. When the path does not have any services, the path reversion is initiated.

Discovery of O-GLSP

The 5620 SAM supports the discovery of the O-GLSPs configured on the CP nodes. See Procedure 11-13 for more information about how to discover the O-GLSPs.

Discovery of the control plane ODU trail

The CP node ODU trail is automatically configured when an Active O-GLSP (that is, with a valid path) is configured. The 5620 SAM supports the discovery of the ODU trail configured on the CP nodes. See Procedure 11-14 for more information about how to discover the ODU trails.

Procedure 11-12 To configure an O-GLSP

You must configure an I-NNI data bearer link before you configure an O-GLSP. To configure an O-GLSP with restoration method, ensure there are sufficient I-NNI links available. See section 11.7 for more information about data bearer link configuration.

1 Perform one of the following to open the Optical GLSP (Create) form.

- **a** Choose Create→ASON GMPLS Topology→O-GLSP from the 5620 SAM main menu. The Optical GLSP (Create) form opens.
- **b** Perform Procedure 11-2 to open the ASON Domain (Edit) form and click Create→Create O-GLSP. The Optical GLSP (Create) form opens.
- **c** Right-click on the GMRE device on the Physical Topology map or equipment tree and choose Create O-GLSP. The Optical GLSP (Create) form opens with Site (Z End) object configured.

2 Configure the general O-GLSP parameters.

3 Configure the required parameters in the Protection and Restoration panel.

4 Configure the required parameters in the Constraints and Violations panel.

5 Right-click on the Sites object on the navigation tree and choose Create O-GLSP Site. The Select Network Element form opens.

6 Choose the sites and click OK. The Site objects are listed under the Optical GLSP tree.

7 Right-click on the Site (A End) object and choose Create O-GLSP Termination Point. The Select Termination Point form opens.

8 Choose the termination point and click OK.

9 Repeat steps 7 to 8 to configure the termination point on the Site (Z End).

10 Click Apply to save your changes.

Configure path constraints

11 Click on the Path Constraints tab and click Create. The Optical Path Constraint (Create) form opens.

12 Configure the Constraint Element parameter.

13 Select the TE link or the O-GLSP, depending on the value configured for the Constraint Element parameter in step 12, and click OK.

Note — You can configure paths constraints when you configure an O-GLSP or modify the path constraints after you configure the O-GLSP.

Configure color

14 Click on the Colors tab.

15 Choose one or more colors from the unassigned list of the Included Colors and Excluded Colors panels and click on the right arrow.

View hops

16 Click on the Nominal path object on the Optical GLSP tree and click on the Connections tab to view the O-GLSP hops.

17 Click Apply to save your changes, and close the forms.

Procedure 11-13 To discover the O-GLSPs

1 Add the GMRE-enabled OCS nodes in the ASON domain. See Procedure 11-5.

2 Click on the O-GLSPs tab to view the list of the discovered O-GLSPs.

Procedure 11-14 To discover the ODU trails

1 Add the GMRE-enabled OCS nodes in the ASON domain. See Procedure 11-5.

Wait until the node resynchronization completes.

2 Choose Administration→Discovery Manager. The Discovery Manager (Edit) form opens.

3 Click on the Resync Status tab and click Search.

Check the resynchronization status of the GMRE-enabled OCS nodes.

4 Choose Manage→OTN→OTN Trails. The Manage OTN Trails form opens.

5 Click Discover Optical Trails. The Discover Optical Trails form opens.

6 Choose the equipment group and click OK. The ODU trails are listed in the Manage OTN trails form.

Each O-GLSP that is configured will have a corresponding ODU trail auto-configured.

11.10 GMRE protection switching

The 5620 SAM allows switching from the main to the spare path and from the spare to the main for internal SNCP and PRC configurations. See Procedure 11-15 for more information about how to perform protection switching from main to spare or spare to main paths.

Procedure 11-15 To perform protection switching from main to spare or spare to main

1 Perform Procedure 11-2 to open the ASON Domain (Edit) form.

2 Perform one of the following:

a To configure from the sub-node, click on the Sub Nodes tab, choose a sub-node, and click Properties. The Sub-node (Edit) form opens.

b To configure from the OGLSP, click on the O-GLSPs tab, choose an SNCP or PRC entry, and click Properties. The Optical GLSP (Edit) form opens.

3 Click on the APS tab, choose an entry, and click Properties. The Protection Switch (Edit) form opens.

4 Configure the Switch Command parameter and switch to main or spare paths.

5 Save the changes and close the forms.

11.11 ASON color management

The 5620 SAM auto-configures 28 pre-defined colors during the ASON domain configuration. The colors can be assigned to TE links, physical connections, logical connections, and O-GLSPs.

Procedure 11-16 To modify color description

1 Perform the Procedure 11-2 to open the ASON Domain (Edit) form.

2 Click on the Colors tab. The 28 pre-defined color IDs are listed.

3 Click on a color ID and click Properties. The Color (Edit) form opens.

4 Configure the Description parameter, click Apply to save the changes, and close the form.

11.12 GMRE software upgrade

The 5620 SAM supports the upgrade of the GMRE software. See Procedure 11-17 for more information about how to view the GMRE software version.

The active network version is the GMRE software version that is currently in use. The installed network version is the GMRE software version at the time of GMRE activation. Only the GMRE features supported by the active network version of the GMRE software are available on the 1830 PSS OCS GMRE device.

During the software upgrade of the 1830 PSS OCS device, the installed network version is upgraded, but not the active network version. The 5620 SAM allows you to upgrade the GMRE software to the installed version. See Procedure 11-18 for more information about how to upgrade the active network version.

Procedure 11-17 View the software version of the CP node

1 Choose Manage→GMPLS→ASON GMPLS Topology from the 5620 SAM main menu. The ASON GMPLS Topology form opens.

2 Click Search to view the default ASON domain.

3 Choose the default ASON domain and click Properties. The ASON Domain (Edit) form opens.

4 Click on the Control Plane Nodes tab, choose an entry, and click Properties. The Control Plane Node (Edit) form opens.

The GMRE Software panel displays the active and installed network version.

Procedure 11-18 Upgrade the active network version of the CP node

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

2 Click on the Software Images tab, then on the OCS Software Images tab, and click Activate GMRE. The Select ASON Domain form opens.

3 Choose the ASON domain and click OK to upgrade the active network version of the GMRE software.

Note 1 — Ensure that all the GMRE nodes have the same network version installed.

Note 2 — Ensure that all the GMRE nodes in the ASON domain are reachable from the 5620 SAM.

11.13 GMRE alarm management and correlation

The 5620 SAM supports alarm management and alarm correlation of the alarms generated from the CP node. See section 20.5 for more information about how to view alarm correlation in the 5620 SAM fault management application.

1830 PSS SDH trails and services

12 — SDH trails and services

12.1 SDH networks overview

The 10SD10G and 24SDM cards support STH port group mode, which provides STM line interfaces and a VC4 based interface toward the backplane. SDH switching and transport over OTN is achieved by using an optical fiber connection between the TDM client and optical client/line cards.

12.2 Workflow to configure a VC4 service

1 Configure TDM cards on an 1830 PSS OCS device by choosing TDM cards as the assigned card type. See Procedure 9-8.

2 Configure VC4 sub-structures. For example, if you need to create a VC4-4C or a VC4-16C service, configure the sub-structures appropriately. See Procedure 12-1.

3 Configure the VC4 service in a bottom-up or top-down approach.

a Configure the VC4 service in a bottom-up approach.

i Configure 1+1 MSP groups on the ports involved in the service hops, if required. See Procedure 12-3.

Note — After the service is created, click on the APS Groups tabs of the Optical Transport Service (Edit) form to view the VCn APS groups and 1+1 MSPs involved in the service.

ii If required, configure the VC4 cross-connects. See section 12.4.

iii Configure an STM trail before configuring a VC4 service with underlying asymmetric ODU trails. See section 12.7.

iv Configure the VC4 service. See section 12.8.

b Configure the VC4 service in a top-down approach.

i Configure an HO-ODU trail between optical client/line cards on the termination sites of the service. See Procedure 13-1.

ii Configure the VC4-4 service. See section 12.8.

Note — The underlying trails are created automatically.

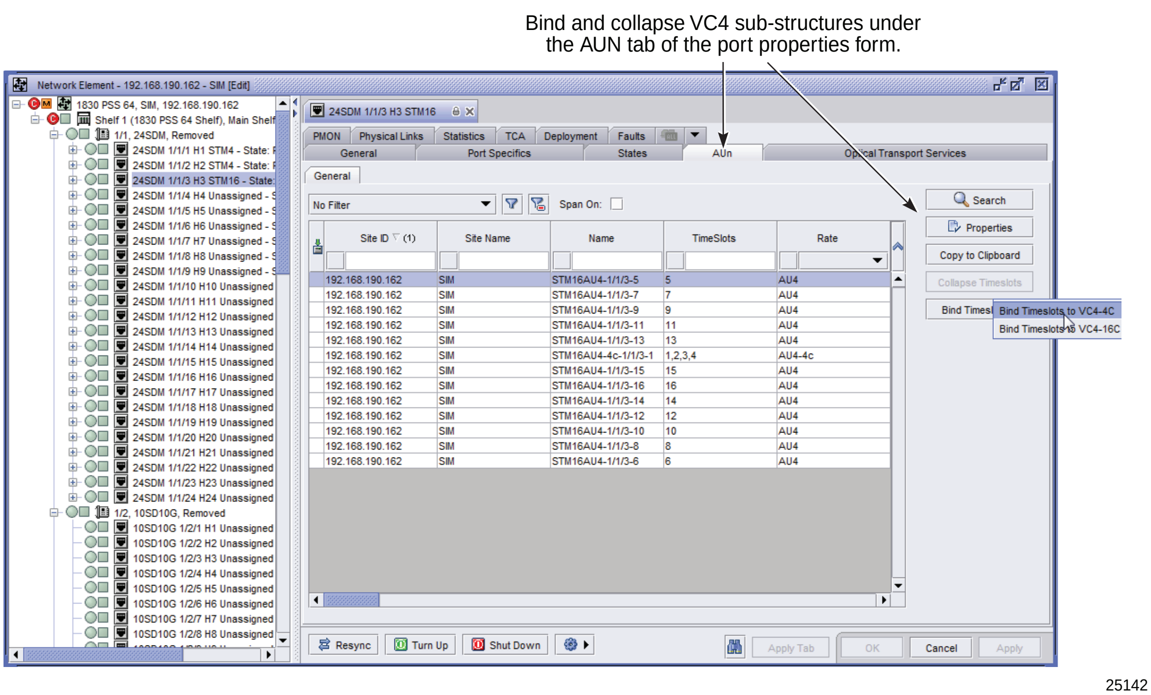
12.3 VC4 sub-structures

The ports with STM rates are further subdivided into administrative units or AUs. These administrative units can be bound together to form virtual containers. See Procedure 12-1. Table 12-1 lists the sub-structuring of ports with STM rates.

Table 12-1 VC4 sub-structures

STM rate	AU-n	Number of AU-n	Maximum possible number of VC4-4C	Maximum possible number of VC4-16C
STM-1	STM1AU4	1	0	0
STM-4	STM4AU4	4	1	0
STM-16	STM16AU4	16	4	1
STM-64	STM64AU4	64	16	4

Figure 12-1 VC4 sub-structures



Procedure 12-1 To bind and collapse VC4 sub-structures

1 On the equipment tree, expand Network→Shelf→Card(10SD10G or 24SDM)→Port.

2 Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

3 Click on the Show All Tabs, then on the AUn tab.

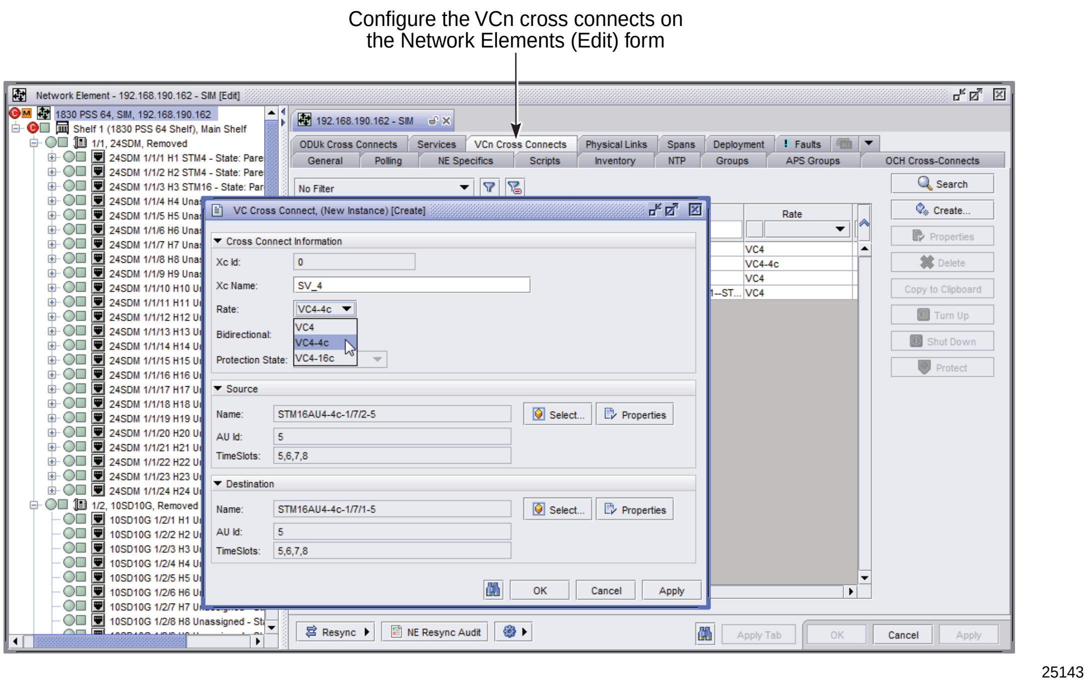
4 Choose the required port, click Bind Timeslots, and choose either Bind Timeslots to VC4-4C or Bind Timeslots to VC4-16C. See Table 12-1.

5 Choose a bound timeslot and click Collapse Timeslots to retrieve the initial STMnAU4.

12.4 VCn cross-connects

The 5620 SAM allows you to configure VCn cross-connects using the VC4 sub-structures. You can also add protection or remove protection from the cross-connects. See Procedure 12-2.

Figure 12-2 VCn cross-connects



Procedure 12-2 To configure a VCn XC and protect/unprotect the VCn XC

Before you configure a VCn XC with a rate of VC4-4c or VC4-16c, ensure that you have created the VC4 sub-structures, as required. See Procedure 12-1.

Configure a VCn XC

1 On the navigation tree, expand Network→1830 PSS.

2 Right-click on the 1830 PSS device and choose Properties. The Network Element (Edit) form opens.

3 Click on the VCn Cross Connects tab.

4 Click Create. The VC Cross Connect (Create) form opens.

5 Configure the parameters in the Cross Connect Information panel.

6 Select the source and destination VC4 sub-structures in the Source and Destination panels respectively.

7 Click OK. The VCn XC is listed in the VCn Cross Connects tab of the Network Element (Edit) form.

Protect a VCn XC

8 Choose the VCn XC and click Protect. The TDM Facility Protection Group form opens.

9 Select the VC4 sub-structure in the Protection panel.

10 Configure the parameters as required in the VCnXC Protection Configuration and Protection Management panels.

11 Click OK. The Working and Protection XCs are listed in the VCn Cross Connects tab.

12 Click on the APS Groups tab to view the TDM facility protection group created.

Unprotect of a VCn XC

13 Choose a TDM facility protection group in the APS Groups tab and click Unprotect.

14 Click Yes to confirm. The Unprotect form opens.

15 Choose the path you need to remove and click OK. The TDM facility protection group is removed from the list in the APS group.

16 Click on the VCn Cross Connects tab. The unprotected VCn XC is displayed.

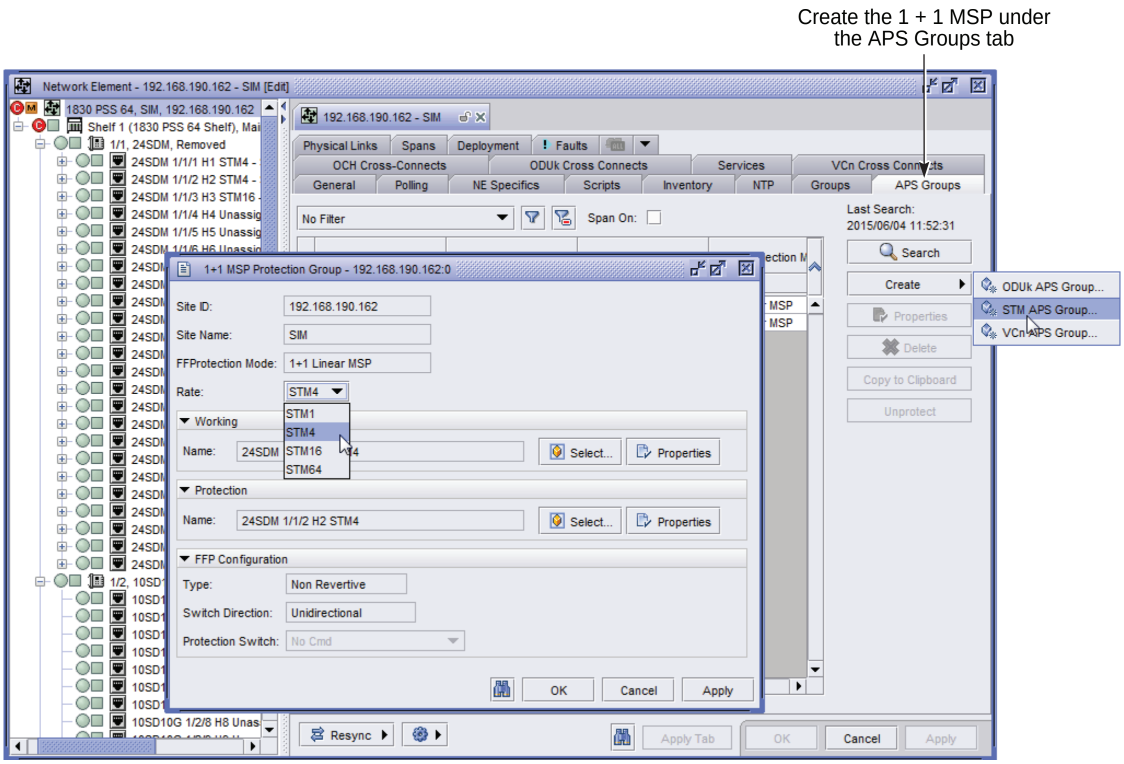
17 Close the form.

12.5 1+1 MSP group

You can configure 1+1 multiplex section protection group on 10SD10G or 24SDM card ports configured with rates STM-1, STM-4, STM-16, or STM-64. Each of the paired ports in the group must have the same STM rate.

The ports can be on the same card or on different cards on the same device. The protection group supports unidirectional and non-revertive switching. See Procedure 12-3. See *Alcatel-Lucent 1830 PSS Product Information and Planning Guide* for more information about 1+1 MSP groups.

Figure 12-3 1+1 MSP group



25144

Procedure 12-3 To configure a 1+1 MSP group

1 On the equipment tree, expand Network→1830 PSS.

2 Right-click on the 1830 PSS device object and choose Properties. The Network Element (Edit) form opens.

3 Click on the APS Groups tab, click Create, then choose STM APS Group. The 1+1 MSP Protection Group form opens.

4 Configure the Rate parameter.

5 Select the working and protection ports in the Working and Protections panels.

6 Click Apply to save the changes.

7 Configure the parameters in the FFP Configuration panel, as required.

8 Save your changes and close the forms.

12.6 SDH line timing synchronization

The capability to synchronize the system to line timing reference transmission ports is restricted to STM-64 ports of the 10SD10G card with SDH termination capability. By default, the synchronization is set to the internal time reference that is provided by the oscillators on the matrix cards of the 1830 PSS OCS devices.

The 5620 SAM allows you to perform the following on an 1830 PSS OCS device:

- configure the attributes on the BITS ports of the power filter cards
- assign these ports to the external time references
- use one of these external time references for the purpose of synchronization

Procedure 12-4 To configure an SDH line timing synchronization

1 On the equipment tree, expand Network→NE→Shelf.

2 Right-click on the shelf object and choose Properties. The Shelf (Edit) form opens.

3 Click on the Synchronization tab and set the Sync Messaging parameter to Enable on the System Timing Reference panel to enable synchronization.

4 Select an alarm profile.

Assign a port to an external or line timing reference

5 Choose an external or line timing reference in the External/Line Timing Reference panel and click Properties. The LineReference (Edit) form opens.

6 Select a port in the Assigned Port panel.

Note 1 — You can assign only ports with STM -64 rates of the 10SD10G cards to the Line Ref 0 through 5.

Note 2 — You cannot assign more than one external or line timing reference to a port.

Table 12-2 External or line timing references and ports

Cards	Ports	External or line reference
PSF3T8 (1830 PSS-64) and PSFC (1830 PSS-36)	BITS0 and BITS1	External Line Ref 0 and External Line Ref 1
10SD10G	H1 to H10 with rate assigned	Line Ref 0 to Line Ref 5

7 Configure the required line timing parameters on the General tab.

Note 1 — If the Signal Type parameter is set to 2MBIT SSM or DS1 ESF in Procedure 9-31, synchronization is based on the value of the Provisioned Quality Level parameter of the external timing reference.

Note 2 — If the Signal Type parameter is set to 2MBIT No SSM or DS1 ESF No SSM in Procedure 9-31, synchronization is based on the value of the Priority parameter of the external timing reference.

8 Click OK. The LineReference (Edit) form closes and the Shelf (Edit) form reappears.

9 Click Apply. The assigned port is listed in the External/Line Timing Reference panel.

10 Repeat steps 5 to 9 for External Line Ref 1, if required.

Switch timing reference

11 Configure the Switch To Timing Reference and Switch Request parameters as required.

Note 1 — By default, the Switch to Timing Reference parameter is set to Sync0/Internal. You can configure it to the required external or line timing reference after assigning ports as described in steps 5 to 10.

Note 2 — If the Switch Request parameter for an external or line timing reference is configured as Lockout, you cannot set the Switch Request to Force Switch. Configure the Switch Request parameter as Clear, click Apply, then configure the Switch Request parameter as Force Switch to switch to the external or line timing reference.

12 Click Apply to save the changes. The Active Line Reference parameter displays the external or line timing reference.

13 Close the form.

12.7 STM trail configuration

Procedure 12-5 To configure an unprotected STM trail

An STM trail is created between STM ports of TDM cards. Before you create an STM trail between two ports with STM rates, perform the following.

- Create an optical link between the STM port of the TDM card and the STM port of an optical client/line card on both Site A and Site Z ends.
- Create an HO-ODU trail between the two sites from one ODUPOOL to the other.

1 Choose Create→STM Trail from the 5620 SAM main menu. The STM Trail (Create) form opens.

2 Configure the required parameters under the General tab.

3 Right-click on the Sites object on the navigation tree and choose Create Trail Site. The Select Network Elements form opens.

4 Choose two network elements and click OK. The Site A End and Site Z End objects are listed in the navigation tree.

5 Right-click on the Site A End object and choose Create Trail Termination Point. The Select Termination Point form opens.

6 Choose the required termination point from the list and click OK. The termination point is listed under the Site A End object on the navigation tree.

Note — Confirm the pre-requisites as indicated at the beginning of this procedure to have the possible termination points listed in the Select Termination Point form.

7 Perform steps 5 to 6 to configure the Site Z end termination point.

8 Click Apply to save the changes.

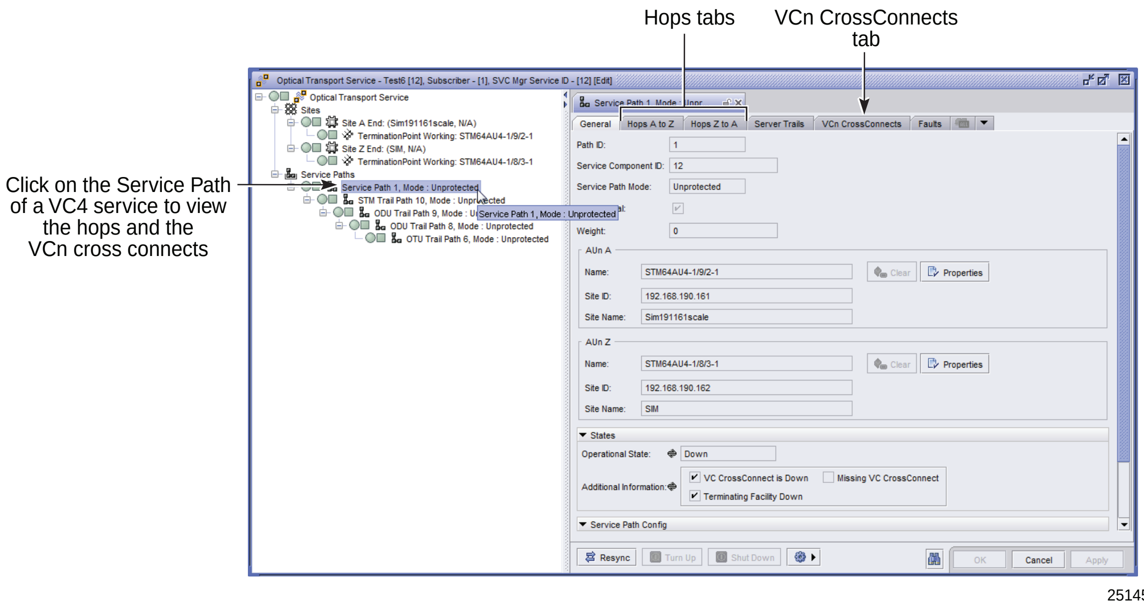
9 Expand Trail Paths to view the underlying STM, LO-ODU, HO-ODU, and OTU trails.

10 Close the form.

12.8 VC4 service configuration

You can create a VC4 service in a top-down or bottom-up approach. In a top-down scenario, configure an HO-ODU trail between the sites, and configure the service between the TDM cards. The underlying STM and LO-ODU trails are created automatically. In a bottom-up scenario, create the LO-ODU, STM, and HO_ODU trails, and then configure a VC4 service using these trails. See section 12.2 and Procedure 12-6 for more information about configuring a VC4 service.

Figure 12-4 VC4 service



Procedure 12-6 To configure a VC4 service

1 Configure VC4 sub-structures as required. See Procedure 12-1.

2 Perform one of the following.

a To configure an unprotected VC4 service, perform Procedure 16-1 with the Rate parameter configured as VC4, VC-4C, or VC-16C, as required.

b To configure a protected VC4 service, configure the Protection Type as ESNCP Protected and configure the working and protection path constraints, as required. See Procedure 16-6 for more information about configuring path constraints.

Note — The VCn cross-connects, STM trail, and VCn APS groups are created automatically when the VC4 service is created in a top-down approach.

1830 PSS OTN layer management

13 — 1830 PSS optical trail configuration

13.1 OTN

OTN is an ITU-T standard (G.709) that describes a method for wrapping signals of different protocols for transport across an optical network. OTN provides transport, multiplexing, routing, management, supervision, and survivability functions for optical channels that carry client signals.

OTN has the following advantages over SDH and SONET:

- stronger forward error correction mechanisms
- more levels of tandem connection monitoring
- transparent transport of client signals
- switching scalability

13.2 Forward error correction

Forward error correction is a method to lower the BER of an optical line signal by adding redundant information, which can be used to correct bit errors that occur when the signal is transmitted over long distances.

The 5620 SAM allows the following forward error correction options for 1830 PSS devices:

- SDFEC
- AFEC
- UFEC
- RSFEC
- EFEC
- EFEC2

SDFEC provides higher error correction when compared to AFEC. The 130SCX10 OT card supports configuration of SDFEC on the line port.

The latency on the 11DPE12A, 11OPE8, 11QCE12X, and 11QPE24 cards is optimized by setting the FEC Mode parameter to No FEC under the Port Specifics tab of the respective Physical Port (Edit) forms.

13.3 OTN layers

The following layers are defined in OTN.

- OPU—information structure that is used to encapsulate client information for transport over an optical channel.
- ODU—consists of the OPU information payload and the ODU-specific overhead.
- OTU—information structure that is required to transport an ODU over an optical channel.
- OCH—an optical channel that transports a digital client signal between re-amplification, re-shaping, and re-timing (3R) regeneration points.
- OMS—provides multiplexing of several wavelengths.
- OTS—provides transmission of optical signals across various types of optical media.

13.4 Workflow to manage OTN trails

1 Configure the ODU trails; see Procedure 13-1.

If required:

- discover the services associated with the ODU trails; see Procedure 13-2.
- configure the path constraints for ODU trails; see Procedure 13-3.
- change the protection type of the ODU trails; see Procedure 13-4.
- configure the ODUCTPs; see Procedure 13-5.

2 Configure the OTU trails; see Procedure 13-6.

If required:

- auto-discover the OTU trails; see Procedure 13-7.
- discover the client trails from the OTU trails; see Procedure 13-8.

3 Configure the OCH trails; see Procedure 13-9.

4 Auto-configure the OMS trails; see Procedure 13-10.

5 View the OTS trails; see Procedure 13-11.

6 If required, discover the optical trails; see Procedure 13-12.

7 If required, view the optical channel usage; see Procedure 13-13.

13.5 OTN layer navigation using the 5620 SAM

The optical trail configuration forms allow you to create optical trails in the 5620 SAM. You can access the optical trail configuration forms from the Create menu or the Manage menu. Figures 13-1 and 13-2 show both methods of accessing optical trail configuration forms.

Figure 13-1 Optical trail configuration form navigation from Create menu

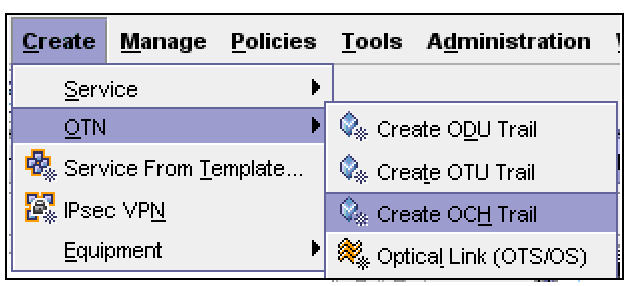
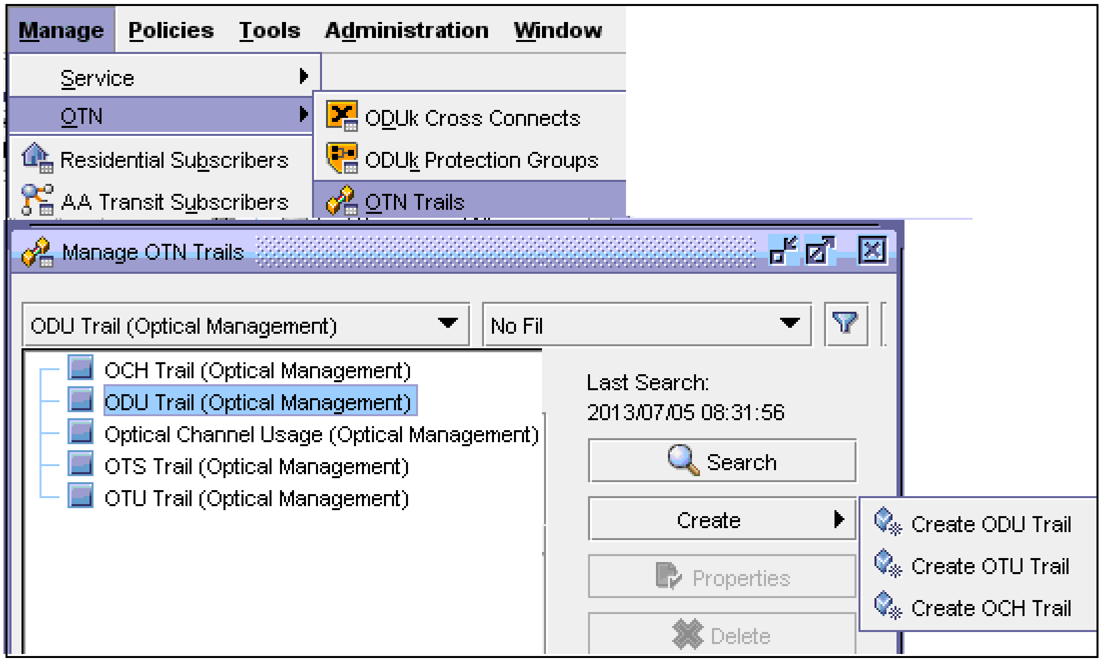


Figure 13-2 Optical trail configuration form navigation from Manage menu



The navigation tree of an optical trail configuration form lists the sites, termination points, and trail paths that are configured for the optical trail.

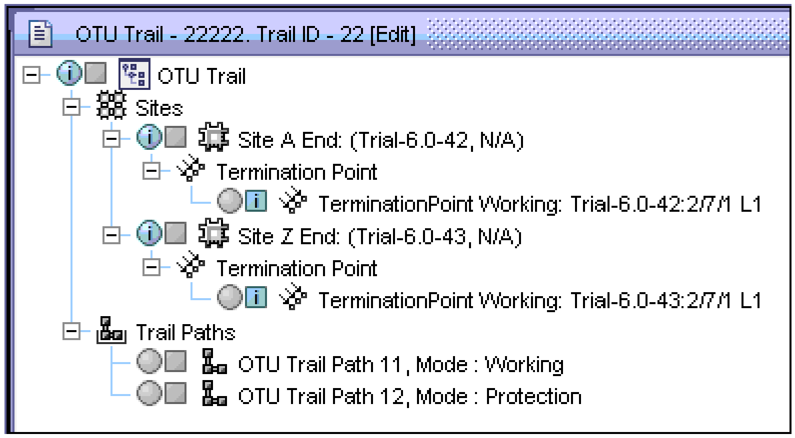
Table 13-1 describes the objects on the navigation tree of the optical trail configuration form, which the 5620 SAM allows you to create and manage.

Table 13-1 Navigation tree objects

Object	Description
Sites	Contains the Site A and Site Z attribute information
Site A End Site Z End	Child objects of the Sites object
Termination Point	Located under the Site A End and Site Z End objects. Contains the termination point attribute information.
Termination Point Working	Child objects of the Termination Point object.
Trail Paths	Contains the optical trail path attribute information.
<ODU/OTU/OCH> Trail Path, Mode: Working <ODU/OTU/OCH> Trail Path, Mode: Protection	Child object of the Trail Paths object.

Figure 13-3 shows the navigation tree objects that you can manage in the optical trail configuration forms.

Figure 13-3 Optical trail navigation tree objects



The 5620 SAM allows you to navigate to the underlying OTN layers from the Service or Trail Paths of the Optical Transport Service, Multipoint Transport Service, ODU Trail, and OTU Trail configuration forms. Figure 13-4 shows the trail hierarchy on the navigation tree of the Optical Transport Service form and Figure 13-5 shows the trail hierarchy on the navigation tree of the ODU Trail form.

Figure 13-4 OTN layer navigation from Optical Transport Service form

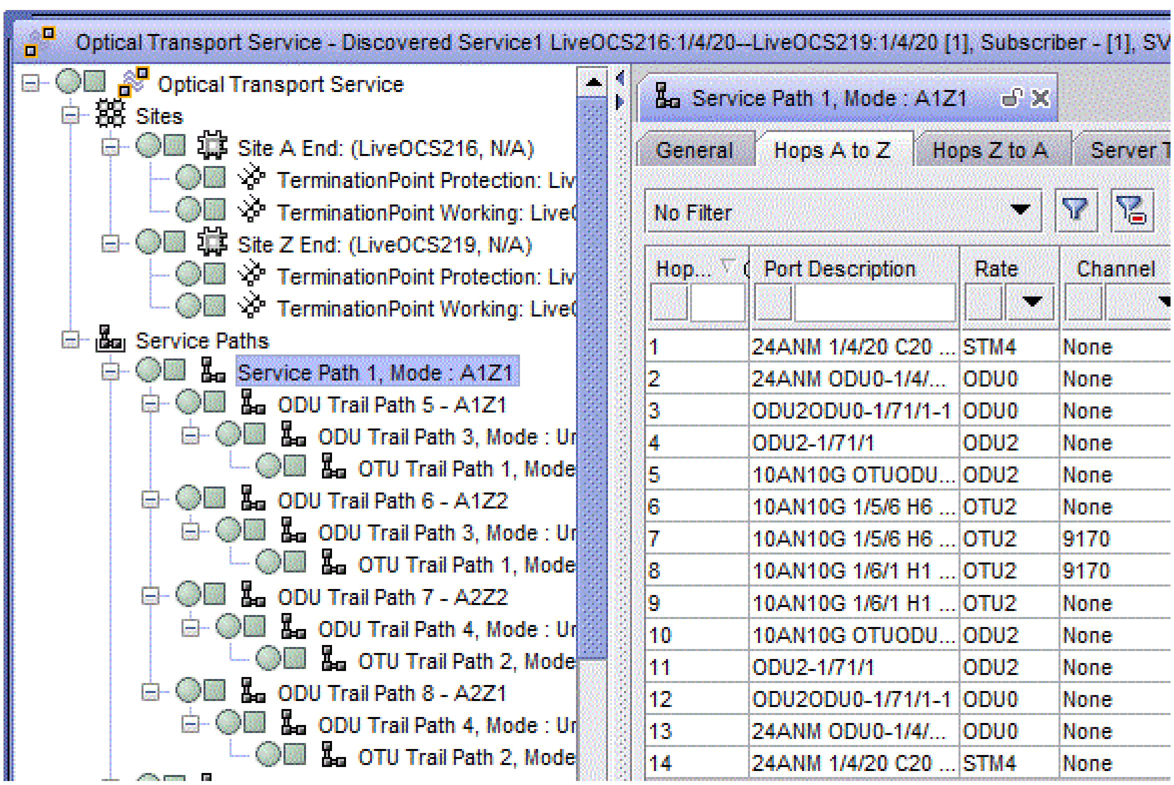
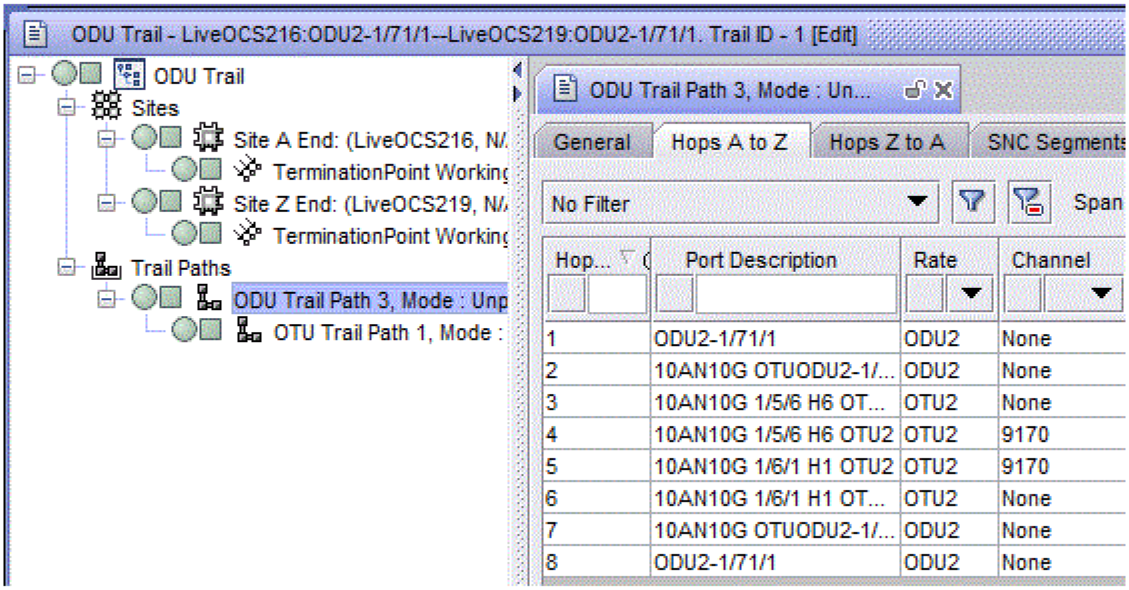


Figure 13-5 OTN layer navigation from trail ODU Trail form



13.6 Force XC creation

The 5620 SAM allows you to create OCH XCs even while the power commissioning is in progress. This option is available during the configuration of:

- OTU trails
- ODU trails
- OCH trails
- optical transport service
- multipoint transport service

During a service or trail configuration, you can enable the Force Create OCH XC check box on the configuration forms and bypass the check to ensure that the OCH XCs are successfully power commissioned.

Note — The 5620 SAM displays a deployment error if you attempt to configure a service or an optical trail when the power commissioning is in progress. The deployment error will not halt service or trail creation.

After a service or trail configuration, you can enable the Force Create OCH XC check box on the configuration forms and click Complete service or Complete Trail to complete the service or trail configuration.

13.7 Delay measurement for OTH path

The 5620 SAM allows you to initiate an on-demand delay measurement for an ODU trail. The following OTs can perform an on-demand delay measurement of ODU trails:

- 11QPA4
- 11QPEN4
- 112SDX11
- 130SCX10
- 130SNX10
- 260SCX2

To initiate a delay measurement, click More Actions on the ODU Trail (Edit) form and choose Delay Measurement→Start. Upon retrieval of the delay measurement values, the DM Current Status and the DM Current Value (us) parameters are updated in the ODU Trail (Edit) form.

To stop the delay measurement, click More Actions on the ODU Trail (Edit) form and choose Delay Measurement→Stop.

The line ports also display the following delay measurement parameters on the General tab of the Physical Port (Edit) form:

- Connection Monitoring End Point Mode
- DM Current Status
- DM Current Value (us)

The Connection Monitoring End Point Mode parameter can be set to ByPass, Source, or Destination. The value is set to ByPass by default.

13.8 Optical trail configuration procedures

Procedure 13-1 To configure an ODU trail

Ensure that the rate and transmit frequency are configured before creating the ODU trail.

1 Choose Create→OTN→ODU Trail from the 5620 SAM main menu. The ODU Trail (Create) form opens.

2 Select a customer in the Customer panel and configure the required parameters.

Note 1 — The Trail ID parameter is configurable when the Auto-Assign ID parameter is disabled.

Note 2 — If you configure the Protection Type parameter as Segment Protected, the Path Search Option parameter is set to User Defined by default and cannot be configured.

Note 3 — If you configure the Protection Type parameter as Segment Protected, the path constraints need to be configured. See step 12.

3 Configure the Wave Key Assign Mode parameter in the OTU/OCH Details panel.

4 Configure the required parameters in the ODUk Attributes panel.

5 Configure the required parameters in the TTI Attributes panel.

Note 1 — Configure the A-Z Source Tx TTI, Z-A Source Tx TTI, A-Z Destination Tx TTI, and Z-A Destination Tx TTI parameters for OCS nodes.

Note 2 — Configure the A-Z Transmitted TTI, Z-A Transmitted TTI, A-Z Expected TTI, and Z-A Expected TTI parameters for WDM nodes.

6 Configure the Administrative State parameter in the States panel.

7 Right-click on the Sites object on the navigation tree and choose Create Trail Site. The Select Network Elements - ODU Trail form opens with a list of 1830 PSS WDM and OCS devices.

8 Select two sites and click OK. The site objects appear on the navigation tree.

9 Right-click on the Site A End object on the navigation tree and choose Create Trail Termination Point. The Select Termination Point - ODU Trail form opens.

10 Choose the termination point and click OK. The termination point objects appear on the navigation tree.

11 Repeat steps 9 to 10 to configure the Site Z End.

12 Configure the path constraints, if required. See Procedure 13-3.

13 Click Apply. The form name changes to ODU Trail (Edit) form.

14 Expand the Trail Paths object on the navigation tree and click on the ODU Trail Path object to view the properties of the ODU trail.

15 Close the ODU Trail (Edit) form.

Procedure 13-2 To discover services associated with ODU trails

1 Choose Manage→OTN→OTN Trails from the 5620 SAM main menu. The Manage OTN Trails form opens.

2 Choose ODU Trail (Optical Management) from the object drop-down menu. A list of ODU trails appears.

3 Choose an ODU trail and click Properties. The ODU Trail (Edit) form opens.

4 Click on the Transported Services tab and click Discover Services. The service is listed in the ODU Trail (Edit) form and the Used By a Service check box of the Manage OTN Trails Form is selected.

5 Close the Manage OTN Trails form.

Procedure 13-3 To configure path constraints for ODU trails

1 Perform one of the following:

a To configure path constraints during an optical trail configuration:

i Configure an ODU trail. See Procedure 13-1.

ii Click on the Path Constraints tab on the ODU Trail (Create) form.

b To configure path constraints for an existing ODU trail:

i Choose Manage→OTN→OTN Trails from the 5620 SAM main menu. The Manage OTN Trails form opens.

ii Choose ODU Trail (Optical Management) from the object drop-down menu. The OTU trails are listed.

iii Choose an ODU trail and click Properties. The OTU/ODU/OCH Trail (Edit) form opens.

iv Click on the Path Constraints tab.

2 Click Create. The Optical Path Constraint (Create) form opens.

3 Configure the required parameters.

Choose Exclusion to exclude the constraint element from the trail path and choose Inclusion to include the constraint element in the trail path.

ODUk Rate is applicable only when the Constraint Element is ODUk Timeslot.

4 Configure the Service Path Type parameter for the Protected ODU trail.

5 Perform one of the following:

a If the constraint element is a port:

i Select a site on the Site panel.

ii Select a port on the Port panel.

b If the constraint element is a site, select a site on the Site panel.

c If the constraint element is a trail, select a trail on the Trail panel.

d If the constraint element is an ODUk timeslot:

i Configure the ODUk Rate parameter.

ii Select a site on the Site panel.

iii Select an ODUk Timeslot on the ODUk Timeslot panel.

e If the constraint element is an optical link:

i Select a site on the Site panel.

ii Select an optical link on the Optical Link panel.

6 Click OK. The Optical Path Constraint (Create) form closes and the ODU Trail (Edit) form reappears.

7 Click Apply to save the changes.

8 Expand the Trail Paths object on the navigation tree and expand the ODU Trail Path object.

9 Click on the Hops A to Z tab to verify the inclusion or exclusion of the path constraint.

10 Close the form.

Procedure 13-4 To modify the protection and route of an ODU trail

The 5620 SAM supports the following modifications of protection and route of the HO-ODU and LO-ODU trails:

- unprotected to SNCN protected
- SNCN protected to unprotected
- unprotected to SNCNC protected
- SNCNC protected to unprotected
- unprotected to segment protected
- segment protected to unprotected
- route modification for HO-ODU (OCS to OCS and OCS to 1830 PSS-32 in the intermediate nodes only)
- route modification for LO-ODU (OCS to OCS and OCS to 1830 PSS-32)

1 Choose Manage→OTN→OTN Trails from the 5620 SAM main menu. The Manage OTN Trails form opens.

2 Choose ODU Trail (Optical Management) from the object drop-down menu.

3 Choose an ODU trail and click Properties. The ODU Trail (Edit) form opens.

4 Configure the required parameters.

5 Configure the Protection Type parameter depending on the conversion from protected to unprotected or unprotected to protected.

Note — The modification of the Protection Type parameter results in the deletion of the APS groups.

6 Perform one of the following.

a Convert a segment protected, SNCN protected, or SNCNC protected ODU trail to an unprotected ODU trail, configure the Path Preference parameter to indicate the path that needs to be retained as the unprotected path.

b Convert an unprotected ODU trail to an segment protected, SNCN protected, or SNCNC protected ODU trail:

i Right click on the Site A End and choose Create Trail Termination Point. The Select Termination Point - ODU Trail form with a list of termination points opens.

ii Choose a termination point from the list and click OK. The Select Termination Point - ODU Trail form closes and the termination point is added to the ODU Trail navigation tree.

iii Perform steps i and ii on Site Z End and add termination point, as required.

7 Configure path constraints, as required. See Procedure 13-3 for more information about configuring the path constraints.

8 Click Apply.

9 Expand the Trail Paths object on the navigation tree to view the trail path attributes.

When you convert a protected ODU trail to an unprotected ODU trail, only the unprotected path object appears instead of the working and protection path objects

---

Procedure 13-5 To configure an ODUCTP

1 On the equipment tree, expand Network→1830 PSS→Shelf→Card→Line Port→ODU.

2 Right-click on the ODU object and choose Properties. The Odu Ctp (Edit) form opens.

3 Configure the required parameters in the ODUk Attributes panel.

4 Configure the required parameters in the TTI Attributes panel.

Note — You can enter the Transmitted TTI and Expected TTI values up to 15 characters for 1830 PSS devices and up to 64 characters for other devices.

5 Save your changes and close the form.

Procedure 13-6 To configure an OTU trail

Perform the following before creating an OTU trail.

- Configure the rate and frequency of the terminating sites.
- Create optical links between the terminating sites.

Note — The OTU trail is created automatically, when you configure an optical link between two OT line ports.

1 Choose Create→OTN→OTU Trail from the 5620 SAM main menu. The OTU Trail (Create) form opens.

2 Select a customer in the Customer panel and configure the required parameters.

Note — The Trail ID parameter is configurable when the Auto-Assign ID parameter is disabled.

3 Configure the required parameters in the OCH panel.

4 Configure the required parameters in the TTI Attributes panel.

Note 1 — Configure the A-Z Source Tx TTI, Z-A Source Tx TTI, A-Z Destination TTI, and Z-A Destination TTI parameters for OCS nodes.

Note 2 — Configure the A-Z Transmitted TTI, Z-A Transmitted TTI, A-Z Expected TTI, and Z-A Expected TTI parameters for WDM nodes.

5 Configure the Administrative State parameter in the States panel.

6 Right-click on the Sites object on the navigation tree and choose Create Trail Site. The Select Network Elements - OTU Trail form opens with a list of 1830 PSS devices.

7 Choose two sites from the list and click OK. The site objects appear on the navigation tree.

8 Right-click on the Site A End object and choose Create Trail Termination Point. The Select Termination Point form opens.

9 Choose the termination point and click OK. The Termination Point object appears on the navigation tree below the Site A End object.

10 Repeat steps 8 to 9 to configure the Site Z End.

11 Expand the Site A End and Site Z End objects on the navigation tree, to view the termination points added on the navigation tree.

12 Click Apply to save the changes. The form name changes to OTU Trail (Edit) form.

13 Expand the Trail Paths object on the navigation tree and click on the OTU Trail Path object to view the properties of the OTU trail.

14 Close the OTU Trail (Edit) form.

Procedure 13-7 To auto-discover an OTU trail

1 Configure internal topological links between the line port of a hybrid card (OCS) or OT card (WDM) and an SFC channel port. See Procedure 9-21 for more information about configuring topological links.

2 Configure an external topological link between the OMD ports of the participating OCS SFC cards. See Procedure 9-21 for more information about configuring topological links.

3 Choose Manage→OTN→OTN Trails from the 5620 SAM main menu. The Manage OTN Trails form opens.

4 Click Discover Optical Trails. The Discover Optical Trails form opens with a list of equipment groups.

5 Choose a equipment group and click OK. The OTN trails are listed in the Manage OTN Trails form.

6 Close the Manage OTN Trails form.

Procedure 13-8 To discover client trails from an OTU trail

When an OTU trail exists between the client port of a 130SCX10 card and a line port of a 11DPM12 card on the same device, you can discover the client trail from the OTU Trail (Edit) form.

1 Choose Manage→OTN→OTN Trails from the 5620 SAM main menu. The Manage OTN Trails form opens.

2 Choose OTU Trail (Optical Management) from the object drop-down list. A list of OTU trails appears.

3 Choose the required OTU trail and click Properties. The OTU Trail (Edit) form opens.

4 Click on the OTU Trail object on the navigation tree of the OTU Trail (Edit) form.

5 Click Discover Client Trails and click on the HO-ODU Trails tab. The discovered ODU trail is listed on the HO-ODU Trails tab.

6 Close the OTU Trail (Edit) form. The Manage OTN Trails form reappears.

7 Choose ODU Trail (Optical Management) from the object drop-down list. A list of ODU trails appears. The ODU trail discovered on the OTU Trail form is displayed in the list.

8 Close the Manage OTN Trails form.

Procedure 13-9 To configure an OCH trail

The following points should be considered before creating the OCH trail:

- Configure the rate, transmit frequency, and receive frequency of the terminating sites.
- Create optical links between the terminating sites.

1 Choose Create→OTN→OCH Trail from the 5620 SAM main menu. The OCH Trail (Create) form opens.

2 Select a customer in the Customer panel and configure the required parameters.

Note — The Trail ID parameter is configurable when the Auto-Assign ID parameter is disabled.

3 Configure the required parameters in the OCH panel.

4 Configure the Administrative State parameter in the States panel.

5 Right-click on the Sites object on the navigation tree and choose Create Trail Site. The Select Network Elements - OCH Trail form opens.

6 Choose two sites from the list and click OK. The site objects are added on the navigation tree.

7 Right click on the Site A End object on the navigation tree and choose Create Trail Termination Point. The Select Termination Point - OCH Trail form opens.

8 Choose the termination point and click OK. The termination point objects appear on the navigation tree.

9 Repeat steps 7 to 8 to configure the Site Z End.

10 Click Apply. The form names changes to OCH Trail (Edit) form.

11 Expand the Trail Paths object on the navigation tree and click on the OCH Trail Path object to view the properties of the OCH trail.

12 Close the OCH Trail (Edit) form.

Procedure 13-10 To auto-configure an OMS trail

1 Configure an internal topological link between the line port of a hybrid card in the OCS device and an SFC channel port in the same OCS device. See Procedure 9-21 for more information about configuring topological links.

2 Configure one of the following to auto-configure an OMS trail:

a an external topological link from the OMD port of the participating SFC card in the OCS device to the OMD port of an SFC card in another OCS device. See Procedure 9-21 for more information about configuring topological links.

b an external topological link from the OMD port of the participating SFC card in the OCS device to the OMD port of an SFC card in a WDM device. See Procedure 9-21 for more information about configuring topological links.

3 To view the auto-configured OMS trail, choose Manage→OTN→OTN Trails from the 5620 SAM main menu. The Manage OTN Trails form opens.

4 Choose OMS Trail (Optical Management) from the object drop-down menu. The auto-created OMS trail is listed.

Note — The OMS trails are deleted when the external topological links configured in step 2 are deleted.

5 Close the Manage OTN Trails form.

Procedure 13-11 To view an OTS trail

1 Choose Manage→OTN→OTN Trails from the 5620 SAM main menu. The Manage OTN Trails form opens.

2 Choose OTS Trail (Optical Management) from the object drop-down menu. A list of OTS trails appears.

3 Choose an OTS trail and click Properties. The OTS Trail (Edit) form opens.

Procedure 13-12 To discover optical trails

1 Choose Manage→OTN→OTN Trails from the 5620 SAM main menu. The Manage OTN Trails form opens.

2 Click Discover Optical Trails. The Discover Optical Trails form opens with a list of equipment groups.

3 Choose a equipment group and click OK. A list of optical trails in the group appears.

4 Close the Manage OTN Trails form.

Procedure 13-13 To view the optical channel usage

1 Choose Manage→OTN→OTN Trails from the 5620 SAM main menu. The Manage OTN Trails form opens.

2 Choose Optical Channel Usage (Optical Management) from the object drop-down menu. The optical channel usage list appears.

3 Choose a channel and click Properties. The Optical Channel Usage (View) form opens.

14 — 1830 PSS OTH facility management

14.1 OTH facility overview

The 5620 SAM supports auto-configuration of the following OTH facilities:

- OTUk
- ODUk
- OCH
- GBE
- OCN
- ODUPTF
- OMS
- OMSOCH
- OMSOCHIF
- OTS

14.2 Transmitted trail trace identifier

The 5620 SAM supports configuration of the following TTI parameters for the OTH facilities.

- Transmit SAPI—transmit source access point identifier, valid for terminated TCM only.
- Expected SAPI—expected incoming source access point identifier, valid for termination and non-intrusive monitoring.
- Transmit DAPI—transmit destination access point identifier, valid for terminated TCM only.
- Expected DAPI—expected incoming destination access point identifier, valid for termination and non-intrusive-monitoring.

Note — The NIM facility objects only have Expected SAPI and Expected DAPI.

The configurations of the TTI parameters can be performed using hexadecimal string format or quoted ASCII string format.

- Hexadecimal string format consists of 31 ASCII characters, that is, X followed by 30 hexadecimal characters. The 15 byte TTI encodes into 30 half-byte characters in hexadecimal format. The string starts after the all-zero header byte generated by the device.
- Quoted ASCII string format consists of 0-15 ASCII valid input characters. If the value consists of all ASCII NULLs, then 15 "." characters is displayed. See *Alcatel-Lucent 1830 Photonic Service Switch TL1 Commands and Messages Guide* for more information.

When the Region parameter on the Network Element (Edit) form is set to ETSI, the TTI parameters can be configured without any restrictions.

When the Region Parameter is set to ANSI and the Command Mode parameter is set to Normal on the Network Element (Edit) form, the TTI parameters cannot be configured. The Command Mode parameter needs to be set to Forced to configure the TTI parameters.

The STMN (STM1, STM4, STM16, STM64) facilities can be configured for the ETSI region nodes. The OCN facilities can be configured for the ANSI region nodes.

14.3 OTUk facility

The 5620 SAM auto-configures the OTUk facility object when the OTUk signal rate is configured on the line or client ports.

14.4 ODUk and NIM facilities

An ODUk entity is used for non-intrusive monitoring (NIM). NIM is a method for reporting defects and performance monitoring for an intermediate path on non-terminated add-drop and through connections.

The 5620 SAM supports the following ODUk facility objects in the physical and virtual planes of the OCS device as listed in Table 14-1. The facilities in the physical plane are associated with an OT or client/line card. The facilities in the virtual plane are associated with the internal shelf matrix. The object IDs for these facilities have slot number as 71.

Table 14-1 ODU facility objects on the 1830 PSS-32s device

ODU facility object	GUI naming convention	Example
Non-terminated HO-ODUs in the physical plane	OTUODUk-<shelf>/<slot>/<port>	OTUODU2-3/3/H1
Non-terminated LO-ODUs in the virtual plane	ODUmODUn-<shelf>/71/<HO-ODU#>-<LO-ODU#>	ODU4ODU1-1/71/1-3
Client-transparent ODUs	ODUk-<shelf>/<slot>/<client port>	ODU1-1/2/C1
Terminated HO-ODUs in the virtual plane	ODUk-<shelf>/71/<ODU#>	ODU4-2/71/1

Non-terminated ODUs

The 5620 SAM supports the following types of non-terminated ODU facilities:

- HO-ODU in the physical plane—OTUODUn
  The 5620 SAM auto-configures the HO-ODU facility object below the OTU facility object on the navigation tree, when the port is configured.
- LO-ODU in the virtual plane—ODUmODUn-(1-xx)-(1-xx)
  The 5620 SAM auto-configures the ODU facility when the terminated HO-ODU is auto-configured as a result of a cross-connect between a non-terminated HO-ODU and an ODUPOOL.

The 5620 SAM supports auto-configuration of the following NIM facilities when the signal rates of the I/O card ports are configured:

- 130SCUP, 130SCUPB, or 130SCUPC—OTU4 with an unterminated higher order ODU4 (higher order ODU4 NIM)
- 11QCUPC—OTU2 with an unterminated higher order ODU2 (higher order ODU2 NIM)
- 43SCUP—OTU3e2 with an unterminated higher order ODU3e2 (higher order ODU3e2 NIM)
- 10AN10G—OTU2 with an unterminated higher order ODU2 (higher order ODU2 NIM)
- 4AN10G—OTU2 with an unterminated higher order ODU2 (higher order ODU2 NIM).

Terminated ODUs

The 5620 SAM supports the following types of terminated ODU facilities:

- Client transparent ODU—ODUk

  The 5620 SAM auto-configures the ODU facility in the physical plane when a non-OTN port is configured.
- HO-ODU in the virtual plane—ODUk-(1-xx)

  The 5620 SAM auto-configures the ODU facility in the virtual plane when a cross-connect is configured between a non-terminated HO-ODU and an ODUPOOL.

14.5 ODUPTF facility

The 5620 SAM auto-configures the ODUPTF when a cross-connect is configured between a non-terminated ODUn and an ODUPOOL.

The 5620 SAM auto-configures the ODUPTF facility when a transparently transported GBE10, STM-64, OC-192, STM-16, OC-48, GBE is created.

14.6 OMS, OTS, OMSOCH, and OMSOCHIF facilities

The 5620 SAM auto-configures the OMSOCHIF on the SFC8 channel port when an internal bidirectional optical link is configured from a 10AN10G or a 4AN10G line port to the SFC8 channel port.

The 5620 SAM auto-configures the OMS, OTS, and OMSOCH facilities on the OMD port of the SFC8 OMD port when an internal bidirectional optical link is configured from a 10AN10G or a 4AN10G port to an SFC8 channel port and an external optical link is configured from the OMD port of the same SFC card to an SFC8 OMD port of a WDM or an OCS node.

14.7 OCH, GBE, and OCN facilities

The 5620 SAM auto-configures the OCH facility when the OCH signal rate is configured on the line or client ports.

The 5620 SAM auto-configures the GBE facility when 1, 10, or 100 GbE signal rates are configured on the line or client ports.

The 5620 SAM auto-configures the OCN facility when OC3, OC12, OC48, or OC192 signal rates are configured on the line or client ports.

14.8 ODUk cross-connection

The 5620 SAM allows you configure the ODUk cross-connect from:

- manage menu—parameter values are not inherited
- shelf object—the site and shelf parameter values are inherited from the current device

For more information about configuring an ODUk cross-connect, see Procedure 14-1.

The 5620 SAM auto-configures the HO-ODUs in the virtual plane when the cross-connects are configured between the non-terminated HO-ODUs and the ODUPOOLs. The ODUs are listed in the Virtual Plane tab of the Shelf (Edit) form. The 5620 SAM supports sub-structuring of the ODUs. See Procedure 14-2 for more information about sub-structuring the ODUs.

14.9 Management of ODUk cross-connect configuration

Procedure 14-1 To configure ODUk cross-connects

1 Perform one of the following to open the ODUk Cross Connect (Create) form.

a Open the ODUk Cross Connect (Create) form from the 5620 SAM main menu.

i Choose Manage→OTN→ODUk Cross Connects. The Manage ODUk Cross Connects form opens.

ii Click Create. The ODUk Cross Connect (Create) form opens.

iii Go to step 2.

b Open the ODUk Cross Connect (Create) form from the Shelf object on the navigation tree.

i On the equipment tree, expand Network→NE→Shelf.

ii Right-click on the Shelf object and choose Properties. The Shelf (Edit) form opens.

iii Click on the ODUk Cross Connects tab.

   iv Click Create. The ODUk Cross Connect (Create) form opens.

   v Go to step 4.

2 Select a site for the ODUk cross connect in the Site panel.

3 Select a shelf for the ODUk cross connect in the Shelf panel.

4 Configure the required parameters.

5 If A or Z end needs to terminate on the ODU pool, configure the Termination on ODUPOOL parameter for A or Z end.

6 Select an HO-ODU facility in the A-End and Z-End panels.

7 Save your changes and close the forms.

Procedure 14-2 To sub-structure ODUk timeslots

1 On the equipment tree, expand Network→NE→Shelf.

2 Right-click on the Shelf object and choose Properties. The Shelf (Edit) form opens.

3 Click on the Virtual Plane tab. The HO-ODUks are listed.

Note — The HO-ODUk is auto-configured in the virtual plane when a cross-connect is configured between an ODUPOOL and a non-terminated HO-ODU. See Procedure 14-1 for more information about configuring ODUk cross-connects.

4 Choose an HO-ODUk from the list and click Properties. The ODU Path Termination (Edit) form opens.

5 Click on the ODU Structure tab.

6 Choose the LO-ODUs based on the timeslot mapping in Table 14-2 and click Bind Timeslots. The LO-ODUk Configuration form opens.

Table 14-2 ODUk timeslot mapping

Auto-configured HO-ODUk	Rate	No of LO-ODUs to bind timeslots	No of timeslots	Size of the tributary slot
ODU2	ODU0	1 ODU0	1	1.25G
	ODU1	2 ODU0s	2	1.25G
		1 ODU01	1	2.5G

(1 of 2)

Auto-configured HO-ODUk	Rate	No of LO-ODUs to bind timeslots	No of timeslots	Size of the tributary slot
ODU3e2	ODU0	1 ODU0	1	1.25G
	ODU1	2 ODU0s	2	1.25G
	ODU2	8 ODU0s or 4 ODU1s	8	1.25G
	ODU2e	8 ODU0s or 4 ODU1s	8	1.25G
	ODU3	32 ODU0s, 16 ODU1s, or 4 ODU2s	32	1.25G
ODU4	ODU0	ODU0	1	1.25G
	ODU1	2 ODU0s	2	1.25G
	ODU2	8 ODU0s or 4ODU1s	8	1.25G
	ODU2e	8 ODU0s or 4ODU1s	8	1.25G
	ODU3	31 ODU0s	31	1.25G

(2 of 2)

7 Configure the required parameters and click OK.

8 Scroll to the bottom of the list to view the newly created timeslot.

9 Choose a bound timeslot and click Collapse Timeslots to retrieve the initial timeslots.

10 Save your changes and close the forms.

14.10 ODUk protection groups

The 5620 SAM supports the configuration of the ODUk protection groups. The ODUk protection group represents a path protected cross-connection in the 5620 SAM. The ODUk protection group can be configured for the rate facilities:

- ODUPOOL
- ODUk NIM
- client transparent ODUk

The ODUPOOL path terminated entity is configured as the client facility of the ODUk protection group.

The protected and protecting ingress POMs (Path Overhead Monitoring) needs to be enabled when the ODUk protection group is configured using the ODUk NIM entities. See Procedure 14-3 for more information about configuring the POMs.

The working and protecting facilities must be configured as the client transparent ODUk facilities, to configure an SNCNC protection type of ODUk protection group. The client transparent facilities can be configured as working and protecting, if they are configured with the SDH or SONET signals rates.

The 5620 SAM allows you configure the ODUk protection groups from the:

- manage menu
- OCS device object
- shelf object (by choosing the unprotected cross-connect)
- port object
- ODU facility object

For more information about configuring a protection group, see Procedure 14-4.

The 5620 SAM supports configuration of protection switching to configure either the working or protection path as active or standby. See Procedure 14-5 for more information about configuring a protection switch.

14.11 Management of ODUk protection groups

Procedure 14-3 To configure ingress path overhead monitoring

1 On the equipment tree, expand Network→1830 PSS→Shelf→Port.

2 Right-click on the port object and choose Properties. The Physical Port (Edit) form opens.

3 Click on the OTUODUk tab, then on the NIM tab. The OTUODU2 source and sink entries are listed.

4 Choose the sink and click Properties. The ODU NIM Point (Edit) form opens.

5 Select the Path Overhead Monitoring check-box and click OK.

6 Save your changes and close the forms.

Procedure 14-4 To configure ODUk protection groups

1 Perform one of the following to open the ODUk Protection Group (Create) form.

a Open the ODUk Protection Group (Create) form from the 5620 SAM main menu.

i Choose Manage→OTN→ODUk Protection Groups. The Manage ODUk Protection Groups form opens.

ii Click Create. The ODUk Protection Group (Create) form opens.

iii Go to step 2.

b Open the ODUk Protection Group (Create) form from the equipment tree.

i On the equipment tree, expand Network→1830 PSS.

ii Right-click on the 1830 PSS object and choose Properties. The Network Element (Edit) form opens.

iii Click on the APS Groups tab.

iv Click Create and choose ODUk APS Group. The ODUk Protection Group (Create) form opens.

v Go to step 4.

c Open the ODUk Protection Group (Create) form from the list of ODUk cross-connects on a shelf object or an ODU facility object.

i On the equipment tree, expand Network→NE→Shelf object or Network→NE→Shelf→Card→Port→ODU facility object.

ii Perform one of the following:

- Right-click on the Shelf object and choose Properties. The Shelf (Edit) form opens.
- Right-click on the ODUk object and choose Properties. The ODU Path Termination (Edit) form opens.
- Right-click on the OTUODUk object and choose Properties. The ODU NIM (Edit) form opens.

iii Click on the ODUk Cross Connects tab.

iv Choose an unprotected ODUk cross-connect and click Protect. The ODUk Protection Group (Create) form opens.

v Go to step 10.

d Open the ODUk Protection Group (Create) form from the port object on the navigation tree.

i On the equipment tree, expand Network→1830 PSS→Shelf→Port.

ii Right-click on the port object and choose Properties. The Physical Port (Edit) form opens.

iii Click on the APS Groups tab.

iv Click Create and choose ODUk APS Group. The ODUk Protection Group (Create) form opens.

e Open the ODUk Protection Group (Create) form from the ODU facility object on the navigation tree.

i On the equipment tree, expand Network→NE→Shelf→Card→Port→ODU object.

ii Perform one of the following:

- Right-click on the ODUk object and choose Properties. The ODU Path Termination (Edit) form opens.

Note — Ensure that the selected facilities are SONET or SDH rates, if you are configuring client transparent facilities for the working and protection parameters.

- Right-click on the OTUODUk object and choose Properties. The ODU NIM (Edit) form opens.

Note — Ensure that the ingress POM is configured before configuring the ODUk protection group for the ODUk NIM entities. See Procedure 14-3 for more information about configuring the ingress POM.

iii Click on the APS Group tab.

iv Click Create. The ODUk Protection Group (Create) form opens.

2 Click Select beside the Name parameter in the Site panel. The Select Site - ODUk Protection Group form opens with a list of 1830 PSS devices.

3 Choose a site and click OK. The Select Site - ODUk Protection Group form closes and the ODUk Protection Group (Create) form reappears with the site information in the Site panel.

4 Click Select beside the Shelf ID parameter in the Shelf panel. The Select Shelf - ODUk Protection Group form opens.

5 Choose a shelf and click OK. The Select Shelf - ODUk Protection Group form closes and the ODUk Protection Group (Create) form reappears with the shelf information in the Shelf panel.

6 Perform one of the following:

a Configure the Client on ODUPOOL parameter. Go to step 8.

b Click Select beside the Name parameter in the Client panel. The Select Client - ODUk Protection Group form opens. Go to step 7.

7 Choose a client and click OK. The Select Client - ODUk Protection Group form closes and the ODUk Protection Group (Create) form reappears with the client information in the Client panel.

8 Click Select beside the Name parameter in the Working Facility panel. The Select Facility - ODUk Protection Group form opens.

Note — Configure the working facility as HO-ODU NIM, if the Client on ODUPOOL parameter is configured.

9 Choose an ODU facility and click OK. The Select Facility - ODUk Protection Group form closes and the ODUk Protection Group (Create) form reappears with the ODU facility information in the Working panel.

10 Click Select beside the Name parameter in the Protection Facility panel. The Select Facility - ODUk Protection Group form opens.

Note — Configure the protection facility as HO-ODU NIM, if the Client on ODUPOOL parameter is configured.

11 Configure the Protection Method parameter.

Note 1 — Configure the Protection Method parameter as PNIM if the protection type is SNCN or SNCNC.

Note 2 — Configure the Protection Method parameter as PADAPT for SNCI protection type.

12 Choose an ODU facility and click OK. The Select Facility - ODUk Protection Group form closes and the ODUk Protection Group (Create) form reappears with the ODU facility information in the Protection panel.

13 Configure the required parameters in the APS Configuration panel.

Note — Configure the Protection Type parameter as SNCNC, if client transparent ODU facilities are configured as working and protection facilities.

14 Save your changes and close the form.

Procedure 14-5 To configure protection switching

1 Perform one of the following to open the ODUk Protection Group (Edit) form.

a Open the ODUk Protection Group (Create) form from the 5620 SAM main menu.

i Choose Manage→OTN→ODUk Protection Groups. The Manage ODUk Protection Groups form opens.

ii Choose a protection group and click Properties. The ODUk Protection Group (Edit) form opens.

b Open the ODUk Protection Group (Create) form from the 1830 PSS device object on the equipment tree.

i On the equipment tree, expand Network→1830 PSS.

ii Right-click on the 1830 PSS object and choose Properties. The Network Element (Edit) form opens.

iii Click on the APS Groups tab.

iv Choose an entry and click Properties. The ODUk Protection Group (Edit) form opens.

c Open the ODUk Protection Group (Create) form from the port object on the equipment tree.

i On the equipment tree, expand Network→1830 PSS→Shelf→Port.

ii Right-click on the port object and choose Properties. The Physical Port (Edit) form opens.

iii Click on the APS Groups tab.

iv Choose an entry and click Properties. The ODUk Protection Group (Edit) form opens.

d Open the ODUk Protection Group (Create) form from the ODU facility object on the equipment tree.

i On the equipment tree, expand Network→NE→Shelf→Card→Port→ODU object.

ii Perform one of the following:

- Right-click on the ODUk object and choose Properties. The ODU Path Termination (Edit) form opens.
- Right-click on the OTUODUk object and choose Properties. The ODU NIM (Edit) form opens.

iii Click on the APS Group tab.

iv Choose an entry and click Properties. The ODUk Protection Group (Edit) form opens.

2 Configure the required parameters in the Protection Management panel.

Note — Configure the Request For parameter to specify the path that needs to be switched.

3 Save your changes and close the form.

14.12 Virtual OCH cross-connections

The 5620 SAM auto-configures a virtual OCH cross-connection when an internal topological link is configured from a line port of the client-line card to a channel port of an SFC8 card. The virtual cross-connections that are auto-configured for an OCS node are listed on the OCH Cross-Connects tab on the Network Element (Edit) form. You can choose an entry and click Properties to open the Virtual Cross Connect (Edit) form.

The 5620 SAM auto-configures working and protection virtual OCH cross-connections during trail (OCH, OTU, or ODU) or service configuration or discovery, involving:

- OPSA card that is configured with the OCHP mode and located in one node with the OPSA A and B ports connected to the filter card in an another node
- OPSA card that is configured with the OMSP mode and located in one node with the OPSA A and B ports connected to the OPSA A and B ports on another node.

1830 PSS service management

15 — 1830 PSS VPLS management

15.1 VPLS management overview

VPLS is a class of virtual private network multipoint L2 service that provides connections to multiple customer sites in a single bridged domain contained within the service provider-managed IP/MPLS network. A VPLS service provides connectivity between two or more SAPs. Customer sites in the VPLS appear to be on the same LAN, even when the sites are geographically dispersed.

The 5620 SAM supports configuration of VPLS service on the following cards:

- 11OPE8
- 11QCE12X
- 11QPE24

The following conditions apply for the VPLS service configured using the L2 cards.

- VPLS is configured at the card level (and not at the NE level).
- A VLAN ID is only applicable when the SAP type is dot1q-preserve.
- A VPLS cannot be deleted if SAPs are defined for the service.

SAP

Each subscriber service type is configured with a minimum of one service access point (SAP). A SAP identifies the customer interface point for a service. The 5620 SAM supports SAPs for the following cards:

- 11OPE8
- 11QCE12X
- 11QPE24

The SAP configuration requires that slot and port information be specified. The slot and port parameters must be configured prior to provisioning a service. A SAP is a local entity to the cards and is uniquely identified by:

- physical Ethernet port or LAG
- encapsulation identifier (ID)

Depending on the port encapsulation, a physical port can have one or more SAPs associated with it. The SAPs are created on ports designated as access or uplink. The 5620 SAM supports the following port encapsulations on access Ethernet ports:

- Null—supports a single service on the port
- Dot1Q—supports multiple services for one or more customers.
- Q in Q—adds an IEEE 802.1ad or 802.1Q tag to the 802.1Q tagged packets entering the access port to expand the VLAN space, producing a double-tagged frame.

The 5620 SAM supports only Q in Q encapsulation on the uplink ports.

Service SAP types

VPLS service requires a service SAP type that specifies the SAPs configured in the service. The following SAP types are supported by the 5620 SAM:

- null-star—choose the option if the SAP in the service can be Null, Dot1Q or Q in Q.
- dot1q-preserve—choose the option if the SAP in the service is Dot1Q. The Dot1Q ID is retained after packets match the SAP.
- any—choose the option if the system processes and forwards only packets with no VLAN tag. All other packets with one or more VLAN tags are not processed are dropped.

15.2 Configuring a VPLS Service

The following needs to be configured for a basic VPLS service:

- Customer ID
- two SAPs specifying access port, uplink port, and encapsulation values.

Procedure 15-1 To create a VPLS

1. Choose Create→Service→VPLS from the 5620 SAM main menu. The VPLS Service (Create) form opens.
2. Select a customer to associate with the VPLS.
3. Configure the required general service parameters.
4. On the equipment tree, right-click on the Sites object and choose Create VPLS Site. The Select Network Elements - VPLS Service form opens with a list of available sites.
5. Choose a site and click OK. The Select ELAN Elements form opens with a list of supported cards.
6. Choose a card and click OK. The VPLS Site (Create) form opens and the VPLS site information is updated in the Network Element panel.
7. Configure the required general VPLS site parameters.
8. If you configure the SAP Type parameter to dot1q-preserve in Step 7, configure the Customer VID parameter.
9. If you want to configure MC LAG, select the Enable MC LAG Binding check box.
10. Click OK. The VPLS Site (Create) form closes and the VPLS Service (Create) form opens.
11. Click Apply to save the changes.

12 Click on the newly created Site object on the equipment tree to view the following:

- The Forwarding Control tab displays the MFIB, FIB, and L2 Access Interface FIB information.
- The Multicast tab displays the IGMP Snooping parameters.
- Statistics, scripts, and fault information is available from the appropriate tabs.

13 Right-click on the VPLS Service→Sites→Site→L2 Access Interfaces object on the VPLS service tree and choose Create VPLS L2 Access Interface. The VPLS L2 Access Interface (Create) form opens.

14 Configure the required general VPLS L2 access interface parameters.

15 Select a SAP TCA profile.

16 Click on the Port tab.

17 Select a terminating port for the L2 access interface.

18 Select an Ethernet ring for the L2 access interface.

19 Configure the Enable Split Horizon parameter, if required.

Note 1 — Enabling the split horizon parameter creates a split horizon group for the VPLS instance.

Note 2 — Ensure that the Enable Split Horizon parameter is configured for the inter-connect site during the manual configuration of a control service for a virtual sub-ring.

20 Click on the IGMP Snooping tab and then on the General sub-tab and configure the required parameters.

21 Click on the Static Mcast Group sub-tab and click Create. The Access Interface Igmp Snooping Mcast Group Display (Create) form opens.

22 Configure the parameters, save the changes and close the forms.

23 Click on the newly created VPLS L2 Access Interface object on the navigation tree to view the following:

- The Forwarding Control tab displays the FIB information.
- The IGMP Snooping tab displays the IGMP Snooping parameters
- The port tab displays the terminating port, encapsulation type, Ethernet ring, and LLF values.
- The QoS tab displays the QoS policy information.
- Statistics, scripts, and fault information is available from the appropriate tabs.

15.3 Split horizon group

An SHG prevents loops in the network by not allowing traffic in one SAP to be forwarded to other members of the group in the same service. The 5620 SAM supports the configuration of SHGs on the following cards:

- 11QPE24
- 11OPE8
- 11QCE12X

You can add ports and LAGs to an SHG. A LAG member cannot be added to the group and the ports in a group cannot become a LAG member. A port and a LAG can only be in one SHG.

Procedure 15-2 To configure an SHG

1 On the equipment tree, expand Network→1830 PSS→Shelf→Card.

2 Right-click on the Card object and choose Properties. The Card Slot (Edit) form opens.

3 Click on the Split Horizon Groups tab, then click Create. The Split Horizon Group (Create) form opens.

4 Configure the required parameters.

5 Save your changes and close the forms.

Procedure 15-3 To add ports to an SHG

The following conditions must be met before you add a port to an SHG:

- The Assigned Rate parameter must be configured on the port.
- The port must not be used in a service.
- The port must be in the Shut Down state.

1 On the navigation tree, expand Network→1830 PSS→Shelf→Card→Port.

2 Right-click on a port where the SHG is configured and choose Properties. The Physical Port (Edit) form opens.

3 Select an SHG in the Split Horizon Group panel and click OK. The Select Split Horizon Group form closes and the Physical Port (Edit) form reappears.

4 Repeat steps 2 to 3 for each additional port that you need to assign to the SHG.

5 Save your changes and close the form.

15.4 E-Tree services

An E-Tree service is a type of Ethernet service that is based on a rooted-multipoint Ethernet virtual connection. An E-Tree service provides a single root for multiple leaf UNIs. Each leaf UNI exchanges data with only the root UNI. A service frame sent from one leaf UNI with a destination address for another leaf UNI is not delivered. The E-Tree service is used for Internet access or video over IP applications, such as multicast or broadcast packet video.

The 5620 SAM supports E-Tree configurations consisting of:

- roots—VPLS service with SAPs not in an SHG
- leaves—VPLS service with SAPs in an SHG

See Procedure 15-1 for more information about configuring a VPLS service and Procedure 15-2 for more information about configuring an SHG. The 5620 SAM supports the following E-Tree services:

- EP-Tree—Ethernet private tree service on the ports that are null-encapsulated
- EVP-Tree—Ethernet virtual private tree service on ports that support other services such as EVPL or EVP-LAN

An E-Tree root can be on the same card as the leaves, or on a different card. There can be more than one root in the network for redundancy. The leaves of the E-Tree are configured on one card in the network to provide the required isolation. The leaf ports are in the same SHG and leaf SAPs are in the same service as that of the leaves and roots. The E-Tree functions are described in Table 15-1.

Table 15-1 E-Tree functions

Function	Description
E-Tree with ERP	The E-Tree is configured over ERP with leaf ports on one node and roots on one or more other nodes.
E-Tree with LAG	The E-Tree leaves are LAGs, or individual ports, or both. The roots are individual ports or LAGs. The roots can be members of an MC LAG.
E-Tree with CFM	Monitoring of an E-Tree is performed using up-MEPs on each root and leaf SAPs in the same association. On the card with the leaves, the CFM association has only the roots listed as remote MEPs. On a card with a root, the association has the leaves and other roots listed as remote MEPs. CFM monitoring is not required when roots and leaves are in the same card.
E-Tree with IGMP snooping	IGMP snooping is used on E-Tree leaves to further optimize the tree for specific multicast groups.

15.5 IGMP Snooping

The 5620 SAM supports the configuration of the IGMP Snooping parameters for a VPLS service. See Procedure 15-1 for more information about configuring a VPLS service.

IGMPv2

IGMP is a multicast protocol that service providers can use to establish multicast group memberships on a LAN. Within the LAN, end users use IGMP to communicate with a local multicast router, which then uses PIM to distribute the IGMP messages to other local and remote multicast routers. Multicast routers send regular membership queries to IGMP hosts which respond with membership reports. Multicast routers can use the reports to determine which hosts are interested in receiving specific multicast messages. The IGMP operates above the network layer on IPv4 networks. See the section, "IGMP configuration procedures" in the *5620 SAM User Guide* for more information about how to configure IGMP.

16 — 1830 PSS optical transport service management

16.1 Optical transport services overview

An optical transport service is a wavelength that traverses the network between two endpoints, which can be tandem wavelengths in some cases. The path that the service takes through the network is defined by the 5620 SAM using shortest path algorithm and the NE adjacencies.

The 5620 SAM supports the configuration of a WDM node with an OCS uplink card. The configuration is supported with DWDM FOADM, ROADM, and TOADM nodes. The following OCS card types are supported:

- 11QCUP—One-degree FOADM
- 11QCUPC—FOADM, ROADM, and TOADM
- 130SCUP—FOADM, ROADM, and TOADM

The connection between a DWDM node and an uplink card is supported on the following port types:

- SFD channel ports (FOADM, ROADM, and TOADM configurations)
- CWR8 and CWR8-88 CLS ports (TOADM configurations)

The cross-connect provisioned for this configuration terminates on the SFD or CWR port, because the uplink card is not managed by the WDM system.

An XC is the path that the service takes through an NE. A cross-connect is defined by the ingress and egress points for the service on the NE. The NE physical topology defines the internal path that the service takes through the NE.

The 5620 SAM supports the following:

- identification of adjoining XCs and management of linked XCs as an optical transport service
- creation, deletion, and discovery of optical transport services, when there are no XCs
- discovery of optical transport service between OTs of the vendor network

Each service is assigned a trail identifier and a pair of Wavelength Tracker wave keys. The trail identifier and ITU channel number (wavelength) and wave key pair, are unique in the network. See Tables 19-3, 19-4, and 19-5 for wave key information.

Because optical transport services create transport connectivity between router ports, they must be created before IP services. Services are created by selecting the endpoints. See Procedures 16-1 and 16-2 to create services. The 5620 SAM supports optical transport services between:

- two 1830 PSS devices
- two non-1830 PSS devices, that is, 7750 SR, 7450 ESS, 7705 SAR, 7210 SAS, and 7950 XRS
- an 1830 PSS device and a non-1830 PSS device, that is, 7750 SR, 7450 ESS, 7705 SAR, 7210 SAS, and 7950 XRS

SR-SR optical transport service and trail

During the SR-SR ODU and OTU trail configurations, the TTI attributes are available for configuration only for the OTU-enabled SR ports. The TTI attributes configured during the trail configuration can also be viewed on the Optical Transport Channel Unit tab of the Physical Port (Edit) form for the OTU-enabled SR ports.

Highlight services and trails on physical topology map

The 5620 SAM allows you to highlight the service, trail, or path on the physical topology map to indicate working, protection, nominal, actual and alarm status. Click Navigate on the trail or service configuration form and choose Physical View : Highlight Path to open the physical topology map with the highlights. Click Legend and choose Highlight Sessions to view the highlight sessions for the current map. See the *5620 SAM User Guide* for more information about the highlight function in the 5620 SAM.

16.2 Optical protection

The 5620 SAM supports the following protection types:

- Diverse route protection. See Section 16.3
- ESNCP protection. See Section 16.4
- OPS protection. See Section 16.5
- Y-Cable protection. See Section 16.6
- Client protection. See Section 16.7

Protection level

Services or trails display the protection level as Unprotected, Protected or Segment Protected on the service and trail configuration forms.

The protection level is displayed as Protected if the service or trail is protected by ESNCP, Y-Cable or OPS, or if all server connections of the service or trail are protected. If only a few or none of the server connections are protected, the protection level of the service or trail is displayed as Unprotected and Segment Protected respectively.

16.3 Diverse route

A diverse route service involves an optical transport service originating at one site with two diverse routes and terminating at two different destinations.

Diverse route services can only be created by using the 5620 SAM and the services are not part of the service discovery operation.

If you unmanage a diverse route and run the discover transport services operation, the 5620 SAM discovers two unprotected services instead of a diverse route service.

16.4 ESNCP

ESNCP is a line side (network side) protection mechanism which protects against loss of the line signal due to an OTM failure, fiber interruption, or a malfunction of an intermediate NE node. The 5620 SAM supports ESNCP protection on the following OTs:

- 4DPA2
- 4DPA4
- 10SD10G
- 11DPE12
- 11DPE12A
- 11DPE12E
- 11DPM12
- 11QPA4
- 11QPEN4
- 24SDM

ESNCP protection is implemented by permanent head-end bridging and dynamic tail-end selection.

The 5620 SAM supports ESNCP across mate 11DPE12A cards. LAG is available on a single card and cannot be used in conjunction with ESNCP across cards.

16.5 OPS protection

The OPS cards provide photonic protection switching in DWDM configurations for channels supported in the C-band, allowing users to provide 1+1 APS protection. There are two types of OPS cards:

- OPSA
- OPSB

The following are the protection modes for the OPSA card:

- OLP
- OCHP
- OMSP

For OPS protected service provisioning, you can only specify the following ports as termination points:

- 11STAR1 client port
- 11STAR1A client port
- 11STGE12 client port
- 11STMM10 client port
- 11QPA4 client port
- 11QPEN4 client port
- 112SNX10 client port
- 112SNA1 client port
- 112SCA1 client port
- 112SCX10 client port
- 112SNA1 client port
- 112SCA1 client port
- 260SCX2 client port
- OPSA SIG

OCHP

The Protection Mode parameter on the Card Specifics form of the OPSA card is OCHP by default. The Assigned Rate parameter for the SIG, A, and B ports is OCH. See Procedure 16-19 to configure an OCHP protected service. The following OT cards support OCHP protection:

- 112SCA1
- 112SNA1
- 112SCX10
- 112SNX10
- 130SCX10
- 130SNX10
- 260SCX2

OLP

The Protection Mode parameter on the Card Specifics form of the OPSA card is set to OLP. The Assigned Rate parameter for the SIG, A, and B ports is OTS. The OLP is a 1+1 protection type that provides two separate fiber connections between adjacent network elements. The OLP provides optical bridging at the source end and switch selection of one of the two signals at the receiving end. The 5620 SAM supports OLP as the protection type for 1830 PSS-32 and 1830 PSS-16 in the ROADM configuration using WR2-88, WR8-88A, and WR8-88AF. The OLP is supported with manual power management. The following OT cards support OLP protection:

- 112SNA1
- 112SNX10
- 11STAR1A
- 11DPM12
- 11DPE12A
- 11DPE12E
- 11QPA4

See Procedure 16-20 to configure an OLP protected service.

OMSP

The Protection Mode parameter on the Card Specifics form of the OPSA card is set to OMSP. The Assigned Rate parameter for the SIG, A, and B ports is OTS. When the OPSA card is used in OMSP protection mode, in the transmit direction, the SFD and ITLB total output channels are separated into two optical multiplex sections routed to different DWDM lines. In the receive direction, the OPSA selector selects one of the two lines as the active path based on power monitoring or manual selection.

The 5620 SAM support for OMSP protection includes:

- configuration of OMSP protection on the OPSA cards. See Procedure 9-5 for information about configuring OMSP protection on the OPSA card.
- creation of OMSP protected service for FOADM configuration.

  See Procedure 16-18 for information about configuring an optical transport service.

  See Procedure 16-23 for information about configuring an optical transport service using 112SDX11 card.

The following SFDs and ITLB cards are supported with OMSP protection:

- SFD-5
- SFD-8
- SFD-40
- ITLB
- SFD-40B
- SFD 44
- SFD 44B

The following OT cards support OMSP protection:

- 112SCX10
- 11QPA4
- 11STAR1
- 112SDX11
- 11STMM10
- 11DPM12
- 11QPEN4

Note — See section 16.19 for more information about service configuration and OTN layer management of the 112SDX11 card.

OPSB

OPSB is an optical protection switch card supporting client-side OPS protection. The OPSB card uses non-latching switch, which means that upon power failure, the OPSB automatically switches back to the default path. The protection mode for the OPSB card is OTUP.

When a pair of transponder cards are part of a client-side OPS protection configuration, the following rules apply.

- The assigned rate, frequency, and OPR mode parameters need to be the same at the client ports of the working and protection OTs.
- The LOS propagation mode is set to LASER OFF.
- The encapsulation mode can be the same or different at the client ports of the working and protection OTs.
- The frequencies supported at the client port that connects to OPSB A and B ports are 1310 nm and 1550 nm.
- When the pair of OTs are 112SCA1 or 112SNA1 cards, and the clients are provisioned for 100 GbE, the errored frame drop mode and LOS propagation parameters need to be the same for both cards.
- When the pair of OTs are 112SCA1 or 112SNA1 cards, and the clients are provisioned for OTU4 signal rate, the FEC Mode and TTI (at both the OTU4 and ODU4 layers) parameters need to be the same for both cards.

The 5620 SAM support for client-side OPS protection includes:

- configuration of client-side OPS protection on the OPSB cards. See Procedure 9-6 for information about configuring client-side OPS protection on the OPSB cards.
- creation of client-side OPS protection service using the OPSB cards. See Procedure 16-17 for information about creating the client-side OPS protected optical transport service.
- creation of client-side OPS protection service using the OPSB card linked to an OT of an 1830 PSS device and another OT of a third-party device. The OT of the 1830 PSS device is linked to the A port of the OPSB card and the OT of the third-party device is linked to the B port of the OPSB card.

Note — The third-party device is transparent to 5620 SAM. Hence an optical link needs to be created from the B port of OPSB card of an 1830 PSS device to the B port of the OPSB card of another 1830 PSS device.

The following OT cards support client-side OPS protection:

- 11QPA4
- 11STAR1
- 11STAR1A
- 11STMM10
- 112SNA1
- 112SCA1
- 130SCA1
- 260SCX2

The following combinations of OTs as working and protection are supported in the client-side OPS protection:

- 11STAR1 with 11STAR1
- 11STAR1A with 11STAR1
- 11STAR1A with 11STAR1A
- 130SCA1 with 130SCA1
- 130SCA1 with 112SNA1
- 130SCA1 with 112SCA1
- 130SCA1 with 260SCX2
- 11STMM10 with 11STMM10
- 112SNA1 with 112SNA1
- 112SCA1 with 112SCA1
- 11QPA4 with 11QPA4
- 11QPA4 with 11STAR1
- 11QPA4 with 11STAR1A
- 260SCX2 with 260SCX2

16.6 Y-cable protection

The Y-cable protection is a network side protection mechanism that protects the line card, client side laser, network side laser, and network side fibers. The protection is based on a pair of OT cards at the near end and far end of the network. The protection can be used with any supported type of OT, but the near-end working OT must be connected to the far-end working OT and the near-end protection OT must be connected to the far-end protection OT. The working and protection ports must be provisioned for the same signal rate, and format and must be configured with the same threshold values at both ends of the network.

Note 1 — The working and protection OTs must be the same type. The 5620 SAM does not allow service creation when card types are different.

Note 2 — The near-end and far-end OTs must be the same type. The 5620 SAM allows service creation when card types are different.

- 11DPM12
- 11QPEN4
- 112SCX10
- 130SCX10
- 11QPA4

Y-cable support on working and protection OTs

43SCX4E card

The Y-cable protection is supported on the 43SCX4E OT card. The 43SCX4E is a double width variant, full height card that is supported on the 1830 PSS-32. The card is similar in functionality to the 43SCX4 card.

11QPEN4 card

The Y-cable protection is supported on the 11QPEN4 OT card. The working and protection OTs must be the same type at the near and far end. For example, there must be an 11QPEN4 card at each end, and near-end port C1 must be connected to the far-end port C1. The same applies to port C2. Unidirectional Y-cable is supported with CBR client mapping, but is not supported with GFP-F client mapping. Up to two protection groups can be created on the 11QPEN4 card. A protection group consists of two line ports and one client port. Each protection group operates independently of the other group, with its protection state.

The 11QPEN4 and the 11QPA4 cards are channels in the Y-cable protection group and are independent channels on working and protection boards. The channel numbering at one end may not be the same as the channel numbering at the other end. For example, channel C1 and L1 in the near-end working and protection pairs can connect to channel L2 and C2 at the far-end working. The protection pairs form an end-to-end protected service.

An 11QPEN4 OTU2 client port (OT A) can be connected to 11DPE12 and 11DPE12E line ports (OT B). Up to four 11DPE12 and 11DPE12E OTs can be connected to one 11QPEN4 card. The configuration is encrypted for GbE services.

An 11QPEN4 OTU2 client port (OT A) can be connected to an 11DPM12 line port (OT B). Up to four 11DPM12 OTs can be connected to one 11QPEN4 card. The configuration is encrypted for GbE, FC100, FC200, and FC400 services.

Note 1 — The operational mode on the 11QPEN4 line port is add-drop only.

Note 2 — The client ports on the 11QPEN4 card cannot be assigned to the OC192/STM64 rate.

Note 3 — The E-SNCP and Y-cable must not coexist on the 11QPEN4 card. For example, if at least one E-SNCP protection group is created on a board, the Y-cable protection must not be on the board and vice versa.

11DPE12A

The 5620 SAM supports Y-cable (for 1 GigE client ports) on mate 11DPE12A cards.

16.7 Client protection

You can configure a client protected optical transport service between I/O cards with OC or STM rates over SNCNC protected lower-order ODU trails, which are configured between I/O cards with OTU rates on OCS devices. See Procedure 16-21 to configure a client protected service with double add-drop cross-connects, select working and protection ports, or trails, or ODUk timeslots as constraints for each of the termination points of the service. See Procedure 16-22.

The 5620 SAM allows configuration of an SNCNC protected trail or a client protected optical service with three termination points. In such a configuration, if Site A has one termination point, Site Z has two termination points; or if Site A has two termination points, Site Z has one termination point. In case of a unidirectional SNCNC protected trail with three termination points, the source site must have two termination points and destination site must have one termination point.

If you configure two termination points on each of the sites (A and Z), four paths created after a trail or service is configured; namely, A1Z1, A1Z2, A2Z1, and A2Z2. Only one of these paths is active at a time. You can modify the active path by modifying the Protection Switch parameter of the APS group. See Procedure 16-30.

16.8 Dual-stage multiplexing

Dual-stage multiplexing is supported on the 1830 PSS-16 and 1830 PSS-32 shelves. A signal is added to an OT client port and multiplexed on a line port with a larger bandwidth. The signal is added a second time at a higher rate OT and multiplexed to the line port. The reverse path occurs if the signal is dropped. See Procedure 16-27 and the *Alcatel-Lucent 1830 Photonic Service Switch User Provisioning Guide* for more information.

16.9 Regeneration services on the 1830 PSS

The 1830 PSS supports provisioning, discovery, and a topological view of the following regeneration services.

- DWDM–DWDM
- DWDM–CWDM
- CWDM–B&W
- DWDM–B&W

To provision the services, see Procedure 16-1. To discover the services, see Procedure 16-3. To view the services in the topological view, see the *5620 SAM User Guide*. The Regen check box is automatically selected when a regen service is created. You can view the Regen parameter on the General tab of the Service Path form.

DWDM-DWDM

DWDM–DWDM single channel OEO regeneration is supported with back-to-back OTs connected through the client ports. Keyed and unkeyed services are supported on the configuration. The following OTs are supported:

- 11STAR1
- 11STAR1A
- 260SCX2
- 43STA1P
- 43STX4P
- 43STX4

Note — For regeneration on the 43STA1P, the client port rate must be OC768 or STM256. Do not use OTU3.

The regeneration is supported with two single port OTs that have line port operational modes configured for regeneration. Client ports are not used in the configuration. The following OTs are supported:

- 112SA1L (drop shelf only)
- 112SCA1
- 112SNA1
- 112SCX10
- 112SNX10
- 112SX10L (drop shelf only)
- 260SCX2
- 43SCA1
- 43SCGE1
- 43SCX4
- 43SCX4E
- 43SCX4L (drop shelf only)

Note — For this configuration, the channels can be different on each SFD or CWR port.

DWDM-CWDM

The 1830 PSS-32 supports single channel regeneration for CWDM and DWDM connections and configurations for CWDM bidirectional transmission with DWDM-CWDM (dual-fiber) regeneration, when regeneration OTs are supported. The rate supported for the service is FC200. Keyed and unkeyed services are supported on the configuration. The following OTs are supported:

- 11STAR1 and 11STAR1A OT—line port is connected to the DWDM signal and the client port is connected to the CWDM signal
- 4DPA4 OT (FlexMux only)—one line and an eVOA port are connected to the DWDM signal; the other line and eVOA port are connected to the CWDM signal. The line ports are configured for CrossRegen mode.
- 11QPA4 OT—a line and an eVOA port are connected to the DWDM signal and the associated client port is connected to the CWDM signal

Note — 11QPEN4 supports regeneration services with the 11QPA4 as the A end and Z end of the service.

CWDM-B&W

The CWDM-B&W single channel OEO regeneration is supported when the 1830 PSS-32 and 1830 PSS-1 GBEH devices are operational. The rate supported for the service is 1Gbe. Unkeyed service is supported on the configuration and no cross-connects are created. The following OTs are supported:

- 4DPA4 OT (FlexMux only)—one line and an eVOA port are connected to the CWDM signal and the other line port is connected to the B&W signal. The line ports are configured for CrossRegen mode.
- 11QPA4 OT—a line port is connected to the CWDM signal and the associated client port is connected to the B&W signal.

Note — The 11QPEN4 card supports regeneration services with the 11QPA4 as the A end and Z end of the service.

CWDM-FOADM

Degree-2 CWDM-FOADM is supported on the 1830 PSS. Any symmetrical combination of OMD-based end terminal configuration is supported. The following configurations are supported:

- SFC-2—SFC-2
- SFC-4—SFC-4
- SFC-8—SFC-8

The following OTs are supported:

- 4DPA4
- 11DPE12

DWDM-B&W

The DWDM-B&W single channel OEO regeneration is supported when the 1830 PSS-32, and 1830 PSS-1 GBEH devices are operational. The rate supported for the service is 1 GbE. The following OTs are supported:

- 11STAR1 and 11STAR1A OT—the line port is connected to the DWDM signal and the client port is connected to the B&W signal. Regeneration occurs from client to line.
- 4DPA4 OT (FlexMux only)—one line and an eVOA port is connected to the DWDM signal and the other line port is connected to the B&W signal. The line ports are configured for CrossRegen mode
- 11QPA4 OT—a line and an eVOA port are connected to the DWDM signal and the associated client port is connected to the B&W signal

Note — The 11QPEN4 card supports regeneration services with the 11QPA4 as the A end and Z end of the service.

16.10 CDC-F ROADM service

The 5620 SAM supports the configuration of colorless, directionless, and contentionless flexible grid ROADM service that provides:

- optical channel add-drop for up to 88 50 GHz spaced channels per degree to the add-drop section of the node
- contentionless add-drop using multicast switches in each add-drop block
- coherent optical demultiplexing at the OT and uplink receivers
- support for eight degree configurations
- support for 12 MCS add-drop blocks
- support for 16 add-drop channels per add-drop block for a maximum of 192 add-drop channels for the node
- hardware readiness for transmission spectrum of 96 50 GHz spaced channels per degree
- hardware readiness for flexible grid operation
- hardware readiness for expansion to add up to 20 additional add-drop blocks

The 5620 SAM supports the following cards in the CDC-F configuration:

- WR20 TFM
- MCS8-16
- AAR-8A
- OTDR
- 260SCX2
- 130SCUPB
- MSH8-FSM
- A4PSWG
- ASWG
- 130SNX10
- 130SCUPC
- MVAC8B

See the *Alcatel-Lucent 1830 PSS Product Information and Planning Guide* for more information about the CDC-F architecture.

The 5620 SAM supports the configuration of the CDC-F service and the underlying trails. See the following procedures for more information:

- Procedure 13-9—OCH trail configuration
- Procedure 13-6—OTU trail configuration
- Procedure 13-1—ODU trail configuration
- Procedure 16-1—Optical transport service configuration

Path search limitations

The CDC network supports up to eight degree configurations, that may result in the timing out of the 5620 SAM system-defined path search function.

To avoid path search timeout:

- configure path constraints with the Constraint Type parameter set to Exclusion during the trail configuration. See Procedure 13-3 for more information about configuring path constraints for trails.
- configure the Path Search Option parameter on the Optical Transport Service form to User Defined and configure path constraints with the Constraint Type parameter set to Exclusion during service configuration. See Procedures 16-1 and 16-6 for more information about service configuration and path constraints configuration for services.

100 GigE and 200 GigE card limitations

The CDC-F service configuration with a 100 GigE or 200 GigE card used for the unidirectional regen configuration in the middle node has certain limitations. Alcatel-Lucent recommends that you follow the bottom-up method: configure the OTU trails, then the ODU trails, and then configure the service.

16.11 Symmetric and asymmetric interworking services

The 5620 SAM supports the configuration of symmetric and asymmetric interworking optical transport services. WDM devices configured with OTH supported cards or OCS devices can interwork with WDM devices configured with non-OTH cards.

The interworking is symmetric when both the OTH and non-OTH ends are configured with the same rates (for example, ODU0).

The interworking is asymmetric when the OTH end is configured with a lower rate (for example, ODU0) and the non-OTH end is configured with a higher rate (for example, ODU2). The Asymmetric Interworking parameter is configured on the ODU trail (Create) form during the ODU trail configuration of an asymmetric interworking service.

16.12 Multipoint services

Multipoint transport service is primarily used to transmit video signals to multiple destinations. The client signals to be transmitted are added at the Add site. The multipoint transport service is categorized in one of the following types:

- Drop and Continue
- Multicast

In drop and continue multipoint transport service, some signals are dropped at the intermediate drop and continue sites. The remaining signals are dropped at the drop site. In the multicast multipoint transport service, intermediate drop and continue sites do not exist.

The 5620 SAM supports the creation of multipoint transport services using 11QPA4 cards interworking with 1830 PSS OCS devices by creating HO-ODU trails where required and creating a multipoint service on top of the HO-ODU trails. The LO-ODU trails are created automatically after the service is created. However, Extend Drop Site and Delete Drop Site is not supported.

You can discover or configure a segment protected drop and continue service using dual stage multiplexing of the 4DPA4 card with the 11DPM12 card. You must create the segment protected unidirectional LO-ODU trail over the required HO-ODU trail, before creating the drop and continue service with the 4DPA4 client port at the Add Site.

The 1830 PSS OCS devices are not used as Add, Drop and Continue, and Drop sites. The 1830 PSS OCS devices are used as the intermediate devices through which regeneration services are created. See Procedure 16-2 for information about creating a multipoint optical transport service.

16.13 Viewing optical services on the 5620 SAM GUI

The 5620 SAM client GUI provides multiple ways of viewing optical transport services. See Table 16-1.

Table 16-1 Multiple ways of viewing optical transport services

Method	Steps
From NEs on the physical topology map	Right-click on one or more NEs and choose Show Services→Optical Transport Services or Optical Multipoint Transport Services
From NEs on the navigation tree	Right-click on one or more NEs and choose Show Services→Optical Transport Services or Optical Multipoint Transport Services
From the NE properties form	• Right-click on an NE on the navigation tree or the physical topology map and choose Properties • Click on the Services tab on the Card Slot (Edit) form • Click on the Optical Transport Services tab or the Optical Multipoint Transport Services tab

(1 of 2)

Method	Steps
From the card properties form	• Expand the equipment navigation tree to the card level • Right-click on a card and choose Properties • Click on the Services tab on the Card Slot (Edit) form • Click on the Optical Transport Services tab or the Optical Multipoint Transport Services tab
From the 5620 SAM main menu	• Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens. • Choose the Optical Transport Service (Optical Management) option from the drop-down menu and click Search. A list of optical transport services appears.

(2 of 2)

16.14 Deleting optical transport services and trails

When you choose to delete an optical transport service from the Manage Services form, the following check boxes are available. You can select either both check boxes or only the second check box.

- Also delete unused trail and XCs
- I understand the implications of this action

Deleting optical transport services

While deleting an optical transport service between two 1830 PSS WDM devices with non-OTH rate cards, if you select both of the preceding check boxes, the optical transport service, underlying ODU and OTU trails, and cross-connects are all deleted. However, if you select only the I understand the implications of this action check box, only the optical transport service is deleted, and the underlying trails and cross-connects are retained. This optical transport service can be rediscovered. If you delete an optical transport service with SubGigE rate or an optical transport service that involves LAG, the VTS XCs are deleted, so the services cannot be rediscovered.

While deleting an optical transport service between two 1830 PSS WDM devices with OTH rate cards, if you select both of the preceding check boxes, the optical transport service, underlying LO-ODU and HO-ODU trails, and cross-connects are all deleted. However, if you select only the I understand the implications of this action check box, only the optical transport service and the LO-ODU trail are deleted, and the HO-ODU trail and cross-connects are retained. If you delete an optical transport service involving 11DPM12 OPTSG service with an LO-ODU trail that is also used by another optical transport service, deletion of the service does not delete the LO-ODU trail. You cannot rediscover the optical transport service in this case.

While deleting an optical transport service between two 1830 PSS OCS devices, irrespective of either selecting both the options or only the second option, the HO-ODU trail is never deleted.

Deleting optical trails

While deleting an ODU trail between two 1830 PSS WDM devices with non-OTH rate cards, if you select both of the preceding check boxes, the ODU trail, underlying OTU trail, and cross-connects are all deleted. However, if you select only the I understand the implications of this action check box, only the ODU trail is deleted, and the underlying OTU trail and cross-connects are retained.

While deleting an LO-ODU trail between two 1830 PSS WDM devices with OTH rate cards, if you select both of the preceding check boxes, the LO-ODU trail, underlying HO-ODU trail, and cross-connects are all deleted. However, if you select only the I understand the implications of this action check box, only the LO-ODU trail is deleted, and the HO-ODU trail and cross-connects are retained.

While deleting an LO-ODU trail between two 1830 PSS OCS devices, irrespective of either selecting both the options or only the second option, the HO-ODU trail is never deleted.

16.15 Administrative state transitions for service and trail

This section describes the administrative state transitions for services and trails.

Table 16-2 Administrative state transitions for service and trail

Transitions	Termination points	Intermediate 1830 PSS OT ports (client, line, VA, and MVAC G)	OCH XC	VTS XC(8)
Service state changed to Maintenance	Maintenance(1)	Maintenance	Down	Down
ODU trail state changed to Maintenance	Maintenance(1)	Maintenance	Down	-
Service state changed from Maintenance to Up(2)	Up	Up	Up	Up
ODU trail state changed from Maintenance to Up(2)	Up	Up	Up	-
Service state changed to AINS	Up with Port AINS enabled(3)	Up with Port AINS enabled(4)	Up	Up
ODU trail state changed to AINS	Up with Port AINS enabled(3)	Up with Port AINS enabled(4)	Up	-
Service state changed from AINS to Up	Up(5)	Up(5)	-	Up
ODU trail state changed from AINS to Up	Up(5)	Up(5)	-	-
Service state changed from AINS to Down	Down(6)	Up(5)	-	Down
ODU trail state changed from AINS to Down	Down	Up(5)	-	-
Service state changed from Down to Up	Up	-	-	Up

(1 of 2)

Transitions	**Termination points**	**Intermediate 1830 PSS OT ports (client, line, VA, and MVAC G)**	**OCH XC**	**VTS XC**[8]
ODU trail state changed from Down to Up[7]	Up	Up	-	-
Service state changed from Up to Down	Down	-	-	Down
ODU trail state changed from Up to Down	Down	-	-	-

(2 of 2)

Notes

(1) When the termination point is an 1830 PSS port.

(2) When a service or ODU trail administrative state is changed from maintenance state to Up or AINS state, the 5620 SAM checks if a loopback is configured on any of the OT or MVAC G ports involved in the service or ODU trail. If a loopback is detected on any of the ports, the administrative state change is unsuccessful.

(3) Port AINS can be enabled only when the termination ports are 1830 PSS ports and the Administrative State parameter is not set to Up.

(4) Port AINS can be enabled only when the Administrative State parameter is not set to Up.

(5) Port AINS is disabled.

(6) The administrative state of the termination points of a SubGigE service is unchanged.

(7) When the ODU trail state is changed from Down to Up, then the states of intermediate 1830 PSS non-OT ports change to Up.

(8) The administrative state of a VTS XC cannot be changed when the VTS XC is a part of a protection group. Hence, the administrative state of the ESNCP SubGigE service does not affect the administrative state of the VTS XC.

Note 1 — The 5620 SAM does not support service administrative state transition from Maintenance state to Down state.

Note 2 — The Port AINS state of a physical port is indicated on the hop objects.

16.16 Administrative and operational states determined by the 5620 SAM

This section explains how the 5620 SAM determines the administrative state and operational state of a service or ODU trail during the service discovery.

Administrative states for service and ODU trails

Table 16-3 Administrative states for service and ODU trails

Service or ODU trail	Termination point A	Termination point Z
Up	Up	Up
Down	Down	Down
Down	Down	Up
Down	Up	Down

Note 1 — If the administrative state of the OT or MVAC G ports that are part of a service path, is changed to maintenance, the service administrative state is changed to maintenance with an inconsistency message in the Optical Transport Service (Edit) form.

Note 2 — If the administrative state of the OT or MVAC G ports that are part of an ODU trail, is changed to maintenance, the administrative state of the ODU trail and all associated services is changed to maintenance with an inconsistency message in the Optical Transport Service (Edit) form of all the associated services.

Note 3 — If none of the OT or MVAC G ports that are part of a service path, is in maintenance state and Port AINS is enabled on one of the ports, the service administrative state is changed to AINS with an inconsistency message in the Optical Transport Service (Edit) form.

Note 4 — If none of the OT or MVAC G ports that are part of an ODU trail, is in maintenance state and Port AINS is enabled one of the ports, the administrative state of the ODU trail and all associated services is changed to AINS with an inconsistency message in the Optical Transport Service (Edit) form of all the associated services.

Administrative states for multipoint service

Table 16-4 Administrative states for multipoint service

Service	Add site	Drop site A	Drop site B
Up	Up	Up	Down
Up	Up	Down	Up
Down	Up	Down	Down
Down	Down	Down	Down

Administrative states for unprotected SubGigE services

Table 16-5 Administrative states for unprotected SubGigE services

Service[(1)]	Source termination point	Destination termination point	Source VTS XC	Destination VTS XC
Up	Up	Up	Up	Up
Down	Up	Up	Up	Down
Down	Up	Up	Down	Up
Down	Up	Up	Down	Down
Down	Up	Down	Up	Up
Down	Up	Down	Up	Down
Down	Up	Down	Down	Up
Down	Up	Down	Up	Up
Down	Up	Down	Down	Down
Down	Down	Up	Up	Up
Down	Down	Up	Up	Down
Down	Down	Up	Down	Up
Down	Down	Up	Down	Down
Down	Down	Down	Up	Up
Down	Down	Down	Up	Down
Down	Down	Down	Down	Up
Down	Down	Down	Down	Down

Note
(1) The administrative state of a VTS XC cannot be changed when the VTS XC is a part of a protection group. The administrative state of the ESNCP SubGigE service does not affect the administrative state of the VTS XC.

Administrative states for Y-cable and OPSB protected services

Table 16-6 Administrative states for Y-cable and OPSB protected services

Service	Working path source	Protection path source	Working path destination	Protection path destination
Up	Up	Up	Up	Up
Up	Up	Up	Up	Down
Up	Up	Up	Down	Up
Up	Up	Down	Up	Up
Up	Down	Up	Up	Up
Up	Up	Down	Up	Down

(1 of 2)

Service	Working path source	Protection path source	Working path destination	Protection path destination
Up	Down	Up	Down	Up
Down	Up	Up	Down	Down
Down	Up	Down	Down	Up
Down	Down	Up	Up	Down
Down	Down	Down	Down	Up
Down	Down	Down	Up	Down
Down	Down	Up	Down	Down
Down	Up	Down	Down	Down
Down	Down	Down	Down	Down

(2 of 2)

Operational states for service and trails

Table 16-7 Operational states for service and ODU trail

Service	Termination point A	Termination point Z
Up	Up	Up
Up	Maintenance	Maintenance
Up	Up	Maintenance
Up	Maintenance	Up
Down	Down	Down
Down	Down	Maintenance
Down	Maintenance	Down
Down	Down	Up
Down	Up	Down

Table 16-8 Operational states for protected multipoint service

Service	Working path	Protection path
Up	Up	Up
Down	Down	Down
Up	Down	Up
Up	Up	Down

Table 16-9 Operational states for Y-cable and OPSB protected services

Service	Working path source	Protection path source	Working path destination	Protection path destination
Up	Up (maintenance)	Up (maintenance)	Up (maintenance)	Up (maintenance)
Up	Up (maintenance)	Up (maintenance)	Up (maintenance)	Down
Up	Up (maintenance)	Up (maintenance)	Down	Up (maintenance)
Up	Up (maintenance)	Down	Up (maintenance)	Up (maintenance)
Up	Down	Up (maintenance)	Up (maintenance)	Up (maintenance)
Up	Up (maintenance)	Down	Up (maintenance)	Down
Up	Down	Up (maintenance)	Down	Up (maintenance)
Down	Up (maintenance)	Up (maintenance)	Down	Down
Down	Up (maintenance)	Down	Down	Up (maintenance)
Down	Down	Up (maintenance)	Up (maintenance)	Down
Down	Down	Down	Down	Up (maintenance)
Down	Down	Down	Up (maintenance)	Down
Down	Down	Up (maintenance)	Down	Down
Down	Up (maintenance)	Down	Down	Down
Down	Down	Down	Down	Down

The transport service operational state and additional information are assigned separately for working paths and for protection paths. The operational state of a path can be Down as a result of many reasons such as:

- Cross Connect Down—at least one of the cross-connections on the path has an operational state set to Down
- Missing Cross Connect—there is a missing cross-connect on the path
- Wavekey Mode Mismatch—there is a wavekey mismatch on the path
- Port (that is not part of CrossConnect) Down—a port that is not part of the cross-connect is operationally Down
- VTS Connection is Down
- Missing VTS Connection
- Missing ODUk Connection

You can click Complete Transport Service to re-create the cross-connections and APS groups if entries are missing and to complete the creation of the service.

Note 1 — You can view the administrative state and operational state information on the hops tab in the protection or working paths in the service.

Note 2 — When you set the administrative state to Down, the 5620 SAM does not generate transport service down or ODU trail down alarms.

Note 3 — If the administrative state of the ODU trail is set to Up from SAM, then the administrative states of all the hops are set to Up.

Note 4 — If the administrative states of the termination points of an OPSB service is set to Up or Down, then the administrative states of the client and SIG ports of the OPSB card is also set to Up or Down respectively.

16.17 AINS parameters for ports and facility objects

You can configure AINS parameters using the Turn Up/AINS option on the equipment tree port object for ports and facility object for OTU or ODU facility objects.

OCS ports

The Port Specifics→General tab of the Physical Port (Edit) form displays the facility and the equipment AINS parameters. The ports of the uplink cards do not have the equipment AINS parameters. The Turn Up/AINS button is also available on the Physical Port (Edit) form. The Administrative State parameter is automatically set to Up when the Turn Up/AINS option is chosen of the equipment tree port object. The AINS mode is disabled when the Turn Up option is chosen from contextual menu of the equipment tree port object.

OCS facility objects

You can configure AINS parameters using the Turn Up/AINS option on the equipment tree facility object. The States tab of the facility object form displays the facility AINS parameters. The Administrative State parameter is automatically set to Up when the Turn Up/AINS option is chosen of the equipment tree facility object. The AINS mode is disabled when the Turn Up option is chosen from the contextual menu of the equipment tree facility object.

WDM ports

You can configure AINS parameters using the Turn Up/AINS option on the equipment tree port object. The Port Specifics→General tab of the Physical Port (Edit) form displays the facility AINS parameters. The Turn Up/AINS button is also available on the Physical Port (Edit) form. The Turn Up/AINS parameter is dimmed when the Administrative State parameter is set to Up.

WDM facility objects

You can configure AINS parameters using the Turn Up/AINS option on the equipment tree facility object. The States tab of the facility object form displays the facility AINS parameters. The Turn Up/AINS parameter is dimmed when the Administrative State parameter is set to Up.

16.18 Procedures to configure optical transport services

Procedure 16-1 To configure an optical transport service

The following points should be considered before creating the service:

- Configure the rate, transmit frequency, and receive frequency of the terminating sites.
- Configure optical links between the terminating sites.
- Configure ODU trails before configuring the optical transport service for OCS devices.

1 Choose Create→Service→Optical→Transport Service from the 5620 SAM main menu. The Optical Transport Service (Create) form opens.

2 Configure the parameters in the Customer panel.

Note — You can create a template for the service at every stage by using the Apply or OK button before you specify the optical sites and termination points. You can use the service template to create a service by adding optical sites and termination points. See steps 6 to 9 to create an optical site.

3 Configure the required parameters.

Note — If you select the Bidirectional check box, bidirectional cross-connects are created and hops from A to Z and Z to A are displayed after service creation

If you deselect the Bidirectional check box, unidirectional cross-connects are created and hops from A to Z are displayed after service creation

4 Configure the parameters in the VLAN Configuration Details panel, if you have configured the Assigned Rate parameter as SubGigE, for Sub GigE services.

Note 1 — For a line SVID configuration with a QinQ Service Stack-VLAN Tagging Configuration of Push-Pop, the value of CE-VLANID - AZ and CE-VLANID - ZA must be the same.

Note 2 — For a line SVID configuration, the value of Stack-VLANID - AZ and Stack-VLANID - ZA must be the same.

5 Perform one of the following to configure the Protection Type parameter:

a For diverse route protection services:

i Configure the Protection Type parameter as Diverse Route.

ii Select the Use Existing Unprotected Service check box.

Note — You can also create a diverse route service by choosing two termination points on the A end site, and two termination points on the Z end site. Go to step 6.

iii Select the working path in the Working Path Service panel and protection path in the Protection Path Service panel. Go to step 12.

Note — When the diverse route service is created, the unprotected services used for the diverse route service are deleted.

b Configure the parameters in the APS Group panel, if you have configured the Protection Type parameter as ESNCP Protected or OPS Protected, for ESNCP protected or OPS protected services.

c Configure the parameters in the YCable APS Group panel, if you have configured the Protection Type parameter as Y-Cable Protected, for Y cable protected services.

6 Right-click on the Sites object in the optical transport service tree and choose Create Optical Site. The Select Network Elements - Optical Transport Service form opens with a list of sites.

7 Choose two sites and click OK. The Select Network Elements - Optical Transport Service form closes and the Site A End and Site Z End objects appear on the optical transport service tree below the Sites object.

Note — You can also create an optical transport service by selecting one or more sites from the physical topology map or the equipment tree. With this method, you do not configure the end site for the chosen site. However, you must configure the termination point for the chosen site. See steps 6 to 9 for information about configuring the termination point for the chosen site.

8 Right-click on the Site A End object and choose Create Termination Point. The Select Termination point form opens.

9 Choose a port and click OK. The Select Termination Point form closes and the Optical Transport Service (Create) form reappears.

> **Note 1 —** In this form, only the termination points that can be configured with the specified service rates are displayed.
>
> **Note 2 —** If a termination point is used in another service, the termination point is not displayed (except for SubGigE services).
>
> **Note 3 —** If a termination point is configured with another valid rate, the termination point is not displayed.

10 Repeat steps 8 to 9 to configure the Site Z End.

11 Expand the Site A End and Site Z End objects on the optical transport service tree to view the termination points created.

12 Perform Procedure 16-6 to configure a path constraint for the service.

13 To configure the preview of the optical transport service:

- **i** Configure the Service Deployment Mode parameter on the General tab of the Optical Transport Service (Create) form as Preview, and click Apply. The preview of the path that the 5620 SAM will take when the service is deployed, is displayed.

- **ii** To select the option to include or exclude a path, click on the Service Paths→Preview Path object on the navigation tree and click on the Hops A-Z or Hops Z-A tab.

iii Choose an entry and click Include Constraint or Exclude Constraint, as required, to add a new path or to exclude an existing path, and perform the path search again.

Note 1 — The service preview information is lost when the form is closed.

Note 2 — When the underlying trails are not configured, only the physical hops are displayed in the preview path and not the logical hops.

Note 3 — The APS groups are not displayed in the preview.

Note 4 — The underlying trails are listed in the Server Trails tab only if the trails are configured before the service configuration.

Note 5 — For the optical services that require the configuration of ODU trails as a prerequisite for service configuration, the preview can only be generated if the trails are configured.

iv Configure the Service Deployment Mode parameter on the General tab of the Optical Transport Service (Create) form as Deploy, to deploy the service on the network.

14 Save the changes and close the forms.

Note — Up to two sites can be specified to create an optical transport service. The sites are named Site A End and Site Z End by the 5620 SAM.

Procedure 16-2 To configure a multipoint transport service

The following are the prerequisites for 11QPA4 multipoint drop and continue service creation:

- For unprotected multipoint drop and continue service, the termination points must have their administrative state set to down.
- Create the APS group on the 1830 PSS. See Procedure 16-29.
- The APS group must be created manually on the drop and continue and drop sites for configuring 11QPA4 ESNCP protected service. The working port must be assigned a rate and the protection port must be unassigned.
- Set the Operational Mode parameter to Drop Continue on the line port when you create a drop and continue multipoint service.
- Set the Operational Mode parameter to Add Only on the line ports of the Add site and to Drop And Continue on the Drop and Continue sites.

- Configure the rate, transmit frequency, and receive frequency of the terminating sites.
- Create optical links between the terminating sites.

1 Choose Create→Service→Optical→Multipoint Transport Service from the 5620 SAM main menu. The Multipoint Transport Service (Create) form opens.

2 Click Select. The Select Customer - Multipoint Transport Service form opens.

3 Choose a customer and click OK. The Select Customer - Optical Transport Service form closes and the Multipoint Transport Service (Create) form reappears.

Note — You can create a template for the service at operational state by using the Apply or OK button before you specify the optical sites and termination points. You can use the service template to create a service by adding optical sites and termination points. See "Managing templates" in the *5620 SAM Scripts and Templates Developer Guide* for the procedure to create a service from a template.

4 Configure the required parameters.

Note — You cannot configure the Administrative State parameter for a protected service.

5 Configure the Rate parameter. Table 16-10 lists the rates supported on 11PDM12 and 11QPA4 cards.

Table 16-10 Rate supported on OT cards

Cards	Service type	Rate supported
11DPM12	Drop and Continue	1 GbE
		HDSDI
		SDSDI
11QPA4	Drop and Continue	10GbE LAN
	Multicast	10GbE LAN
4DPA4	Drop and Continue	1 GbE
		HDSDI
		SDSDI

6 Right-click on the Sites object in the navigation tree and choose Create Add Site. The Select Network Elements - Multipoint Transport Service form opens with a list of sites.

7 Choose a site and click OK. The Select Network Elements - Multipoint Transport Service form closes.

8 Right-click on the Site Add object in the multipoint transport service tree and choose Create Termination Point. The Select Termination Point form opens.

9 Choose a port and click OK. The Select Termination Point form closes and the Multipoint Transport Service (Create) form reappears.

Note — The Select Termination Point form lists only the termination points that can be configured for the Rate parameter value configured in Step 5.

10 Repeat steps 8 to 9 to configure drop and continue and drop sites.

Note — Configure two drop sites for an ESNCP service.

11 Go to step 12 for ESNCP service and step 14 for unprotected service.

12 Configure one of the drop sites as working and the other as protection. Click on the Site Drop object on the multipoint transport service tree. The properties of the drop site appears in the right panel.

13 Configure the required parameters for the drop sites.

14 To create path constraints, click on the Multipoint Transport Service object on the multipoint transport service tree.

15 Click on the Path Constraints tab and click Create. The Optical Path Constraint (Create) form opens.

16 Click Select in the Site panel. The Select Site - Optical Path Constraint form opens.

17 Choose the drop and continue sites as path constraints.

18 Click OK. The Select Site - Optical Path Constraint form closes.

19 Click Select in the Port panel. The Select Port - Optical Path Constraint form opens.

20 Choose the port as path constraints.

21 Save your changes and close the forms.

Note 1 — If the termination points are not added for any of the drop and continue sites during service creation, repeat steps 6 to 9 to add the termination points after the service is created. The path constraints are updated automatically.

Note 2 — If you need to delete any of the termination points in a drop and continue site, right-click on the termination point and choose Delete. The path constraints are updated automatically.

Procedure 16-3 To discover optical transport services

The optical transport services are not discovered automatically during NE discovery. The discovery of an optical transport service includes sub-tasks such as discovery of ODU trails, OTU trails, and OCH trails. The status of an optical transport service discovery is displayed as In Progress in the Task Manager form, until all the sub-tasks are completed successfully. The status also displays the number of new optical transport services, ODU trails, OTU trails, and OCH trails discovered. See the *5620 SAM User Guide* for more information about monitoring the 5620 SAM task manager.

Perform this procedure after all of the 1830 PSS devices are synchronized in the 5620 SAM.

1 Perform one of the following:

a From the Manage menu for services:

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Click Optical Transport Service and select Discover Transport Services. The Discover Transport Services form opens with a list of equipment groups displayed.

iii Choose a physical equipment group and click OK. The Discover Transport Services form closes and the Manage Services form reappears with a list of discovered optical transport services within the specified group.

b From the Manage menu for trails:

i Choose Manage→OTN→OTN Trails from the 5620 SAM main menu. The Manage OTN Trails form opens.

ii Choose ODU Trail (Optical Management) from the object drop-down menu. A list of ODU trails appears.

iii Choose an ODU trail from the list and click Discover Transport Services. The discovered service is listed in the Manage Services form.

c From the physical topology map:

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 or on the empty space in the map and choose Discover Transport Services in Group. The Manage Services form opens with a list of discovered optical transport services within the group to which the NE belongs.

d On the equipment tree, right-click on the equipment group object, NE object, or multiple NE objects, and choose Discover Transport Services in Group. The Manage Services form opens with a list of discovered optical transport services within the group to which the NE belongs.

2 Close the form.

Note — You can perform the same procedure to discover services created in 1354 PhM.

Procedure 16-4 To unmanage an optical transport service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form appears.

2 Choose Optical Transport Service (Optical Management) option.

3 Choose the optical transport service that you need to unmanage and click Optical Transport Service, then choose Unmanage Service.

4 Save your changes. The optical transport service is unmanaged. The optical transport service appears on the Manage Services form with the Managed check box deselected.

Note — The deselected Managed check box indicates the following:

- The APS groups and VTS XCs are disassociated from the service.
- The service paths are removed.
- The sites with the termination points are retained.
- The information on the General tab of the Optical Transport Service (Edit) form is retained.

Procedure 16-5 To remanage an unmanaged optical transport service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form appears.

2 Choose Optical Transport Service (Optical Management) option and click Search. A list optical transport services on the 1830 PSS appears on the Manage Services form.

3 Perform one of the following:

a From the Manage Services form:

i Choose the unmanaged service and click Optical Transport Service.

ii Choose Complete Transport Service.

iii Save your changes and close the form.

b From the Optical Transport Service (Edit) form:

i Choose the unmanaged optical transport service from the Manage Services form and click Properties. The Optical Transport Service (Edit) form opens.

ii Click Complete Transport Service.

iii Save your changes and close the form.

Procedure 16-6 To configure path constraints for a service

1 Perform one of the following:

a To configure path constraints during service configuration:

i Configure an optical transport service or a multipoint transport service. See Procedure 16-1 and 16-2.

ii Click on the Path Constraints tab in the Optical or Multipoint transport Service (Create) form.

b To configure path constraints for a configured service:

i Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

ii Choose Optical Transport Service and click Search.

iii Choose an optical or multipoint transport service and click Properties. The Optical or Multipoint Transport Service (Edit) form opens.

iv Click on the Path Constraints tab.

2 Click Create. The Optical Path Constraint (Create) form opens.

3 Configure the required parameters.

> **Note —** Configure the Constraint Type parameter as Exclusion to exclude the constraint element from the service path, and as Inclusion to include the constraint element in the service path

4 Perform one of the following:

a The constraint element is a port:

i Select a site on the Site panel.

ii Select a port on the Port panel.

b Select a site on the Site panel, if the constraint element is a site.

c Select a trail on the Trail panel, if the constraint element is a trail.

d The constraint element is an ODUk timeslot:

> **Note 1 —** Ensure that you have configured the ODUk timeslots. See Procedure 16-13.
>
> **Note 2 —** The constraint element, ODUk timeslot, is available for configuration only on the 1830 PSS, Release 5.5 and later.

i Configure the ODUk Rate parameter.

ii Select a site on the Site panel.

iii Select an ODUk Timeslot on the ODUk Timeslot panel.

e The constraint element is an OPTSG timeslot:

> **Note 1 —** Ensure that you have configured the OPTSG timeslots. See Procedure 16-15.
>
> **Note 2 —** This option is applicable only for an optical transport service.
>
> **Note 3 —** The constraint element, OPTSG timeslot, is available for configuration only on the 1830 PSS Release 5.5 and later.

i Select a site in the Site panel.

ii Select an OPTSG timeslot in the OPTSG Timeslot panel.

f The constraint element is an optical link:

i Select a site on the Site panel.

ii Select an optical link on the Optical Link panel.

5 Click OK. The Optical Path Constraint (Create) form closes and the Optical Transport Service (Edit) form reappears. Go to step 7.

6 Perform the following for 4DPA4 card:

i On the optical transport service tree, expand Sites→Site A End→Termination Point→TerminationPoint Working. The TP form opens.

ii Click Properties. The Physical Port (Edit) form opens.

iii Click Configure Time Slots. The Configure Time Slots for: 4DPA4 form opens.

iv Configure the Select Line Port parameter and choose the L1 or L2 timeslots based on the configured line port.

v Click OK. The Configure Time Slots for: 4DPA4 form closes and the Physical Port (Edit) form reappears.

vi Click OK. The Physical Port (Edit) form closes and the TP form reappears.

vii Save your changes.

7 On the optical transport service tree, expand Service Paths→Service Path and click on the Hops A to Z tab to view the changes in the path hops due to the path constraints modifications.

8 Close the form.

Procedure 16-7 To convert an unprotected service to an ESNCP service on a 4DPA4 FlexMux card

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose Optical Transport Service from the drop-down menu and click Search.

3 Choose an unprotected optical transport service and click Properties. The Optical Transport Service (Edit) form opens.

4 Configure the Protection Type parameter to ESNCP Protected.

5 Save your changes.

6 On the optical transport service tree, expand Service Paths. The protection path is added as a service path.

Note — If no protection path is available, the conversion is unsuccessful and an error message appears.

7 Close the forms.

Procedure 16-8 To convert an ESNCP service to an unprotected service on a 4DPA4 FlexMux card

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose Optical Transport Service and click Search.

3 Choose an ESNCP Protected optical transport service and click Properties. The Optical Transport Service (Edit) form opens.

4 Perform one of the following to convert an ESNCP service to an unprotected service.

  a Convert an ESNCP Protected service to an Unprotected service and retain the working path:

    i Configure the Protection Type parameter to Unprotected.

    ii Configure the Path Preference parameter to Retain Working Path.

    iii Click Apply.

  b Convert an ESNCP Protected service to an Unprotected service and retain the protection path:

    i Configure the Protection Type parameter to Unprotected.

    ii Configure the Path Preference parameter to Retain Protection Path.

    iii Click Apply to save the changes.

    iv Perform step 6 of Procedure 16-6 to configure the timeslots manually.

5 Close the forms.

Procedure 16-9 To display services riding on external or internal optical links

1 From the Physical Topology - Network view, double-click on an external or internal optical link. The Physical Link Group List form opens.

2 Choose an external or internal optical link and click Properties. The Optical Link (Edit) form opens.

3 Choose the Optical Transport Services option and click Search.

4 Choose a service and click Properties. The Optical Transport Service (Edit) form opens.

Note 1 — You can view optical services on an OCH cross-connect. Choose NE→Properties→OCH CrossConnects→Choose a cross connect→Properties. The OCH Cross Connect (Edit) form opens. Click on the Optical Transport Services tab to view the optical services on the selected cross-connect.

Note 2 — You can also view optical services on ports from the Physical Port (Edit) form by clicking on the Optical Transport Services tab.

Note 3 — The services must be discovered in the 5620 SAM in order to view services on the external and internal optical links, the OCH cross-connect, and the ports.

Procedure 16-10 To view the service hops

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose Optical Transport Service and click Search.

3 Choose an optical transport service and click Properties. The Optical Transport Service (Edit) form opens.

4 On the optical transport service tree, expand Service Paths→Service Path. The Service Path form opens.

5 Click on the Hops A to Z, Hops Z to A, ODU Hops A to Z, and ODU Hops Z to A tabs, as required, to view the hops in a service along the service path and ODU trail.

16.19 Procedures to configure service using 11DPM12, 11DPM8, and 11DPM4M cards

Procedure 16-11 To configure an unprotected service routing through an SNCN protected ODU trail on 11DPM12, 11DPM8, and 11DPM4M cards

1 Perform Procedure 13-1 to configure an SNCN protected LO-ODU trail. Choose SNCN Protected as the option for the Protection Type parameter.

Note — You can configure an unprotected OPTSG service through the SNCN protected ODU1PTF LO-ODU trails by choosing ODU1 as the value for the Assigned Rate parameter and ODU1PTFs as termination points on the 11DPM12 card.

2 Perform Procedure 16-1 and configure an unprotected optical transport service routing through the LO-ODU trail configured in Step 1.

Note 1 — You can route the service through the LO-ODU trail by choosing the client ports used in the ODU trail configuration as the termination points.

Note 2 — You can configure an unprotected OPTSG service through the SNCN protected ODU1PTF LO-ODU trails. Choose the OC3 or OC12 as the value for the Assigned rate parameter and client ports used in the ODU trail configuration as the termination points on the 11DPM12 card.

Procedure 16-12 To extend a drop site on an unprotected multipoint service in an 11DPM12 card

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose Optical Transport Service from the drop-down menu.

3 Choose an unprotected multipoint service from the list and click Properties. The Multipoint Transport Service (Edit) form opens.

4 On the navigation tree, right-click on the Site Drop object and choose Extend Drop Site. The Extend Drop Site form opens.

5 Select the new drop site. The new drop site object is added on the navigation tree.

6 Right-click on the newly created Site Drop object and choose Create Termination Point. The Select Termination Point form opens.

7 Choose a termination point and click OK. The Termination Point object appears on the navigation tree.

8 Click Apply. The extended drop site changes into a drop and continue site.

Procedure 16-13 To configure an ODU timeslot assignment for 11DPM12 cards

1 On the equipment tree, expand Network→NE→Shelf→Card→Line Port.

2 Right-click on the line port and choose Properties. The Physical Port (Edit) form opens.

3 Click Configure Timeslots. The Timeslot Assignments form opens.

4 Specify the required timeslot configuration. Table 16-11 lists the timeslot mapping.

Table 16-11 12xANY timeslot mapping

Client signal type	ODU0 XC (default)	ODU1 XC (TS)	ODUFlex XC (TS)	OPTSG XC (TS)
FC100	1	—	—	—
OC3/STM1	1	—	—	1
OC12/STM4	1	—	—	4
GbE	1	—	—	—
SDSDI	1	—	—	—
FE	1	—	—	—
OTU1	—	2	—	—
OC48/STM64	—	2	—	—
HDSDI	—	2	—	—
FC200	—	2	—	—
FC400	—	—	4	—
3GSDI	—	—	3	—

5 Save your changes and close the forms.

Procedure 16-14 To associate a line-side LO-ODUk on the 11DPM12 card

1 Configure the timeslots as described in Procedure 16-13.

2 Perform one of the following:

a 1830 PSS Release 5.5 and later.

i On the equipment tree, expand Network→1830 PSS→Shelf→Card→ODUPTF.

ii Right-click on the ODUPTF Object and choose Associate Line Side LO-ODUk Facility. The ODU1Ptf Association with Line side LO-ODUk (Create) form opens.

b Earlier releases of the 1830 PSS device.

i On the equipment tree, expand Network→1830 PSS→Shelf→Card.

ii Right-click on the Card object and select Properties. The Card Slot (Edit) form opens.

iii Click on the ODU1PTF Objects tab, choose an ODU1PTF and click Properties. The ODU1PTF (Edit) form opens.

iv Click Associate Line Side LO-ODUk Facility. The ODU1Ptf Association with Line side LO-ODUk (Create) form opens.

3 Select a line-side LO-ODUk facility in the Line Side LO-ODUk Facility panel.

Note — You can sub-structure the ODU1PTF object to create OPTSG objects only when ODU1PTF is associated with Line side LO-ODUk.

4 Click OK to confirm, save your changes, and close the forms.

Procedure 16-15 To configure OPTSG

1 Configure the ODU1 timeslots as described in Procedure 16-13.

2 Associate an ODU1PTF object with the line port ODUk facility object to create the cross-connect as described in Procedure 16-14. The ODU1PTF can be associated only with the ODU1 container (with two timeslots) on a line port.

3 On the equipment tree, expand Network→1830 PSS→Shelf→Card→ODUPTF

4 Right-click on the ODUPTF object and choose Configure ODU1PTF Timeslots. The Timeslot Assignments form opens.

5 Configure the timeslots and click OK.

Note — OPTSG configuration is applicable for keyed and unkeyed services.

Procedure 16-16 To delete an ODUk XC on the 11DPM12 card

Note — You cannot delete an ODUk XC when it is associated with a service or an APS Group.

1 On the equipment tree, expand Network→1830 PSS

2 Right-click on the 1830 PSS object and choose Properties. The Network Element (Edit) form opens.

3 Click on the ODUk Cross Connects tab, choose the cross-connect to be deleted, and click Delete. A Warning dialog box appears.

4 Select the check box on the Warning dialog box and click Yes. The ODUk XC deleted and disassociates the client port from the line port.

16.20 Procedures to configure OPS protection services

Procedure 16-17 To configure client-side OPS protection service

1 Configure an OPSB card. See Procedure 9-6.

2 Configure a protected optical transport service. See Procedure 16-1 for more information about configuring an optical transport service.

3 Choose OPS Protected as the Protection Type parameter option on the Optical Transport Service (Create) form in step 5 of Procedure 16-1.

4 Upon completion of service creation, the Optical Translator Unit Protection check box is automatically enabled on the Optical Transport Service (Edit) form.

Note — If the 5620 SAM detects a port configuration mismatch during optical transport service creation, an error message appears and the service creation is unsuccessful.

When the mismatch is corrected, the service creation is successful.

If the mismatch is detected during service discovery, the mismatch is indicated on the General tab of the Optical Transport Service form and cleared when the mismatch is corrected.

Procedure 16-18 To configure an OMSP protection service

1 Configure the OPSA cards as described in Procedure 9-5.

2 Configure the Protection Mode parameter as OMSP on the Card Specifics tab of the OPSA cards.

3 Configure the optical links for the following as described in Procedure 9-18.

OT (line port)←→SFD (Channel port): SFD (OMD)←→OPSA (SIG port): OPSA (A port)←→AMP1 (SIG port): AMP1 (LINE port)←→AMP1 (LINE port): AMP1 (SIG port) ←→OPSA (A port): OPSA (SIG port)←→SFD (OMD): SFD (Channel port)←→OT (line port)

OT (line port)←→SFD (Channel port): SFD (OMD)←→OPSA (SIG port): OPSA (B port)←→AMP2 (SIG port): AMP2 (LINE port)←→AMP2 (LINE port): AMP2 (SIG port) ←→OPSA (B port): OPSA (SIG port)←→SFD (OMD): SFD (Channel port)←→OT (line port)

4 Configure an unprotected optical transport service as described in Procedure 16-1 between the client ports of the OTs used in the configuration in step 3.

Note — The OPS Protected OTU trail is created automatically by the 5620 SAM.

Procedure 16-19 To configure an OCHP protection service

1 Configure the OPSA cards as described in Procedure 9-5.

2 Configure the Protection Mode parameter as OCHP on the Card Specifics tab of the OPSA cards.

3 Configure the optical links for the following as described in Procedure 9-18:

OT (line port)←→OPSA (SIG port): OPSA (A port)←→SFD1 (Channel port): SFD1 (OMD port)←→AMP1 (SIG port): AMP1 (LINE port)←→AMP1 (LINE port): AMP1 (SIG port)←→SFD1 (OMD port): SFD1 (Channel port)←→OPSA (A port): OPSA (SIG port)←→OT (line port)

OT (line port)←→OPSA (SIG port): OPSA (B port)←→SFD2 (Channel port): SFD2 (OMD port)←→AMP2 (SIG port): AMP2 (LINE port)←→AMP2 (LINE port): AMP2 (SIG port)←→SFD2 (OMD port): SFD2 (Channel port)←→OPSA (B port): OPSA (SIG port)←→OT (line port)

4 Configure an unprotected optical transport service as described in Procedure 16-1 between the client ports of the OTs used in the configuration in step 3.

Note — The OPS Protected OTU trail is created automatically by the 5620 SAM.

Procedure 16-20 To configure an OLP service

1 Configure the OPSA cards as described in Procedure 9-5.

2 Configure optical links for the following as described in Procedure 9-18:

OT→SFD→AMP (line port)→OPSA (A port)→OPSA (A port)→AMP (line port)→SFD→OT

OT→SFD→AMP (line port)→OPSA (B port)→OPSA (B port)→AMP (line port)→SFD→OT

Note — The OTS trail is automatically created when the optical link is configured from OPSA (A port) to OPSA (A port) and OPSA (B port) to OPSA (B port). The OTS trail cannot be deleted.

3 Configure an unprotected optical transport service as described in Procedure 16-1, routing through the OTU trails automatically created in step 2.

Note — You can route the service through the OTU trails by choosing the client port of the OTs used for creating optical links in step 2 as termination points.

16.21 Procedures to configure client protection services

Procedure 16-21 To configure a client protected optical service on OCS devices

Before performing this procedure, ensure that you configure the I/O cards with the OTU rates in card slots 33 to 48 on an 1830 PSS-64 device, or in any I/O card slots of an 1830 PSS-36 device.

1 Perform Procedure 13-6 to configure an unprotected higher-order OTU trail between two I/O cards, with the Rate parameter configured as OTU2.

2 Perform Procedure 13-1 to configure an unprotected higher-order ODU trail between the sites containing the I/O cards used in step 1, with the Rate parameter configured as ODU2 and termination points as the ODUPOOLS of the sites.

3 Configure the required I/O cards with OC or STM rates on the sites used in steps 1 and 2.

4 Perform one of the following:

- **a** Configure the lower-order ODU trail and discover the client protected service:
  - **i** Perform Procedure 13-1 to configure an SNCNC protected lower-order ODU trail between the two client ports of I/O cards configured in step 3, with the Rate parameter configured as ODU0.
  - **ii** Perform Procedure 16-3 to discover the service between the termination points used in step i. Before discovering the optical service, ensure that the necessary optical links are configured as required.
- **b** Perform Procedure 16-1 to configure a client protected service between the two client ports of I/O cards configured in step 3, with the Rate parameter set to an OC or STM rate, as required. Before configuring the optical service, ensure that the necessary optical links are configured as required. The lower-order ODU trail between the two client ports of I/O cards configured in step 3 is created automatically.

Procedure 16-22 To configure a client protected service with double add-drop

Before performing this procedure, ensure that you configure the I/O cards with the OTU rates in card slots 33 to 48 on an 1830 PSS-64 device, or in any of the I/O card slots of an 1830 PSS-36 device.

1 Perform steps 1 and 2 of Procedure 16-21, twice, to create two unprotected OTU and ODU trails.

2 Perform steps 3 and 4 of Procedure 16-21.

3 Click on the Path Constraints tab and configure one of the OTU trails as the Working constraint and the other as Protection constraint.

4 Save your changes and close the form.

16.22 112SDX11 card—OTN layer management and service configuration

The 112SDX11 card has an OTM-0.4v4 interface carrying a four-lane optical signal containing one OTU4. The L1 port of the 112SDX11 card is configured with the signal rate of OTL4.4. The OTL4.4 signal is mapped to four optical transport lane carriers or OTLC physical ports, L1 to L4. The four OTLC signals are multiplexed into one OTLC group, identified as OTLCG. The L1 to L4 ports belong to one OTLCG and the optical attributes of the ports are provisioned only on the first port. The frequency and primary state of the L2, L3, and L4 port are determined by the parameters provisioned on the L1 port.

The OTLCG signal is mapped to an OPSMnk. The OPSMnk is a physical optical signal consisting of four multilanes using wavelength division multiplexing for n = 4 and containing one OTU4 signal.The OPSMnk signal is sent to the OTM-0.4v4 interface.

The 5620 SAM supports configuration of the OCH cross-connect groups on the 112SDX11 card. The OCH cross-connect groups are automatically created during a service configuration and the OCH cross-connect group comprises the OCH cross-connects. See Procedure 16-24 for more information about viewing the OCH cross-connect groups for an 1830 PSS device.

The 5620 SAM automatically creates the underlying optical trails during service configuration. One LO-ODU trail, one HO-ODU trail, one OTU trail, and four OCH trails—one each from the L1 to L4 ports—are created during the service configuration and can be viewed from the 5620 SAM.

The first OCH trail (associated with the L1 port) is called the primary OCH trail and the remaining three OCH trails (associated with the L2 to L4 ports) are called sibling OCH trails. You can view the OCH cross-connect groups from the primary OCH trail. The sibling OCH trails display only the OCH cross-connects. See Procedure 16-25 for more information about viewing the OCH cross-connect groups from the primary OCH trail.

Dual-rate support

The 112SDX11 card supports the configuration of dual-rate (default 100GbE and OTU4) 100GBASE-LR4 CFP in the OTU4 mode on the L1 port to interconnect with the external OTN networks. The Pluggable Module Type parameter of the L1 port is set to C113G4Cd on the Port Specifics→General tab of the Physical Port (Edit) form. When the 112SDX11 card is configured with the CFP module on a line port, the device be connected to the external OTN network with another device configured with the same 100GBASE-LR4 CFP. The external OTN network provides an unterminated ODU4 connection between the 112SDX11 cards.

ISL trunking

The 5620 SAM supports ISL trunking through client ports assigned with rates FC400, FC800, or FC1600 on the 112SDX11 card. To establish ISL trunking using 5620 SAM:

- Configure the same Link Group ID on the client ports with rates FC400, FC800, or FC1600 on the 112SDX11 cards of two 1830 PSS devices.
- Configure an optical transport service with one of the client ports from each of the 1830 PSS devices as termination points.

SR-SR optical transport service using fan-out cable

The 5620 SAM allows you to discover an optical transport service between two 7750 SR devices that are connected to two 1830 PSS devices using a fan-out cable. One end of the fan-out cable is connected to a 100GbE port on a 7750 SR device and the other ten ends are connected to ten client ports, each with the CBR10G3 rate of the 112SDX11 card configured on an 1830 PSS device. You must first configure an optical transport service between the two 1830 PSS devices, then discover the service on the 7750 SR devices.

- Before configuring the optical transport service between the two 1830 PSS devices, set the Link Group ID parameter to the same value on all ten client ports of the 112SDX11 card connected to the fan-out cable on each of the 1830 PSS devices. The Link Group ID parameter is on the OT panel of the General sub-tab of the Port Specifics tab of the physical port properties form.
- Before creating the service, delete the optical links between the client ports of 112SDX11 cards on the 1830 PSS devices and the 100GbE cards on the 7750 SR devices. Create an optical transport service, with a rate of CBR10G3, between two client ports of the two 112SDX11 cards on the 1830 PSS devices. The 5620 SAM automatically creates nine more optical transport services.
- After configuring the optical transport service between the two client ports of the 112SDX11 cards, recreate the optical link between the client ports of the 112SDX11 cards, used to create the optical transport service, and the ports of the 100GbE cards on the 7750 SR devices. Choose Optical Transport Service→Discover Transport Services on the Manage Services form. The services from the remaining client ports of the 112SDX11 cards are discovered by 5620 SAM. All the client ports are extended to the 7750 SR device and one of the termination points of all the ten services is the same port of the 100GbE card on the 7750 SR device.

Note — You can also discover optical transport services in the same way, when one end of the fan-cable is connected to a 40GbE port on a 7750 SR device and the other four ends are connected to four client ports, each with the CBR10G3 rate of the 112SDX11 card configured on an 1830 PSS device.

Procedure 16-23 To configure an OMSP protection service using 112SDX11

1 Configure the OPSA cards as described in Procedure 9-5.

2 Configure the Protection Mode parameter as OMSP on the Card Specifics tab for the OPSA cards.

3 Configure the optical links for the following as described in Procedure 9-18:

OT (L1 to L4)←→MVAC8B (C1 to C4): MVAC8B (L1 to L4)←→SFD (Channel port): SFD (OMD)←→OPSA (SIG port): OPSA (A port)←→AMP1 (SIG port): AMP1 (LINE port)←→AMP1(LINE port): AMP1 (SIG port) ←→OPSA (A port): OPSA (SIG port)←→SFD (OMD): SFD (Channel port)←→MVAC8B (C1 to C4): MVAC8B (L1 to L4)←→OT (L1 to L4)

OT (L1 to L4)←→MVAC8B (C1 to C4): MVAC8B (L1 to L4)←→SFD (Channel port): SFD (OMD)←→OPSA (SIG port): OPSA (B port)←→AMP2 (SIG port): AMP2 (LINE port)←→AMP2 (LINE port): AMP2 (SIG port) ←→OPSA (B port): OPSA (SIG port)←→SFD (OMD): SFD (Channel port)←→MVAC8B (C1 to C4): MVAC8B (L1 to L4)←→OT (L1 to L4)

See steps 4 and 5 for more information about the sequence of configuring the optical links for unkeyed and keyed services respectively.

Unkeyed service

4 To configure the optical links between 112SDX11 L(1 to 4) ports to the SFD channel ports for an unkeyed service:

i Configure four optical links, from the 112SDX11 card line ports L1 to L4 to the SFD channel ports.

If the L1 port does not have the frequency set, the 1830 PSS creates a connection and automatically sets the port frequency to the SFD channel frequency value.

ii Configure L1 optical links before L2 to L4 links because only the wavelength of L1 can be configured. The L1 optical link must be deleted after L2 to L4 links are deleted.

If the L1 to L4 ports are configured with a frequency that is different from the SFD channel, the 1830 PSS does not create a connection.

Keyed service

5 Perform one of the following for a keyed service.

a To configure the optical links between the 112SDX11 L(1 to 4) ports to the MVAC8B C(1 to 8) ports and the SFD channel ports:

- The optical link from the MVAC8B line to the SFD must be created before the optical link from the OT line to the MVAC8B client is created.
- The optical link from the OT line to the MVAC8B client must be deleted before the optical link from the MVAC8B line to the SFD channel is created.
- If the L1 to L4 ports have the frequency set to a different value than the MVAC8B line frequency, the 1830 PSS does not create the connection.
- If the L1 port does not have the frequency set, the 1830 PSS creates a connection and automatically sets the port frequency to the SFD or MVAC8B line frequency value.

b To configure the optical links between the 112SDX11 L(1 to 4) ports to the MVAC G(1 to 8) ports and the SFD channel ports:

- The optical link from the MVAC G port to the SFD must be created before the optical link from the 112SDX11 line to the MVAC G port is created.
- The optical link from the 112SDX11 line to the MVAC G port must be deleted before the optical link from the MVAC G port to the SFD channel is created.
- If the 112SDX11 L1 to L4 ports have the frequency set to a different value than the MVAC G frequency, the 1830 PSS does not create the connection.
- If the L1 port does not have the frequency set, the 1830 PSS creates a connection and automatically sets the port frequency to the SFD or MVAC G frequency value.

6 Configure an unprotected optical transport service as described in Procedure 16-1 between the client ports of the OTs used in the configuration in step 3.

Note — The OPS Protected OTU trail is created automatically by the 5620 SAM.

Procedure 16-24 To view the OCH cross-connect group from the NE

1 On the equipment tree, expand Network→1830 PSS.

2 Right-click on the 1830 PSS object and choose Properties. The Network Element (Edit) form opens.

3 Click on the OCH Cross-Connect Groups tab, choose an OCH cross-connect group, and click properties. The OCH Cross Connect Group (Edit) form opens.

4 Click on the OCH Cross-Connects tab. The OCH cross-connects are listed.

Procedure 16-25 To view the OCH cross-connect group from the primary OCH trail

1 Choose Manage→OTN→OTN Trails from the 5620 SAM main menu.

2 Choose OCH Trail (Optical Management) from the object drop-down menu. The OCH trails are listed.

3 Choose the primary OCH trail and click Properties. The OCH Trail (Edit) form opens.

4 Click on the Trail Paths and on the OCH Trail Path object on the OCH trail tree. The OCH trail path attributes appear on the right panel.

5 Click on the OCH CrossConnect tab, choose an OCH cross-connect group, and click Properties. The OCH Cross Connect Group (Edit) form opens.

6 Click on the OCH CrossConnects tab. The OCH cross-connects are listed.

Procedure 16-26 To bind and collapse HO-ODUk timeslots

1 On the equipment tree, expand Network→1830 PSS→Shelf→Card→Port→ODU.

2 Perform one of the following:

a To open the ODU NIM (Edit) form, right-click on the OTUODUk object and choose Properties.

b To open the ODU Path Termination (Edit) form, right-click on the ODUk object and choose Properties.

3 Click on the ODU Structure tab.

4 Choose two ODU0s, eight ODU0s, or four ODU1s, and click Bind Timeslots. The LO-ODUk Configuration form opens.

Note — Bind timeslots as follows:

- Two ODU0s to form one ODU1.
- Four ODU1s or eight ODU0s to form one ODU2.

5 Configure the required parameters and click OK.

6 Scroll to the bottom of the list to view the newly created timeslot.

7 Choose a bound timeslot and click Collapse Timeslots to retrieve the initial timeslots.

16.23 Procedures to configure dual-stage muxing services

Procedure 16-27 To configure dual-stage multiplexing services on an 1830 PSS for keyed and unkeyed services

Dual-stage multiplexing service support is provided on the 1830 PSS 16/32 shelves for the following cards:

- 11DPM12 OTU1 client port (OT A) connected to a 4DPA4 line port (OT B). Up to four 4DPA4 OTs can be connected to one 11DPM12.
- 11QPEN4 client port (OT A) connected to an 11DPE12A line port (OT B). Up to four 11DPE12A OTs can be connected to one 11QPEN4.
- 11QPEN4 client port (OT A) connected to an 11OPE8 line port (OT B). Up to four 11OPE8 OTs can be connected to one 11QPEN4.
- 11QPEN4 client port (OT A) connected to an 11QPE24 line port (OT B). Up to four 11QPE24 OTs can be connected to one 11QPEN4.
- 11STMM10 OTU1 client port (OT A) connected to a 4DPA4 line port (OT B). Up to four 4DPA4 OTs can be connected to one 11STMM10.
- 43SCX4 and 43SCX4E OTU2 client port (OT A) connected to an 11DPM12 line port (OT B). Up to four 11DPM12 OTs can be connected to one 43SCX4 or 43SCX4E.
- 43SCX4E client port (OT A) connected to an 11DPE12A line port (OT B). Up to four 11DPE12A OTs can be connected to one 43SCX4E.
- 43SCX4E client port (OT A) connected to an 11OPE8 line port (OT B). Up to four 11OPE8 OTs can be connected to one 43SCX4E.
- 43SCX4E client port (OT A) connected to an 11QPE24 line port (OT B). Up to four 11QPE24 OTs can be connected to one 43SCX4E.
- 43STX4P OTU2 client port (OT A) connected to an 11DPM12 line port (OT B). Up to four 11DPM12 OTs can be connected to one 43STX4P.
- 112SCX10 OTU2 client port (OT A) connected to an 11DPM12 line port (OT B). Up to ten 11DPM12 OTs can be connected to one 112SCX10.
- 112SCX10 OTU2 client port (OT A) connected to an 11QPEN4 line port (OT B). Up to ten 11QPEN4 OTs can be connected to one 112SCX10.
- 112SDX11 OTU2 client port (OT A) connected to an 11DPM12 line port (OT B). Up to ten 11DPM12 OTs can be connected to one 112SDX11.
- 112SNX10 OTU2 client port (OT A) connected to an 11DPM12 line port (OT B). Up to ten 11DPM12 OTs can be connected to one 112SNX10.
- 112SNX10 OTU2 client port (OT A) connected to an 11QPEN4 line port (OT B). Up to ten 11QPEN4 OTs can be connected to one 112SNX10.
- 112SNX10 client port (OT A) connected to an 11DPE12A line port (OT B). Up to ten 11DPE12A OTs can be connected to one 112SNX10.

- 112SNX10 client port (OT A) connected to an 11OPE8 line port (OT B). Up to ten 11OPE8 OTs can be connected to one 112SNX10.
- 112SNX10 client port (OT A) connected to an 11QPE24 line port (OT B). Up to ten 11QPE24 OTs can be connected to one 112SNX10.
- 130SCX10 OTU2 client port (OT A) connected to an 11QPEN4 line port (OT B). Up to ten 11QPEN4 OTs can be connected to one 130SCX10.
- 130SCX10 OTU2 client port (OT A) connected to an 11DPM12 line port (OT B). Up to ten 11DPM12 OTs can be connected to one 130SCX10.
- 130SCX10 client port (OT A) connected to an 11DPE12A line port (OT B). Up to ten 11DPE12A OTs can be connected to one 130SCX10.
- 130SCX10 client port (OT A) connected to an 11OPE8 line port (OT B). Up to ten 11OPE8 OTs can be connected to one 130SCX10.
- 130SCX10 client port (OT A) connected to an 11QPE24 line port (OT B). Up to ten 11QPE24 OTs can be connected to one 130SCX10.

Prerequisites:

- An internal topological link is provisioned between the OT A client port and the OT B line port.
- The cross-connect terminates on the OT A line port. The OT B is not included in the cross-connect.
- Because there is no wave key encoding on OT B, the eVOA port is not used.
- There is no alarm correlation between OT A and OT B.

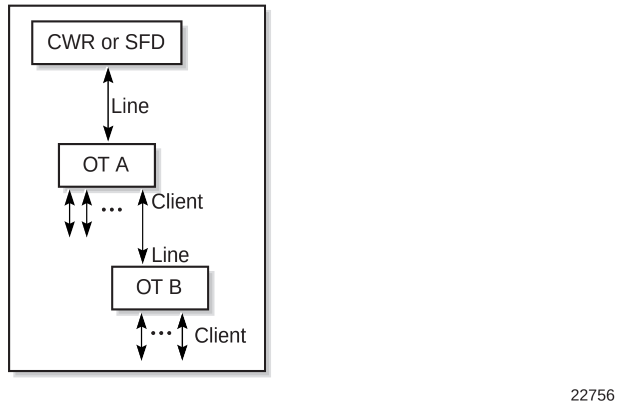
Note 1 — Dual Trans mode and Flex Mux mode are supported on the 4DPA4 card.

Note 2 — Keyed and unkeyed services are supported in the Wave key Assign mode.

See Procedure 16-1 to create an optical service. See Procedure 15-1 to create a VPLS service. See Procedure 25-1 to create an Ethernet ring.

Figure 16-1 shows the dual-stage multiplexing.

Figure 16-1 Dual-stage multiplexing



Procedure 16-28 To configure CWDM and DWDM single fiber bidirectional service

You can configure single fiber, bidirectional service on the 5620 SAM by creating two unidirectional trails between the same client ports using SFDs or SFCs. Each bidirectional transmission requires different CWDM or DWDM wavelengths in each direction. This is accomplished with two fiber connections in the transmit and receive directions from the OT to two adjacent wavelengths connections on the MUX (in) side of the filter.

The CWDM single fiber, bidirectional unkeyed service support on the 1830 PSS-4/16/32 is provided for the following fiber and OT cards:

- SFC-2
- SFC-4
- SFC-8
- 4DPA4
- 11STAR1
- 11STAR1A
- 11STMM10
- 11DPE12(E)

The DWDM single fiber, bidirectional, keyed and unkeyed service support on the 1830 PSS-4/16 is provided for the following fiber and OT cards:

- SFD-4
- SFD-8
- SFD-44 (1830 PSS-16)
- 11QPA4
- 11DPM12
- 112SDX11 (1830 PSS-16)
- 130SCA1 (1830 PSS-16)
- 4DPA4
- AHPHG (keyed service)

Prerequisites:

- The SFC must be connected in a OneFiber MuX mode. The default is TwoFiberMux. You must set the mode before you create an optical link. The mode can be configured on the Card Specifics tab of the Card (Edit) form. See

Procedure 9-7 for more information.

- You can only create unidirectional internal optical links between the OT and filter channels.
- External optical links are always bidirectional. After the service is created, you can view the channel, frequency used, and direction in the topology view.

Perform Procedure 16-1 to configure an optical service.

For more information about single fiber, bidirectional services, see the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide*.

16.24 Procedures to configure APS groups

Procedure 16-29 To configure an APS group

1 On the equipment tree, expand Network→1830 PSS.

2 Right-click on the 1830 PSS object and choose Properties. The Network Element (Edit) form opens.

3 Click on the APS Groups tab, then click Create. The APS Group (Create) form opens.

4 Configure the required parameters in the Protection Attributes panel:

5 Select a port in the Port panel, if applicable.

6 Select a working LO-ODUk facility in the Working LO-ODUk facility panel, if applicable.

7 Select a protection LO-ODUk facility in the Protection LO-ODUk facility panel, if applicable.

8 Select a working port in the Working Port panel, if applicable.

9 Select a protection port in the Protection Port panel, if applicable.

10 Configure the required parameters as applicable:

- Channel
- Working VTS
- Protection VTS

11 Click OK. The APS Group (Create) form closes.

Procedure 16-30 To modify the protection switch for an APS group

You can modify the protection switch from the Network Element (Edit) form or from the Optical Transport Service (Edit) form.

1 Perform one of the following to open the APS Group (Edit) form.

a From the Network Element (Edit) form:

i Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

ii Choose Network→1830 PSS.

iii Right-click on the 1830 PSS device object and choose Properties. The Network Element (Edit) form opens.

iv Click on the APS Groups tab. A list of APS groups appears.

v Choose an entry and click Properties. The APS Group (Edit) form opens.

b From the Optical Transport Service (Edit) form.

i Choose Manage→Service→Services from the 5620 SAM main menu.

ii Choose Optical Transport Service from the drop-down menu.

iii Click Search and choose the protected optical transport service for which the protection switch needs to be modified.

iv The Optical Transport Service (Edit) form opens.

v Click on the APS Groups tab. A list of APS groups appears.

vi Choose an entry and click Properties. The APS Group (Edit) form opens.

2 Choose the protection switch type based on the working or protection path in the Protection Switch drop-down menu of the Protection Management panel. The options for Protection Switch parameter are:

- Protection Lockout
- Forced Switch to Protection
- Forced Switch to Working
- Manual Switch to Protection
- Manual Switch to Working
- No Cmd

Note — The Protection Switch drop-down menu is active only when the card on which the protection port is present is equipped on the 1830 PSS device.

3 Click OK. The APS Group (Edit) form closes.

16.25 Procedures to configure services using LAGs

Procedure 16-31 To configure 11DPE12A service using LAGs

1 Create LAGs on SR. See Procedure “To create a LAG” in the *5620 SAM User Guide* for information about creating LAGs on an SR.

2 Create LAGs on an 11DPE12A card. See Procedure 9-24.

3 Create optical links between the SR and 11DPE12A LAG ports. See Procedure 9-18.

4 Choose Create→Service→Optical→Create Transport Service from the 5620 SAM main menu. The Optical Transport Service (Create) form opens.

5 Click Select in the Customer panel to choose a customer to associate with the optical transport service. The Select Customer - Optical Transport Service form opens.

6 Choose a customer for the optical transport service and click OK. The Select Customer - Optical Transport Service form closes and the Optical Transport Service (Create) form reappears with the customer information displayed on the General tab.

7 Configure the required parameters:

- Service Name
- Description
- Service ID

8 Set the Rate parameter to SubGigE.

9 Configure the required parameters in the VLAN Configuration Details panel:

- Is SubGigE Service QinQ
- CE-VLANID-AZ
- CE-VLANID-ZA
- Stack-VLANID-AZ
- Stack-VLANID-ZA

10 Click on the Service Sites tab and click Create. The Select Network Elements - Optical Transport Service form opens with a list of sites.

11 Choose the SR sites and click OK. The A and Z sites are displayed in the navigation tree.

12 Choose A End in the Service Sites tab and click Properties. The Optical Site (Create) form opens.

13 Click on the Termination Point tab and click Create on the right panel. The Termination Point (Create) form opens

14 Click Select. The Select Termination Point form opens.

15 Choose the one of the LAG ports and click OK. The Select Termination Point form closes and the Termination Point (Create) form reappears.

16 Configure the required parameters in the Optical Access Port Virtual Time Slot panel:

- Ingress VTS Number
- Egress VTS Number

17 Configure the required parameters in the Optical Working Network Port Virtual Time Slot panel:

- Line Port
  Click Select. The Select Line Port - Termination Point form opens with a list of line ports. Choose the line port.
- Ingress VTS Number
- Egress VTS Number

18 Click Apply. The Termination Point (Create) form closes and the Optical Transport Service (Create) form reappears.

19 Perform steps 12 to 18 to add the termination point for Site B.

20 Click OK to complete the service configuration.

16.26 Procedures to configure timeslots

Procedure 16-32 To configure a port-timeslot assignment on channelized cards

1 Right-click on a channelized port and choose Properties. The Physical Port (Edit) form opens.

2 Click on the Port Specifics tab.

3 Configure the Assigned Rate parameter.

4 Click Configure Timeslots. The Timeslot Assignments form opens.

5 Choose the required timeslot configuration and click OK. The Timeslot Assignments form closes.

6 Click OK. The Physical Port (Edit) form closes.

16.27 Procedures to configure VTS maps and XCs

Procedure 16-33 To configure VTS maps on 11DPE12/E/A cards

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→NE→Shelf→Card→Port.

3 Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

4 Click on the Port Specifics tab and click on the VTS Map tab.

Note — You can see the VTS Map tab on the Physical Port (Edit) form of a port on the 11DPE12 card, only when the Card Rate Mode parameter is set as QinQ in the Card Slot (Edit) form of the 11DPE12 card.

5 Click Create. The Port Specifics (Create) form opens.

6 Configure the required parameters:

- VTS Map Number
- VTS Direction
- Classification Mode

Note — If the Classification Mode is configured to Port in case of a client port VTS map configuration, go to step 8.

7 Configure the VTS map information based on the values configured for the VTS Direction and Classification Mode parameters:

a VTS Egress CE-VLANID—If the VTS Direction is configured to Egress and Classification Mode is configured to CE-VLAN Tagged or Untagged

b VTS Egress S-VLAN ID—If the VTS Direction is configured to Egress and Classification Mode is configured to S-VLAN Tagged

c VTS Ingress CE-VLAN ID—If the VTS Direction is configured to Ingress and Classification Mode is configured to CE-VLAN Tagged or Untagged

d VTS Ingress S-VLAN ID—If the VTS Direction is configured to Ingress and Classification Mode is configured to S-VLAN Tagged

e CE-VLAN ID—If the VTS Direction is configured to Ingress and Egress and Classification Mode is configured to CE-VLAN Tagged or Untagged

f Stack-VLAN ID—If the VTS Direction is configured to Ingress and Egress and Classification Mode is configured to S-VLAN Tagged

8 Click OK. The Port Specifics (Create) form closes and the VTS map is added to the list of maps under the VTS Map tab.

9 Click OK. The Physical Port (Edit) form closes.

Procedure 16-34 To configure VTS XCs on 11DPE12/E/A cards

Perform Procedure 16-33 before configuring a VTS cross-connect.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→NE.

3 Right-click on the NE and choose Properties. The Network Element (Edit) form opens.

4 Click on the VTS Connections tab.

5 Click Create. The VTS Connection (Create) form opens.

6 Configure the VTS Connection Name parameter.

7 Click Select in the VTS Connection Source panel. The Select VTS Connection Source Port form opens.

8 Choose a port from the list and click OK. The Select VTS Connection Source Port form closes.

9 Configure the Source VTS Number parameter in the VTS Connection Source panel.

10 Click Select in the VTS Connection Destination panel. The Select VTS Connection Destination Port form opens.

11 Choose a port from the list and click OK. The Select VTS Connection Destination Port form closes.

12 Configure the Destination VTS Number parameter in the VTS Connection Destination panel.

13 Configure the required parameters on the VTS Connection Details panel:

- Committed Information Rate(Mb/s)
- Peak Information Rate(Mb/s)
- Committed Burst Size(kb/s)
- Peak Burst Size(kb/s)

14 Click OK. The VTS Connection (Create) form closes.

17 — 1830 PSS mirror service management

17.1 Mirror service management

In a mirror service, packets from one or more sources are forwarded to their configured destinations. 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 that can be added under a mirror service. The mirrored packets are transported unidirectionally through the core network using IP or MPLS tunneling. For more information about mirror services, see *5620 SAM User Guide*.

Table 17-1 Mirror service management references

Topics	Chapter	Document
Mirror service overview	Mirror service management	*5620 SAM User Guide*
Sample mirror service configuration	Mirror service management	*5620 SAM User Guide*
Mirror service procedures	Mirror service management	*5620 SAM User Guide*

1830 PSS performance management

18 — 1830 PSS performance management

18.1 Performance monitoring overview

PM is the in-service, non-intrusive monitoring of transmission quality and equipment health. The 1830 PSS tracks the signal quality and equipment health through the continuous collection and analysis of performance data. The user can retrieve current and past values for an overview of the health of the system. The PM function applies to optical lines, channels, ports, and equipment. The user can provision threshold parameters to the required level of performance degradation.

Proactive maintenance refers to following up on a performance degradation before a failure and alarms are generated. Reactive maintenance refers to following up on a system alarm. Crossing a performance parameter threshold indicates a potential network quality or performance degradation when the transported services are not impacted. If performance degradation continues, alarms are generated to resolve or repair the problem.

The 5620 SAM supports viewing raw PM data from the 5620 SAM Equipment View application. See Procedure 10-1 for more information about launching the application. Right-click on the port icon and choose View Raw PM data. The data can be refreshed every 60, 90, 120, 150, or 180 seconds. You can export the data to CSV format by clicking on the Export Data to CSV icon.

PM thresholds

PM statistics are collected for all service cards and interface ports that perform OEO conversions or protection switching. The statistics are grouped by functional category. Each category has several monitored parameters for which you can configure TCAs. A threshold is the mechanism for generating a notification in response to changes in PM parameter values. The 1830 PSS allows you to provision performance parameter thresholds, which can be set by the user to indicate degraded performance. You can configure how much data is collected and stored, and how and when you are notified if thresholds levels are crossed. For information about performance management requirements see the *Alcatel-Lucent 1830 Photonic Service Switch User Provisioning Guide* and the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide*.

PM process

The 1830 PSS provides the following PM processing functions:

- monitor and accumulate digital and analog parameters for a physical or logical access point
- store and manage historical accumulated data; up to thirty two 15-minute and seven 24-hour accumulation registers can be stored
- validate threshold crossing processing
- assign threshold values to profile port entities
- use free-running counters for monitored points

PM functions are performed on physical and logical points within the 1830 PSS devices that represent the boundary with other devices or an external system. A user can define and monitor QoS at individual points in which a local NE interacts with other network entities.

18.2 Performance statistics

The 5620 SAM can be configured to collect statistics counters from 1830 PSS devices and 5620 SAM servers.

The 5620 SAM supports the following for 1830 PSS devices:

- assign the default 1830 PSS Performance Management Policy to the 1830 PSS device.
- enable the policy by setting the Administrative State to Up.
- configure the protocol for the statistics collection.
- specify a retention period in the Statistics Policy which indicates the period after which the statistics records are removed from the database.
- collect scheduled statistics using TFTP or SFTP to view historical statistics by selecting the required PM group and clicking Search.
- collect on-demand statistics using SNMP polling to view historical and real-time statistics by clicking Collect or Collect All.

Bins and intervals

The performance parameters groups obtained during the parameter processing are collected in registers over 15-min and 24-h measurement periods. A bin is the collection of registers associated with a PM group and collection period. The bins can be cleared by configuring the number of bins to be cleared for each interval. See Procedure 18-5 for information about clearing the 1830 PSS bins.

1830 PSS device

The 15-min bins collect data at quarterly time intervals (that is, 00, 15, 30, or 45) of the 1830 PSS clock. The 24-h bins collect data from midnight to midnight based on the UTC (not the local time). At the end of each 15-min time interval, the contents of the 15-min bin are transferred to the previous 15-min bin. The 15-min bins are then initialized to zero and a new record is initiated. Each PM group consists of thirty-two 15-min bins and seven 24-h bins. When the storage capacity of thirty-two 15-min bins is reached, the oldest bin is dropped. The 24-h bins are managed in the same way. 1830 PSS also supports raw bins for the parameters that can be monitored through raw bins for the supported PM profiles. The raw bins are 32-bit or 64-bit registers that count the monitored events until it rolls over, or are reset or cleared by the user.

1830 PSS statistics storage on the 5620 SAM server

The 1830 PSS statistics are stored in the following directory on the 5620 SAM server:

/opt/5620sam/server/nms/tftp_home/stats

The files are retained for 24 h by default.

Statistics collection

The file-based statistics are collected from the files on the 1830 PSS devices using TFTP or SFTP. The statistics are available for scheduled collection and enable viewing of the historical statistics.

The MIB-based statistics are collected from the 1830 PSS MIBs using SNMP polling. The statistics are available for on-demand collection and enable viewing of the real-time and historical statistics.

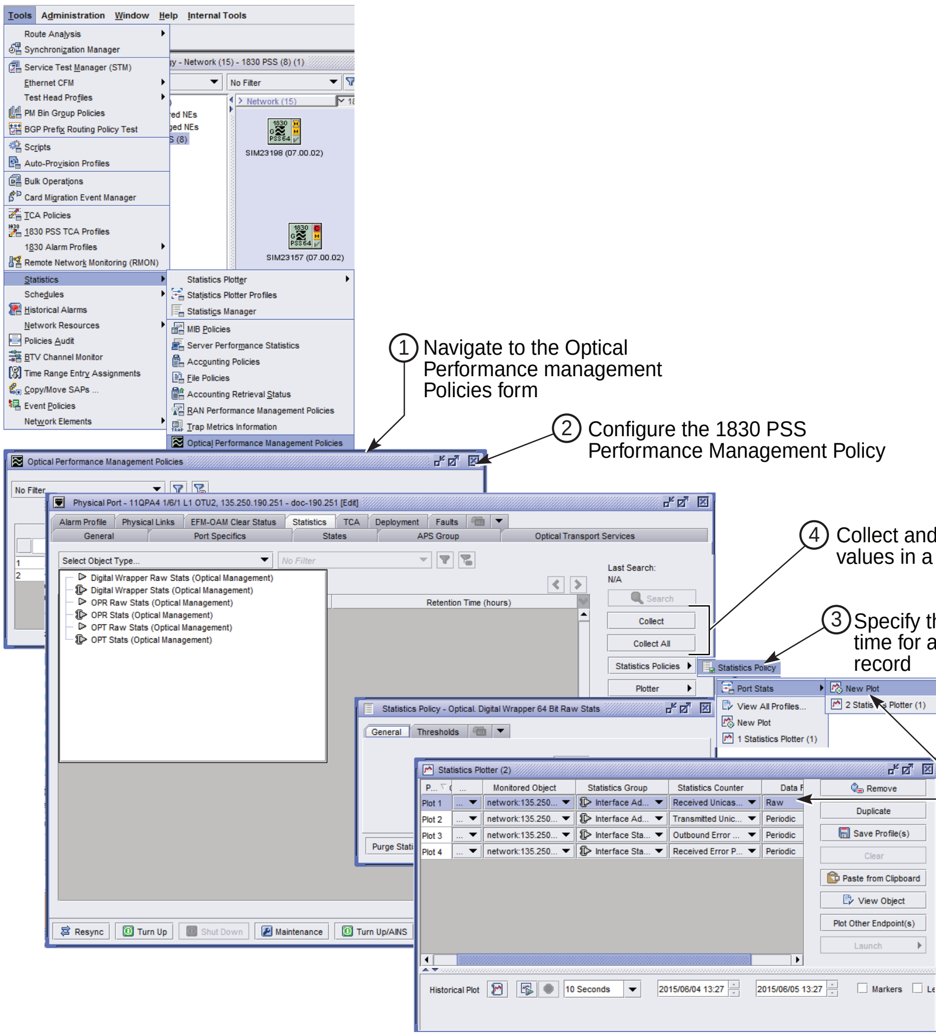
Scheduled and on-demand statistics are stored in the 5620 SAM database for a configurable retention period, as specified in Procedure 18-4, and are available to the 5620 SAM operators. When the retention period elapses, the statistics are removed from the database.

Statistics that are collected for real-time display are available only for the duration of the session and for the operator who initiates the session. Real-time statistics are not stored in the 5620 SAM database.

The 5620 SAM allows you to back up statistics data to another location. See “To back up the 5620 SAM database using the client GUI” in the *5620 SAM System Administrator Guide* for information about how to back up the 5620 SAM database.

18.3 Workflow for performance statistics collection

Figure 18-1 Performance management workflow



1 Modify 1830 PSS Performance Management Policy to assign 1830 PSS devices to the policy and enable the policy by setting the Administrative State to Up. See Procedure 18-1.

2 Specify the retention time for a statistics record. See Procedure 18-4.

3 Collect and display the statistics values in a current statistics record. See "To view on-demand statistics" in the *5620 SAM Statistics Management Guide* for information about viewing on-demand statistics.

4 Configure real-time and historical statistics graph. See “Graphical statistics view” in the *5620 SAM Statistics Management Guide* for information about creating a real-time and historical statistics graph.

5 Use the 5620 SAM-O interface to retrieve the performance statistics records from the 5620 SAM for processing by a third-party application. See the *5620 SAM XML OSS Interface Developer Guide* for information about using the 5620 SAM-O to transfer statistics records from the 5620 SAM database to an OSS client application.

18.4 1830 PSS statistics procedures

Perform the procedures in this section to configure the 5620 SAM for 1830 PSS statistics collection.

Procedure 18-1 To configure an 1830 PSS Performance Management Policy

1 Choose Tools→Statistics→Optical Performance Management Policies from the 5620 SAM main menu. The Optical Performance Management Policies form opens.

2 Choose the first default 1830 PSS performance management policy and click Properties. The 1830 PSS Performance Management Policy - 1 (Edit) form opens.

3 Configure the Administrative State parameter.

Note — The default value for the Administrative State parameter is Down for an 1830 PSS Performance Management Policy.

4 Perform one of the following to configure the Protocol parameter:

a Choose SFTP from the drop-down menu and configure the User ID and Password parameters.

b Choose TFTP from the drop-down menu.

5 Click Apply. A dialog box appears.

6 Click Yes.

7 Click on the 1830 PSS Elements tab.

8 Configure the filter criteria, if required, and click Search to generate a list of 1830 PSS elements that are already assigned to the 1830 PSS performance management policy.

9 Click Assign 1830 PSSs. The Assign “Default” and Assign “Default” Filter forms open.

10 Configure the filter criteria, if required, and click OK to close the Assign “Default” Filter form and return to the Assign “Default” form.

11 Use the right and left arrows to move the 1830 PSS devices between the Unassigned PSSs list and the Assigned PSSs list, as required.

12 Click Apply to deploy the 1830 PSS performance management policy to the assigned PSS.

Note — Alternatively, when an 1830 PSS device is discovered, the 5620 SAM assigns the default 1830 PSS performance management policy to it automatically.

13 Close the Assign “Default” form.

14 Click OK. The 1830 PSS Performance Management Policy - 1 (Edit) form closes.

15 Close the Optical Performance Management Policies form.

Procedure 18-2 To configure an 1830 PSS OCS performance management policy

1 Choose Tools→Statistics→Optical Performance Management Policies from the 5620 SAM main menu. The Optical Performance Management Policies form opens.

2 Choose the Default SFTP 1830 PSS performance management policy and click Properties. The 1830 PSS Performance Management Policy - 2 (Edit) form opens.

3 Configure the Administrative State parameter.

4 Configure the Protocol parameter as SFTP.

Note — Do not configure the Protocol parameter as TFTP for 1830 PSS OCS devices.

5 Configure the required parameters on the FTP Settings panel:

- User ID
- Password

6 Click Apply. A dialog box appears.

7 Click Yes.

8 Click on the 1830 PSS Elements tab.

9 Configure the filter criteria, if required, and click Search to generate a list of 1830 PSS elements that are already assigned to the 1830 PSS performance management policy.

10 Click Assign 1830 PSSs. The Assign “Default SFTP” form opens followed by the Assign “Default SFTP” Filter form.

11 Configure the filter criteria, if required, and click OK to close the Assign “Default SFTP” Filter form and return to the Assign “Default SFTP” form.

12 Use the right and left arrows to move the 1830 PSS devices between the Unassigned PSS list and the Assigned PSS list, as required.

13 Click Apply to deploy the 1830 PSS performance management policy to the assigned PSS.

Note — Alternatively, when an 1830 PSS device is discovered, the 5620 SAM assigns the default 1830 PSS performance management policy to it automatically.

14 Close the Assign “Default” form.

15 Click OK. The 1830 PSS Performance Management Policy - 2 (Edit) form closes.

16 Close the Optical Performance Management Policies form.

Procedure 18-3 To enable PMON configuration on an 1830 PSS OCS device

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose PMON Configuration (Optics Specifics) from the object drop-down menu and click Search. A list of available PMON configurations appears.

3 Choose one or more configurations from the list and click Properties. The PMON Configuration (Edit) form opens.

4 Select the Enable check box. The selected PMON configurations are enabled.

5 Configure the Mode Type parameter.

6 Click Clear PM Counters to clear the counters of the selected PMON counters, if required.

7 Select the Delete PM Bin History check box, if required.

8 Click OK. A dialog box appears.

9 Click Yes. The PMON Configuration (Edit) form closes and the Manage Equipment form reappears with the Enable field selected for the chosen PMON configurations.

10 Close the Manage Equipment form.

Procedure 18-4 To configure retention time for file-based statistics

1 On the navigation tree, expand Network→1830 PSS→Shelf→Card Slot→Port.

> **Note —** Choose the PM-supported ports.

2 Right-click on the Port and choose Properties. The Physical Port (Edit) form opens.

3 Click on the Statistics tab. The Administrative State and Retention Time columns are displayed.

4 Choose an object type from the Select Object Type drop-down menu.

5 Click Statistics Policies and choose the Statistics Policy from the drop-down menu. The Statistics Policy form appears with the name of the selected Object Type.

6 Configure the required parameters:

- Retention Time (hours)
- Administrative State

7 Click on the Purge Statistics Records to purge all statistics records. If the buttons are not visible, click More Actions and choose the corresponding option from the drop-down menu.

8 Click OK. A dialog box appears. Click Yes. The Statistics Policy form closes.

9 Click OK. The Physical Port (Edit) form closes.

Procedure 18-5 To clear the 1830 PSS bins on an EC card

1 On the navigation tree, expand Network→1830 PSS→Shelf→EC Card.

2 Right-click on the EC card and choose Properties. The Card Slot (Edit) form opens.

3 Click on the Card Specifics tab.

4 Click on the Performance tab.

5 Choose either 15-min or 24-h bin, and click Properties. The TCA Profile Assignment form opens.

6 Configure the Number of Bins parameter.

7 Click Clear Count and perform one of the following actions:

a Choose Bins to clear the 15-h or 24-h bin

b Choose Raw Bins to clear the raw bin counters

8 Close the TCA Profile Assignment form. The Card Slot (Edit) form reappears.

9 Click on the Show All Tabs tab. Click on the Statistics tab.

10 Choose the profile type for which the bins are cleared and click Collect. The new counts are displayed.

11 Close the Card Slot (Edit) form.

Procedure 18-6 To clear the 1830 PSS bins on a port

1 On the navigation tree, expand Network→1830 PSS→Shelf→Card→Port.

2 Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

3 Click on the Port Specifics tab.

4 Click on the Performance tab.

Note — For 11QPE24 ports, click on the Port TCA Profile Assignment tab under the Performance tab.

5 Choose either 15-min or 24-h bin, and click Properties. The TCA Profile Assignment form opens.

6 Configure the Number of Bins parameter, if required.

7 Click Clear Count and perform one of the following actions:

a Choose Bins to clear the 15-min or 24-h bin

b Choose Raw Bins to clear the raw counts

8 Close the TCA Profile Assignment form. The Physical Port (Edit) form reappears.

9 Click on the Show All Tabs tab. Click on the Statistics tab.

10 Choose the profile type for which the bins are cleared and click Collect. The new counts are displayed.

11 Close the Physical Port (Edit) form.

18.5 PM profile types supported for line ports on amplifier cards

Inter-device management and control information is communicated over the amplifier cards. The amplifier card line ports support their statistics profiles. The amplifier is a separate optical channel that operates at the STM-1/OC-3 rate of 155 Mb/s. The amplifier card transfers management and control information between the ECs of two adjacent NEs, regardless of whether any of the DWDM payload channels are terminated between the two NEs. The channel transports IP and OSI PDUs. See the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide* for more information.

18.6 Managing TCA profiles

The 5620 SAM supports all of the TCAs that are provided by the NE. The support includes configuring thresholds, distributing TCA profiles, and reporting, for example, generating and clearing appropriate alarms. See the *Alcatel-Lucent 1830 Photonic Service Switch User Provisioning Guide* for more information about TCA support on the 1830 PSS.

TCA profiles

You can configure and assign a profile to an interval to monitor the value of each parameter in the active bin and generate a log event if a threshold level is reached. If a specified threshold is crossed, an alarm is generated.

You can configure each PM group with up to eight profiles. Each profile can have different threshold levels. The 5620 SAM allows you to modify the TCA profiles. The threshold levels that you configure depend on the following factors:

- interval length—for example, to gather statistics for an interface over 15-min and 24-h intervals you must define two profiles: one for each interval
- service level of the traffic using the interface

18.7 Workflow to manage TCA profiles

1 Configure a global or local 1830 PSS TCA profile.

  a Configure a global 1830 PSS card TCA profile, release, and distribute the policy to an 1830 PSS WDM device, or create a local 1830 PSS card TCA profile at an L2 card level on an 1830 PSS WDM device, as required. See Procedure 18-7.

  b Configure a global 1830 PSS OCS TCA profile, release, and distribute the policy to an 1830 PSS OCS device. See Procedure 18-11.

2 Assign a TCA profile to supporting objects.

a Assign an Ethernet TCA profile to an L2 card port or a SAP. See Procedure 18-8.

b Assign a TCA profile to an EC card slot or other card ports. See Procedure 18-9.

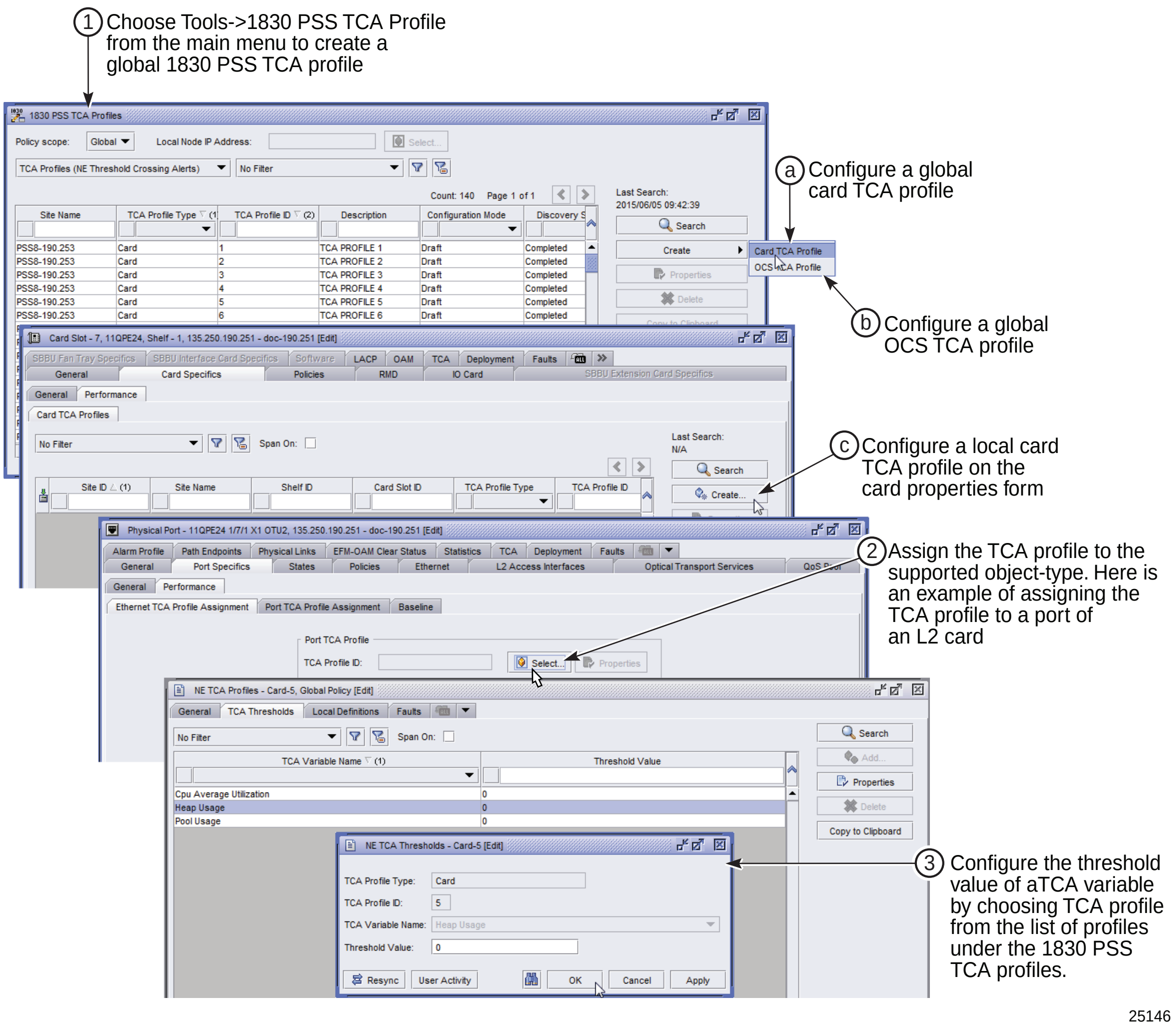
c Assign an OCS TCA profile to the supporting objects of an 1830 PSS OCS device, as required. See Procedure 18-12.

3 Configure the threshold values of a TCA profile, as required.

a Configure the NE and card TCA profile threshold values, as required. See Procedure 18-10.

b Configure the OCS TCA profile threshold values, as required. See Procedure 18-13.

Figure 18-2 TCA profile management



18.8 TCA profile management procedures

Procedure 18-7 To configure L2 card TCA profile

1 Perform one of the following:

a Open the 1830 PSS Card TCA Profile, Global Policy (Create) form from the 5620 SAM main menu.

i Choose Tools→1830 PSS TCA Profiles from the 5620 SAM main menu. The 1830 PSS TCA Profiles form opens.

ii Choose Card TCA Profiles (NE Threshold Crossing Alerts) from the object drop-down menu.

iii Click Create and choose Card TCA Profile. The 1830 PSS Card TCA Profile, Global Policy (Create) form opens.

b Open the 1830 PSS Card TCA Profile, Local Policy (Create) form from the card properties form.

i On the navigation tree, expand Network→NE→Shelf→Card.

ii Right-click on the card and choose Properties. The Card Slot (Edit) form opens.

iii Click on the Card Specifics tab and click on the Performance tab.

iv Click Create. The 1830 PSS Card TCA Profile, Local Policy (Create) form opens.

2 Configure the required parameters:

- TCA Profile Type
- TCA Profile ID
- Description
- Number of 15-min Bins
- Number of 1-day Bins

3 Click OK. The 1830 PSS Card TCA Profile (Create) form closes and the 1830 PSS TCA Profiles form reappears with the policy listed.

4 To distribute a global policy created using step 1 option a:

i Choose the global policy from the list of policies in the 1830 PSS TCA Profiles form and click Properties. The 1830 PSS Card TCA Profile, Global Policy (Edit) form opens.

ii Click Switch Mode. A dialog box appears.

iii Click Yes. The value of the Configuration Mode parameter changes to Released and the Release - Card TCA Profile form opens.

iv Choose the nodes from the Available Nodes list and click on the right-arrow button. The selected nodes move to the Selected Nodes list.

v Click Distribute.

vi Close the Release - Card TCA Profile form and the 1830 PSS Card TCA Profile, Global Policy (Edit) form.

5 Close the 1830 PSS TCA Profiles form.

Note — See Procedure 18-10 to configure TCA threshold values.

Procedure 18-8 To assign an Ethernet TCA profile to an L2 card port or SAP

1 To assign an Ethernet TCA profile to an 11QPE24 port or SAP:

a To assign an Ethernet TCA profile to an 11QPE24 port:

i On the navigation tree, expand Network→NE→Shelf→Card→Port.

ii Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

iii Click on the Port Specifics tab and click on the Performance tab.

iv Click Select beside the TCA Profile ID parameter in the Port TCA Profile panel. The Select Port TCA Profile form opens displaying a list of port TCA profiles.

b To assign an Ethernet TCA profile to a SAP:

i Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels form opens.

ii Choose Service Management→ VPLS in the object drop-down box and click Search.

iii Choose the required VPLS service from the list and click Properties. The VPLS Service (Edit) form opens.

- **iv** Choose VPLS Service→Sites→Site→L2 Access Interfaces→L2 Access Interface Port.

- **v** Click Select beside the TCA Profile ID parameter in the SAP TCA Profile panel. The Select SAP TCA Profile form opens displaying a list of SAP TCA profiles.

2 Choose a TCA profile and click OK. The TCA Profile selection form closes.

Note — See Procedure 18-14 to generate TCA alerts after the TCA profile is assigned.

Procedure 18-9 To assign TCA profiles to an EC card slot and other card ports

You can assign unique profiles for 15-min intervals and 24-h intervals for each EC card and port.

1 On the navigation tree, perform one of the following actions:

- **a** To assign the TCA profile to EC card slot:
  - **i** Expand Network→NE→Shelf→ EC Card on the equipment tree.
  - **ii** Right-click on the card and choose Properties. The Card Slot (Edit) form opens.
  - **iii** Click on the Card Specifics tab and then on the Performance tab. Go to step 2.
- **b** To assign the TCA profile to a port:
  - **i** Expand Network→NE→Shelf→Card→Port on the equipment tree.
  - **ii** Right-click on the port and choose Properties. The Physical Port (Edit) form opens.
  - **iii** Click on the Port Specifics tab and then on the Performance tab. Go to step 2.

2 Choose a profile and click Properties. The TCA Profile Assignment (Edit) form opens.

3 Configure the parameters in the General tab.

4 Select a TCA profile in the Select Profile panel under the General tab.

5 Click Apply to save your changes and close the forms.

Procedure 18-10 To configure thresholds for NE and Card TCA profiles

All NE and Card TCA profiles contain a set of counters and parameters for which threshold values can be configured. The NE TCA profiles are always on the 1830 PSS and cannot be deleted. However, the Card TCA profiles can be deleted.

1 Choose Tools→1830 PSS TCA Profiles from the 5620 SAM main menu. The 1830 PSS TCA Profiles form opens.

Note — See step 4 of Procedure 18-7 to release and distribute a global policy to a specific 1830 PSS. To modify a specific 1830 PSS policy, modify only the local definitions.

2 Choose a profile type from the list and click Properties. Depending on the profile chosen, the NE TCA Profiles (Edit) form or the 1830 PSS Card TCA Profile (Edit) form opens.

3 Click on the TCA Thresholds tab in the NE TCA Profiles (Edit) form or the Card TCA Thresholds tab in the 1830 PSS Card TCA Profile (Edit) form.

4 Choose a TCA variable name and click Properties. The NE or Card TCA Thresholds (Edit) form opens.

5 Configure the Threshold Value parameter and click OK.

Note — By default, profile ID 7 specifies threshold values that can be applied to the 15-minute interval, and profile ID 8 contains threshold values that can be applied to the 24-hour interval in case of a NE TCA profile.

6 Click Apply to save your changes and close the forms.

Procedure 18-11 To configure an OCS TCA profile

1 Choose Tools→1830 PSS TCA Profiles from the 5620 SAM main menu. The 1830 PSS TCA Profiles form opens.

2 Click Create and choose OCS TCA Profile. The OCS NE TCA Profiles, Global Policy (Create) form opens.

3 Configure the required parameters in the General tab.

4 Click Apply to save your changes.

5 Click Switch Mode. The Release - TCA Profile form opens.

6 Choose the devices from the Available Objects list and click on the right-arrow button. The selected devices move to the Selected Objects list.

7 Click Distribute and close the form after the policy is distributed successfully.

8 Click on the Local Definitions tab in the OCS NE TCA Profiles, Global Policy (Edit) form to view the devices to which the policy is distributed.

9 Close the form.

Procedure 18-12 To assign an OCS TCA profile

By default, all objects that support an OCS TCA profile are assigned the default OCS TCA profile. However, you can perform this procedure to assign a different OCS TCA profile to supporting objects.

1 Perform one of the following on the equipment tree:

a Assign an OCS TCA profile to a port with an STM rate.

i Expand Network→NE→Shelf→Card→Port on the navigation tree.

ii Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

iii Click on the Port Specifics tab.

iv Go to step 2.

b Assign an OCS TCA profile to an ODUPTF facility object.

i Expand Network→NE→Shelf→Card→Port on the navigation tree.

ii Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

iii Click on the ODUPTF tab.

iv Go to step 2.

c Assign an OCS TCA profile to an ODUk object.

i Expand Network→NE→Shelf→Card→Port→ODUk on the navigation tree.

ii Right-click on the ODUk object and choose Properties. The ODU Path Termination (Edit) form opens.

iii Go to step 2.

d Assign an OCS TCA profile to an OTUk object.

i Expand Network→NE→Shelf→Card→Port→OTUk on the navigation tree.

ii Right-click on the OTUk object and choose Properties. The OTUk (Edit) form opens.

iii Go to step 2.

e Assign an OCS TCA profile to an OTUODUk object.

i Expand Network→NE→Shelf→Card→Port→OTUk→OTUODUk on the navigation tree.

ii Right-click on the OTUODUk object and choose Properties. The ODU NIM (Edit) form opens.

iii Go to step 2.

2 Click Select beside the TCA Profile parameter. The Select TCA Profile form opens with a list of OCS TCA profiles.

3 Choose a profile from the list and click OK. The Select TCA Profile form closes.

4 Click OK. The properties form closes.

Procedure 18-13 To configure thresholds for an OCS TCA profile

1 Choose Tools→1830 PSS TCA Profiles from the 5620 SAM main menu. The 1830 PSS TCA Profiles form opens.

2 Choose OCS NE TCA Profiles (NE Threshold Crossing Alerts) from the object drop-down menu. A list of OCS TCA profiles appears.

3 Choose a profile for which the threshold needs to be modified and click Properties. The OCS NE TCA Profiles (Edit) form opens.

4 Click on the TCA Thresholds tab. A list of parameters for which the thresholds are monitored appears.

5 Choose the required monitored parameter type and click Properties. The OCS NE TCA Thresholds, Global Policy (Edit) form opens.

6 Configure the Threshold Value parameter.

7 Click OK. The OCS NE TCA Thresholds, Global Policy (Edit) form closes and the OCS NE TCA Profiles (Edit) form reappears with the modified value in the Threshold Value field.

8 Click OK. A dialog box appears.

9 Click Yes. The OCS NE TCA Profiles (Edit) form closes and the 1830 PSS TCA Profiles form reappears.

10 Close the 1830 PSS TCA Profiles form.

18.9 Managing performance monitoring

You can configure PM and view PM data.

Configuring PM

The prerequisites to configure PM are:

- Determine the interfaces and cards that you must configure to collect PM data.
- Configure the profiles to specify the threshold levels at which log events are generated for the PM groups to be monitored on the NE.
- Configure each of the interfaces and cards on the NE for which you must collect PM statistics.
- Configure the PM statistics to collect, the interval period over which they are collected, and the profile used for each interval period.

Viewing PM data

PM data is recorded in logs or bins. Logs record all of the TCAs that occur on the NE. The bins store data collected for a specific card or interface over a specific interval. A raw bin for each PM group collects data until the data is cleared.

Note — When PM data is not available, PM parameter names are displayed with blank values.

Displaying PM data for an EC card

You can display PM data only for an EC card.

Note — Card-level PM is not supported for other card types.

Procedure 18-14 To enable PM TCA alerts

1 On the navigation tree, expand Network→NE.

2 Right-click on the NE and choose Properties. The Network Element (Edit) form opens.

3 Click on the NE Specifics tab.

4 Perform the following in the Performance Management panel.

i Select the Enable PM TCA Alerts check box in the Performance Management panel to enable the 5620 SAM to generate all TCA alerts.

Note — If the check box is disabled, the 5620 SAM does not generate the TCA alerts.

ii Select the default PM policy in the File based PM Policy panel to enable collection of scheduled statistics.

5 Save your changes and close the form.

Procedure 18-15 To clear PM counters of a TCA profile bin associated with a port or SAP on L2 card

Ensure that the port or SAP, where the PM counters needs to be cleared, have a TCA profile assigned to it. See Procedure 18-9 to assign a TCA profile to a card or SAP.

1 Perform one of the following:

a To clear PM counters from port properties of L2 card:

i On the navigation tree, expand Network→NE→Shelf→Card→ Port.

ii Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

iii Click on the Port Specifics tab, then on the Performance tab.

iv Go to step 2.

b To clear PM counters from 5620 SAM main menu:

i Choose Tools→1830 PSS TCA Profiles from the 5620 SAM main menu. The 1830 PSS TCA Profiles form opens.

ii Choose Card TCA Profiles (NE Threshold Crossing Alerts) from the object drop-down box and click Search.

iii Choose the required TCA Profile from the list and click Properties. The 1830 PSS Card TCA Profile (Edit) form opens.

iv Click on the Associations tab, then click Search.

Note — By default,

- for SAP TCA profile type, L2 Access Interfaces tab opens under the Associations tab.
- for Port TCA profile type, Ports tab opens under the Associations tab.

v Choose the required ports as SAPs. Go to step 2.

2 Click Clear PM Counters.

3 Close the forms.

18.10 Cards and ports that support PM data

Table 18-1 lists cards and ports that support PM data.

Note — The 11STMM10 hardware does not support GBE PM statistics in the egress direction. The transmit side of the PM data is not displayed for the 4DPA2 client or line ports.

Table 18-1 Cards and ports supporting PM data

Cards	Ports
Card Type - Amplifier and associated cards	
A2325A AHPHG AHPLG ALPHG AM2017B AM2325B	LINE, LINE- (9170~9605), OSC
A2P2125 A4PSWG AM2032A AM2125A AM2125B AM2318A AM2625A ASWG	LINEIN, LINEIN- (9170~9605), LINEOUT, LINEOUT- (9170~9605), OSCSFP
AA2DONW	LINE, OSCSFP, SIG
ALPFGT	LINE, OSC, OSCSFP
OSCT	LINE, LINE- (9170~9605), OSCSFP

(1 of 4)

Cards	Ports
RA2P	LINEIN
WTOCM WTOCMA	IN (1 to 4)-(9170~9605)
Dedicated card	
EC	No port, PM data collected on the EC card and not on the port level
Optical Client/Line Cards	
1AN100G	H1
2AN40G	H (1,2)
24ANM 24ANMB 24ET1G 24ET1GB	C (1 to 24)
4AN10G	H (1 to 4)
8ET1GB	C (1 to 8)
10AN10G 10AN10GC 10OTH10G	H (1 to 10)
10ET10G 10ET10GC	C (1 to 10)
11QCUP 11QCUPC	L (1 to 4)
43SCUP 130SCUP 130SCUPB 130SCUPC	L1
Optical Transponder Cards	
1DPP24M Master PSS1P21	C (1 to 21), L1
1DPP24M Slave	C (1 to 21)
4DPA2	C (1, 2), L (1, 2)
4DPA4 DualTran	C (1, 3), L (1, 2), VA (1, 2)
4DPA4 FlexMux	C (1 to 4), L (1, 2), VA (1, 2)
4QPA8 11QPA4 11QPEN4	C (1 to 4), L (1 to 4), VA (1 to 4)
11DPE12 11DPE12A 11DPE12E 11DPM12	C (1 to 12), L (1, 2), VA (1, 2)

(2 of 4)

Cards	Ports
11DPM4M	C (1 to 4) and L (1, 2) without adjacent 11DPM4E card C (1 to 8) and L (1, 2) with adjacent 11DPM4E card
11DPM8	C (1 to 8), L (1, 2), VA (1, 2)
11OPE8	C (1,2), M (1 to 4), VA (1 to 4), X (1 to 6)
11QCE12X	C (1 to 22), M (1 to 4), VA (1,2), X (1 to 4)
11QPE24	C (1 to 11, 24), VA (1 to 4), X (1 to 4)
11STAR1 11STAR1A 112SA1L 112SCA1 112SNA1 130SCA1 43SCA1 43SCGE1 43STA1P SVAC	C1, L1
11STGE12 11STMM10 112SCX10 112SNX10 112SX10L 130SCX10 130SNQ10 130SNX10	C (1 to 10), L1
43SCX4 43SCX4E 43SCX4L 43STX4 43STX4P	C (1 to 4), L1
112SDX11	C (1 to 14), L (1 to 4)
260SCX2	C (1,2), L1
MVAC	G (1 to 8)
MVAC8B	C (1 to 8), L (1 to 8)
PSS1GBE	C (1 to 12), L (1, 2)
PSS1MD4 (Card Mode = DualTran)	C (1, 3), L (1, 2)
PSS1MD4 (Card Mode = FlexMux)	C (1 to 4), L (1, 2)
PTP cards	
PTPCTL	P (1 to 6)
PTPIO	TP (1,2), ITP (1,2)

(3 of 4)

Cards	Ports
TDM Cards	
10SD10G	H (1 to 10)
24SDM	H (1 to 24)

(4 of 4)

Table 18-2 lists the dedicated cards that are required to boot the 1830 PSS.

Table 18-2 Dedicated cards and ports

Cards	Ports
FAN	—
USRPNL	OAMP, VOIP, E1, E2
EC	CIT (Local Ethernet Port), AUX, ES1, ES2
PFDC50 50A	No ports
PFDC60 60A	No ports

1830 PSS power management

19 — 1830 PSS power management

19.1 Power management overview

Power management is configured using the 5620 SAM to improve transmission performance. The 1830 PSS supports automatic and manual power management of the technology types. Auto-power managed networks have restricted topologies, but can be commissioned and the NE automatically adjusts power levels. Manual-power managed networks support more flexible topologies, but the power levels and commissioning can be configured. For protection configurations, the working and protection lines can be auto-power managed, or manual-power managed, or one can be auto-power managed and the other can be manual-power managed. See Procedure 19-1 for more information about display of optical power levels.

The TOADM and ROADM configurations support auto-power management. The FOADM configurations support manual-power management. There are FOADM configurations that support auto-power management. See Procedure 19-4 for information about configuring auto-power adjustment using the 5620 SAM.

Power adjustments are supported for the following configurations:

- SR–PSS services (also supports SR DWDM tunable OTs)
- PSS–PSS services when there is a drop shelf OT at the endpoints of the service
- PSS–PSS services when there is an internal PSS OT that has a manual power adjustment

19.2 Power management settings

The 5620 SAM supports configuring the power management parameters.

LD port settings

The 5620 SAM supports viewing and modifying the power management parameters for the following LD ports:

- A2325A, AA2DONW, AHPHG, AHPLG, ALPHG, AM2318A, and OSCT LINE ports
- AM2032A, A4PSWG, A2P2125, AM2125A, AM2125B, AM2318A, ASWG, and AM2625A LINEOUT ports

Table 19-1 lists the configurable power management parameters for LD ports. The parameters are configured on the Port Specifics→General tab on the Network→1830 PSS→Shelf→Card→Port→Physical Port form.

Table 19-1 Power management parameters for LD ports

Parameter	Card restrictions
Power Management	
Power Management Type	Read-only for AA2DONW and OSCT
Service Launch Attenuation Offset (dB)	Not applicable for AA2DONW and OSCT

(1 of 2)

Parameter	Card restrictions
Span Loss Tilt (dB)	Not applicable for AA2DONW and OSCT
Auto Gain Adjustment Enabled	Read-only for OSCT and not applicable for AA2DONW
Auto Tilt Adjustment Enabled	Read-only for OSCT and not applicable for AA2DONW
Auto Tilt Maintenance Mode Enabled	Read-only for OSCT and not applicable for AA2DONW
Commissioning Completed	Not applicable for AA2DONW
Gain Adjustment settings	
Time Offset Past Hour (HH:MM:SS)	Not applicable for AA2DONW and OSCT
Time Period Between Adjustments (HH:MM:SS)	Not applicable for AA2DONW and OSCT
Allocated Adjustment Time (HH:MM:SS)	Not applicable for AA2DONW and OSCT
Wavelength Tracker Settings	
Wavelength Tracker Decoder Usage	Not applicable for AA2DONW and OSCT

(2 of 2)

The power management parameters are configurable under the following conditions:

- You can configure the power management parameters only if the Ap Opp Direction Port Addr parameter on the Port Specifics→General tab of the Network→1830 PSS→Shelf→Card→Port→Physical Port (Edit) form is configured.
- The Power Management Type parameter cannot be set to auto if the shelf where the card is provisioned has the Wavelength Tracker Enabled parameter deselected for 1830 PSS-32 devices.
- If you configure the Power Management Type parameter as auto, the Service Launch Attenuation Offset (dB) parameter is available for configuration.

WR port settings

The 5620 SAM supports viewing and modifying the power settings for the following WR ports:

- WR8-88A SIG port
- WR8-88AF SIG port

Table 19-2 lists the configurable power management parameters for WR ports. The parameters are configured on the Port Specifics→General tab on the Network→1830 PSS→Shelf→Card→Port→Physical Port form.

Table 19-2 Power management parameters for WR ports

Parameter	Values
Power Management Type	Auto Manual

(1 of 2)

Parameter	Values
Commissioning Completed	—

(2 of 2)

The power management parameters are configurable under the following conditions:

- You can configure the power management parameters only if the Level in Optical Node parameter of the WR8-88A and WR8-88AF Card Specifics tab on the Network→1830 PSS→Shelf→Card→Card Slot form is set to 1.
- The Power Management Type parameter cannot be configured as Auto if the shelf where the card is provisioned has Wavelength Tracker Enabled parameter deselected for 1830 PSS-32 devices.
- If you configure the Power Management Type parameter as Auto, the Service Launch Attenuation Offset (dB) parameter is available for configuration.

WR20-TFM DGE configuration

The DGE configuration equalizes the power gain on LDs using variable attenuators on a WR20-TFM card. The DGE configuration consists of two WR20TFM cards. The DROPOUT port of the first WR20TFM card is connected to the ADDIN port of the second WR20TFM card in one direction, and the reverse, in the other direction. The following cards can be used in a DGE configuration:

- WR20TFM
- ASWG
- A4PSWG
- OTDR
- WTOCM
- WTOCM-F

See *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide* for more information about DGE configuration.

Note — The DROP2OUT port of the first WR20TFM card must not be connected to ADD2IN port of the second WR20TFM card for a DGE configuration, as it creates fiber loops.

WTOCM, WTOCMA, and WTOCM-F port settings

The 5620 SAM supports configuring the following parameters for the WTOCM, WTOCMA and WTOCM-F IN ports:

- Ap Wtocm Conn Address
- Monitored Port Connection Loss (dB)
- OSNR Measurement Enabled
  (only for WTOCMA)

The IN ports are automatically configured and deleted with the card. The 5620 SAM allows the user to select the monitored port. The supported port types are the LINE and SIG ports for the following LD card types:

- A2325A
- AHPHG

- ALPHG
- LINEOUT

LINEOUT ports for the following LD card types:

- A2P2125
- A4PSWG
- AM2032A
- AM2125A
- AM2318A
- AM2625A
- ASWG
- AM2125B

19.3 Power chart

The 5620 SAM displays the optical power levels on the:

- ports
- OTU and OCH trails
- optical transport services

Port power chart

The port power chart displays the following power values for each wavelength (direction (IN or OUT) and a port):

- measured power—a measurement that provides the current power level
- expected power—a provisioned value that indicates to the 1830 PSS device the power level that must be achieved
- expected power deviation—a provisioned value that represents the deviation from the expected power level that is considered healthy

In automatically powered equipment, the expected power and deviation values are determined by SCOT. In manually powered equipment, the user can change the values. See Procedure 19-5 to manage the expected power levels and deviation at a wavelength tracker detection point.

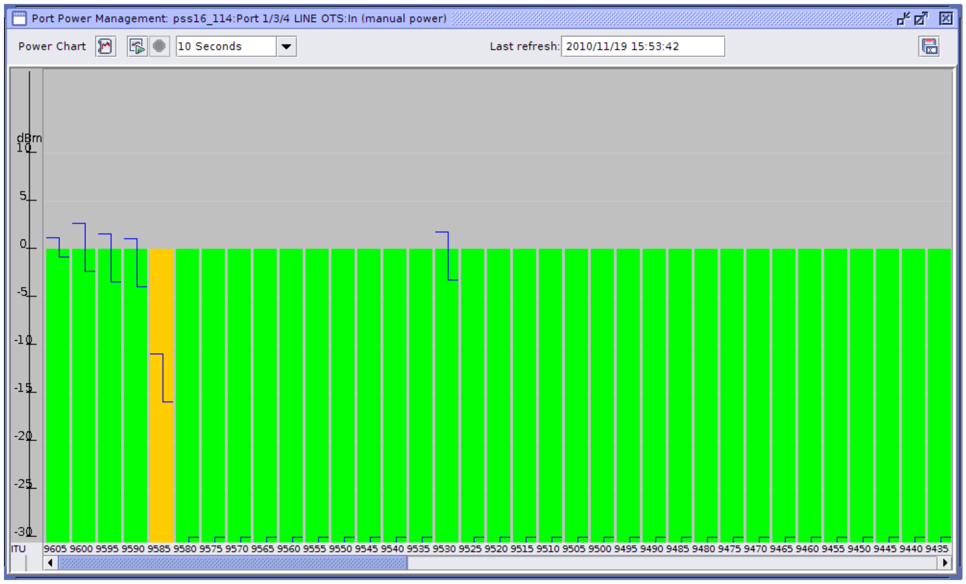
You can navigate to the optical transport services configured for a specific channel by choosing Show service on the power chart. The Optical Transport Service edit form opens, if the channel has only one service configured. The Select Transport Service form opens with a list of services, if the channel has multiple services configured.

Optical power levels are represented by bars, and the high and low watermarks are represented by a Z bar. Figure 19-1 shows a port optical power chart.

The color legends used on the port power chart are as follows:

- Green—within range
- Orange—out of range (OoR, but within the chart interval which ranges from –30 to +10)

Figure 19-1 Port power chart



OTU and OCH trails power chart

The power chart can also be displayed from the optical trail. The power chart generated from the OCH Trail (Edit) form (Manage→OTN→OTN Trails→OTU or OCH Trail (Edit) form→OTU, or OCH Trail Path→Power A to Z or Power Z to A.

The OCH trail power chart displays:

- received power on all the points along the OCH trail of a keyed service, on a single channel for the A to Z direction and Z to A direction, except the client ports
- power loss on each power monitored ports calculated as the difference of the expected power with the actual power value

The color legend for the service power chart (as shown in 19-2) is as follows:

- Green—within range
- Orange—out of range (OoR but within the interval which ranges from -30 to +10
- White—the power levels are -99 and less than -30
- Black—the power levels are -99

Service power chart

The service power chart displays:

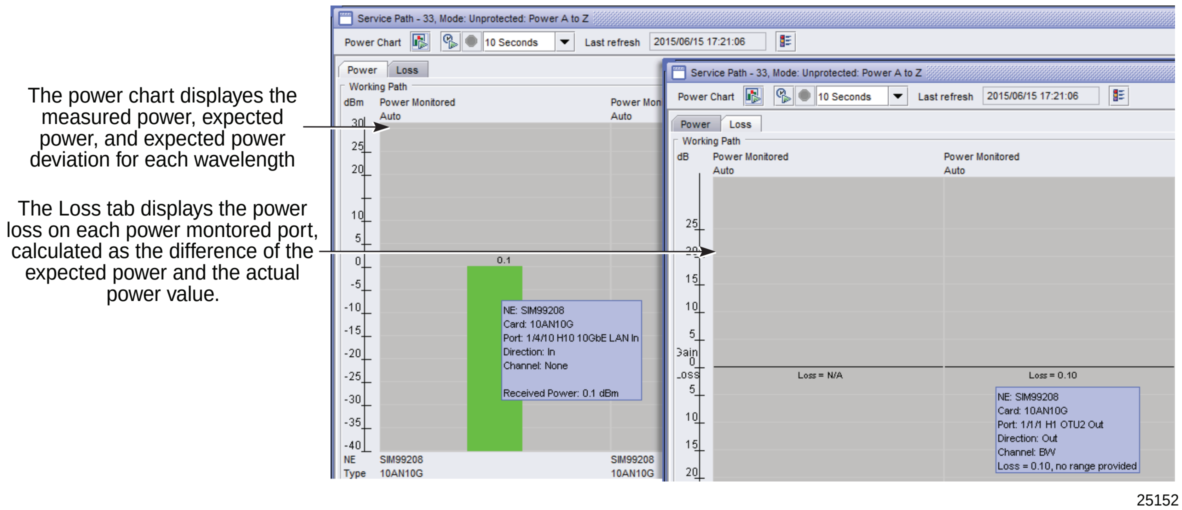
- received power on all of the points along the service path on a single channel for the A to Z direction and Z to A direction
- power loss on each power monitored ports calculated as the difference of the expected power with the actual power value

See Procedure 19-1 for more information about displaying optical power levels along a service path.

The color legend for the service power chart (as shown in 19-2) is as follows:

- Green—within range
- Orange—out of range (OoR but within the interval which ranges from -30 to +10
- White—the power levels are -99 and less than -30
- Black—the power levels are -99

Figure 19-2 Service power chart



19.4 Wavelength tracker and wave key

The Wavelength Tracker allows the 1830 PSS device to manage wavelengths at different stages of an optical path. Each wavelength can be traced as it passes through the network, which allows you to ensure that the network connections are correct. A unique identifier, known as a wave key pair, is encoded on each wavelength that enters the network through an 1830 PSS device. By detecting and identifying the encoded wave keys, the wavelength can be traced through the network. Tables 19-3, 19-4, and 19-5 list the ITU channel numbers and corresponding ALU wave keys for the L-band, C-band, and S-band channels. See Procedure 19-10 for more information about managing wave keys using the 5620 SAM GUI.

The 5620 SAM assigns the wave keys on the SR DWDM ports and on the PSS cross-connects to ensure that the encoded wave keys on the SR DWDM ports are the same as on the 1830 PSS. If the user changes the wave keys using the WebUI or CLI, the user needs to ensure that the same wave keys are assigned to respective SR source ports in order to view accurate power levels on the 1830 PSS encoder and decoder points. AutoKeying (NMS) is the only wave key assign mode supported for services originating on the SR and traversing through a network of 1830 PSS.

Note — The 5620 SAM does not support manual modification of wave keys. You can use the WebUI or CLI for modifications.

Table 19-3 L-band channel wave keys

ITU channel number (THz)	nm	ALU channel number	ITU channel number (THz)	nm	ALU channel number
100 GHz grid			**50 GHz offset**		
186.00	1611.79	8600	186.05	1611.35	8605
186.10	1610.92	8610	186.15	1610.49	8615
186.20	1610.06	8620	186.25	1609.62	8625
186.30	1609.19	8630	186.35	1608.76	8635
186.40	1608.33	8640	186.45	1607.90	8645
186.50	1607.47	8650	186.55	1607.04	8655
186.60	1606.60	8660	186.65	1606.17	8665
186.70	1605.74	8670	186.75	1605.31	8675
186.80	1604.88	8680	186.85	1604.46	8685
186.90	1604.03	8690	186.95	1603.60	8695
187.00	1603.17	8700	187.05	1602.74	8705
187.10	1602.31	8710	187.15	1601.88	8715
187.20	1601.46	8720	187.25	1601.03	8725
187.30	1600.60	8730	187.35	1600.17	8735
187.40	1599.75	8740	187.45	1599.32	8745
187.50	1598.89	8750	187.55	1598.47	8755
187.60	1598.04	8760	187.65	1597.62	8765
187.70	1597.19	8770	187.75	1596.76	8775
187.80	1596.34	8780	187.85	1595.91	8785
187.90	1595.49	8790	187.95	1595.06	8795
188.00	1594.64	8800	188.05	1594.22	8805
188.10	1593.79	8810	188.15	1593.37	8815
188.20	1592.95	8820	188.25	1592.52	8825
188.30	1592.10	8830	188.35	1591.68	8835
188.40	1591.26	8840	188.45	1590.83	8845
188.50	1590.41	8850	188.55	1589.99	8855
188.60	1589.57	8860	188.65	1589.15	8865
188.70	1588.73	8870	188.75	1588.30	8875
188.80	1587.88	8880	188.85	1587.46	8885
188.90	1587.04	8890	188.95	1586.62	8895
189.00	1586.20	8900	189.05	1585.78	8905
189.10	1585.36	8910	189.15	1584.95	8915
189.20	1584.53	8920	189.25	1584.11	8925
189.30	1583.69	8930	189.35	1583.27	8935

(1 of 2)

ITU channel number (THz)	nm	ALU channel number	ITU channel number (THz)	nm	ALU channel number
100 GHz grid			**50 GHz offset**		
189.40	1582.85	8940	189.45	1582.44	8945
189.50	1582.02	8950	189.55	1581.60	8955
189.60	1581.18	8960	189.65	1580.77	8965
189.70	1580.35	8970	189.75	1579.93	8975
189.80	1579.52	8980	189.85	1579.10	8985
189.90	1578.69	8990	189.95	1578.27	8995
190.00	1577.86	9000	190.05	1577.44	9005
190.10	1577.03	9010	190.15	1576.61	9015
190.20	1576.20	9020	190.25	1575.78	9025
190.30	1575.37	9030	190.35	1574.95	9035
190.40	1574.54	9040	190.45	1574.13	9045
190.50	1573.71	9050	190.55	1573.30	9055
190.60	1572.89	9060	190.65	1572.48	9065
190.70	1572.06	9070	190.75	1571.65	9075
190.80	1571.24	9080	190.85	1570.83	9085
190.90	1570.42	9090	190.95	1570.01	9095

(2 of 2)

Table 19-4 C-band channel wave keys

ITU channel number (THz)	nm	ALU channel number	ITU channel number (THz)	nm	ALU channel number
100 GHz grid			**50 GHz offset**		
191.00	1569.59	9100	191.05	1569.18	9105
191.10	1568.77	9110	191.15	1568.36	9115
191.20	1567.95	9120	191.25	1567.54	9125
191.30	1567.13	9130	191.35	1566.72	9135
191.40	1566.31	9140	191.45	1565.90	9145
191.50	1565.50	9150	191.55	1565.09	9155
191.60	1564.68	9160	191.65	1564.27	9165
191.70	1563.86	9170	191.75	1563.45	9175
191.80	1563.05	9180	191.85	1562.64	9185
191.90	1562.23	9190	191.95	1561.83	9195
192.00	1561.42	9200	192.05	1561.01	9205
192.10	1560.61	9210	192.15	1560.20	9215
192.20	1559.79	9220	192.25	1559.39	9225

(1 of 3)

ITU channel number (THz)	nm	ALU channel number	ITU channel number (THz)	nm	ALU channel number
100 GHz grid			**50 GHz offset**		
192.30	1558.98	9230	192.35	1558.58	9235
192.40	1558.17	9240	192.45	1557.77	9245
192.50	1557.36	9250	192.55	1556.96	9255
192.60	1556.55	9260	192.65	1556.15	9265
192.70	1555.75	9270	192.75	1555.34	9275
192.80	1554.94	9280	192.85	1554.54	9285
192.90	1554.13	9290	192.95	1553.73	9295
193.00	1553.33	9300	193.05	1552.93	9305
193.10	1552.52	9310	193.15	1552.12	9315
193.20	1551.72	9320	193.25	1551.32	9325
193.30	1550.92	9330	193.35	1550.52	9335
193.40	1550.12	9340	193.45	1549.72	9345
193.50	1549.32	9350	193.55	1548.91	9355
193.60	1548.51	9360	193.65	1548.11	9365
193.70	1547.72	9370	193.75	1547.32	9375
193.80	1546.92	9380	193.85	1546.52	9385
193.90	1546.12	9390	193.95	1545.72	9395
194.00	1545.32	9400	194.05	1544.92	9405
194.10	1544.53	9410	194.15	1544.13	9415
194.20	1543.73	9420	194.25	1543.33	9425
194.30	1542.94	9430	194.35	1542.54	9435
194.40	1542.14	9440	194.45	1541.75	9445
194.50	1541.35	9450	194.55	1540.95	9455
194.60	1540.56	9460	194.65	1540.16	9465
194.70	1539.77	9470	194.75	1539.37	9475
194.80	1538.98	9480	194.85	1538.58	9485
194.90	1538.19	9490	194.95	1537.79	9495
195.00	1537.40	9500	195.05	1537.00	9505
195.10	1536.61	9510	195.15	1536.22	9515
195.20	1535.82	9520	195.25	1535.43	9525
195.30	1535.04	9530	195.35	1534.64	9535
195.40	1534.25	9540	195.45	1533.86	9545
195.50	1533.47	9550	195.55	1533.07	9555
195.60	1532.68	9560	195.65	1532.29	9565
195.70	1531.90	9570	195.75	1531.51	9575

(2 of 3)

ITU channel number (THz)	nm	ALU channel number	ITU channel number (THz)	nm	ALU channel number
100 GHz grid			**50 GHz offset**		
195.80	1531.12	9580	195.85	1530.72	9585
195.90	1530.33	9590	195.95	1529.94	9595

(3 of 3)

Table 19-5 S-band channel wave keys

ITU channel number (THz)	nm	ALU channel number	ITU channel number (THz)	nm	ALU channel number
100 GHz grid			**50 GHz offset**		
196.00	1529.55	9600	196.05	1529.16	9605
196.10	1528.77	9610	196.15	1528.38	9615
196.20	1527.99	9620	196.25	1527.60	9625
196.30	1527.22	9630	196.35	1526.83	9635
196.40	1526.44	9640	196.45	1526.05	9645
196.50	1525.66	9650	196.55	1525.27	9655
196.60	1524.89	9660	196.65	1524.50	9665
196.70	1524.11	9670	196.75	1523.72	9675
196.80	1523.34	9680	196.85	1522.95	9685
196.90	1522.56	9690	196.95	1522.18	9695
197.00	1521.79	9700	197.05	1521.40	9705
197.10	1521.02	9710	197.15	1520.63	9715
197.20	1520.25	9720	197.25	1519.86	9725
197.30	1519.48	9730	197.35	1519.09	9735
197.40	1518.71	9740	197.45	1518.32	9745
197.50	1517.94	9750	197.55	1517.55	9755
197.60	1517.17	9760	197.65	1516.78	9765
197.70	1516.40	9770	197.75	1516.02	9775
197.80	1515.63	9780	197.85	1515.25	9785
197.90	1514.87	9790	197.95	1514.49	9795
198.00	1514.10	9800	198.05	1513.72	9805
198.10	1513.34	9810	198.15	1512.96	9815
198.20	1512.58	9820	198.25	1512.19	9825
198.30	1511.81	9830	198.35	1511.43	9835
198.40	1511.05	9840	198.45	1510.67	9845
198.50	1510.29	9850	198.55	1509.91	9855
198.60	1509.53	9860	198.65	1509.15	9865

(1 of 2)

ITU channel number (THz)	nm	ALU channel number	ITU channel number (THz)	nm	ALU channel number
100 GHz grid			**50 GHz offset**		
198.70	1508.77	9870	198.75	1508.39	9875
198.80	1508.01	9880	198.85	1507.63	9885
198.90	1507.25	9890	198.95	1506.87	9895
199.00	1506.49	9900	199.05	1506.12	9905
199.10	1505.74	9910	199.15	1505.36	9915
199.20	1504.98	9920	199.25	1504.60	9925
199.30	1504.23	9930	199.35	1503.85	9935
199.40	1503.47	9940	199.45	1503.10	9945
199.50	1502.72	9950	199.55	1502.34	9955
199.60	1501.97	9960	199.65	1501.59	9965
199.70	1501.21	9970	199.75	1500.84	9975
199.80	1500.46	9980	199.85	1500.09	9985
199.90	1499.71	9990	199.95	1499.34	9995
200.00	1498.96	2000	200.05	1498.59	2000
200.10	1498.21	2001	200.15	1497.84	2001
200.20	1497.46	2002	200.25	1497.09	2002
200.30	1496.72	2003	200.35	1496.34	2003
200.40	1495.97	2004	200.45	1495.60	2004
200.50	1495.22	2005	200.55	1494.85	2005
200.60	1494.48	2006	200.65	1494.11	2006
200.70	1493.73	2007	200.75	1493.36	2007
200.80	1492.99	2008	200.85	1492.62	2008
200.90	1492.25	2009	200.95	1491.88	2009

(2 of 2)

In addition, the Wavelength Tracker can measure the optical power level at each detection point for each encoded channel that passes through a port on an 1830 PSS device. The 5620 SAM power management function uses the Wavelength Tracker feature and other equipment readings to provide a graphical representation of power levels and a mechanism to track changes in the network.

For more information about the Wavelength Tracker tool, see the Alcatel-Lucent *1830 Photonic Service Switch User Provisioning Guide* and the Alcatel-Lucent *1830 Photonic Service Switch Product Information and Planning Guide.*

Rekeying service

The 5620 SAM allows you to rekey wave keys that are associated with an optical transport service. You can rekey a wave key to resolve duplicate wave key values that are assigned to a service. See Procedure 19-10 for more information about rekeying wave key values of a service.

19.5 OSNR measurement

The 5620 SAM supports Optical Signal to Noise Ratio (OSNR) measurement for supported channels or a specific channel upon activation. The OSNR monitors system aging using the WTOCMA card. The WTOCMA can monitor up to four optical lines.

The OSNR measurement time for one channel is 30 s. The first scan is performed with the filter set at the center of the target channel and the second scan is performed with the filter set slightly de-tuned from center. By comparing the two sets of measurements, an in-band OSNR measurement is obtained. The OSNR measurement of 40 Gb/s and 100 Gb/s signals requires an inter-leaver for transmission.

The 5620 SAM supports OSNR measurement upon selecting the Port Specifics→On Demand OSNR→General tab of the WTOCMA Physical Port (Edit) form. The on-demand OSNR scan can be performed on a specific channel or channels. See Procedure 19-13 for more information about configuring an on-demand OSNR scan.

19.6 OTDR scan

An OTDR scan is used to characterize a fiber span before configuring a service, determine the location of a fiber cut, and monitor the fiber while in-service. The LD cards that support OTDR scan include A4PSWG and ASWG cards.

External topological links must exist between the ports of the OTDR card and the OTDRRX or OTDRTX ports of the LD to allow OTDR scans through LINEIN or LINEOUT ports. Consider the following while configuring the external topological links to enable OTDR scans:

- In an ILA, the OTDR scan can be performed through the LINEIN port of the OTDR card, by connecting the LINEIN port to the OTDRRX port of the amplifier. Similarly, the OTDR scan can be launched from the LINEOUT port of the OTDR card, by connecting the LINEOUT port to the OTDRTX port of the amplifier.
- In a ROADM configuration with an ingress LD, the OTDR scan can be performed through the LINEIN port of the OTDR card by connecting the LINEIN port to the OTDRRX port of the ingress LD.
- In a ROADM configuration with an egress LD, the OTDR scan can be performed through the LINEOUT port of the OTDR card by connecting the LINEOUT port to the OTDRTX port of the egress LD.

See Procedure 19-14 for more information about configuring an OTDR scan.

19.7 Technology types

The technology types are:

- reserved types that are discovered on the node
- unreserved types that are discovered on the 5620 SAM

The 5620 SAM allows you to view the reserved technology types. You can create, view, and modify the unreserved technology types. See Procedure 19-11 for more information about configuring unreserved technology type.

Note 1 — You cannot create a technology type on the 5620 SAM if a specific Bit Rate Key and the Encoding Key parameter value is already present.

Note 2 — You cannot modify the Bit Rate Description and the Encoding Description parameters for the unreserved technology types with Bit Rate Key and Encoding Key parameter values that are for the reserved technology types. The values range from 1 to 1000 and 9001 to 10000.

Note 3 — You cannot modify the WTOCM/WTOCMA Calibration and the OSNR Calibration parameters for the unreserved technology types with Bit Rate Key and Encoding Key parameter values that are for the reserved technology types. The values range from 9001 to 10 000.

You can delete a technology type under the following conditions:

- technology type is not a reserved
- technology type is not associated with a cross-connect. The AZ and ZA configured and received Bit Rate Key and Encoding Key parameter values do not match on a cross-connect.

You can set the technology type on OCH cross-connects on the 1830 PSS. See Procedure 19-12 for more information about setting the technology type.

19.8 Power management procedures

The following procedures describe how to manage optical power levels using the 5620 SAM.

Procedure 19-1 To display optical power levels along a service path

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Choose Optical Transport Service from the object type drop-down menu and click Search. A list of managed optical transport services appears.
3. Choose a service and click Properties. The Optical Transport Service (Edit) form opens.
4. Choose Service Paths→Service Path on the navigation tree. The Service Path properties form opens.
5. Click on one of the following:
    - Power A to Z
    - Power Z to A

If the buttons are not visible, click More Actions and choose the corresponding option from the drop-down menu.

The optical power level graph opens, displaying all of the points along the service path for the selected direction.

Note — The power levels that are displayed have the following characteristics:

- When the SR DWDM card has the Port Type parameter set to Fixed on the Wavelength Tracker tab under the Optical tab of the Physical Port (Edit) form, the transmitted power from the wavelength tracker is displayed.
- When the SR DWDM card has the SFP VOA Present parameter selected on the Wavelength Tracker tab under the Optical tab of the Physical Port (Edit) form, the transmitted power from the wavelength tracker is displayed.
- When the SR DWDM card has the SFP VOA Present parameter deselected on the Wavelength Tracker tab under the Optical tab of the Physical Port (Edit) form, the coherent transmitted and received power are displayed for the coherent cards.
- When the SR DWDM card has the SFP VOA Present parameter deselected on the Wavelength Tracker tab under the Optical tab of the Physical Port (Edit) form and the Rx Amplifier parameter is set to True on the Optical Amplifier tab under the Optical tab of the Physical Port (Edit) form, the received power is displayed from the amplifier.
- For all other configurations of the SR DWDM card, the power from the Lane DDM or DDM is displayed, depending on the card type.
- The received power of the SR non-DWDM ports in the power graph is from the Lane DDM or DDM, depending on the card type.

6 Click on the Loss tab. The power chart displays a bar graph representing the power loss and gain for the power monitored ports along the service path in the specified direction. The 5620 SAM calculates the power loss or gain of a power monitored port from the difference in its measured power value and the measured power value of the previous power monitored port.

The Loss tab also displays a Z bar that indicates the minimum and maximum power loss or gain values for the following ports:

- Bidirectional Amplifier SIG OUT
- Unidirectional Amplifier LINEOUT
- CWR THRU OUT
- WR SIG OUT

Procedure 19-2 To refresh the optical power chart display

1. Open an optical power chart. See Procedure 19-1 for more information.
2. Choose the number of seconds between refreshes from the Power Chart drop-down menu.
3. Perform one of the following:
   a. To configure an automatic refresh, choose the number of seconds between refreshes from the Power Chart drop-down menu and click on the Auto-refresh power chart icon. The optical power chart updates at the configured time interval.
   b. To manually refresh the optical power chart, click Refresh power chart. The latest power readings for all of the points are displayed. The optical power chart is refreshed and the last refresh time is displayed.

Procedure 19-3 To configure automatic power adjustment rules on a 5620 SAM optical transport service

The automatic power adjustment rules allow users to configure parameters to adjust power levels for optical transport services between the source port and the target port. The power converge parameters for source and destination ports can be configured using the automatic power adjustment rules. The automatic power adjustment rules can be applied to, for example, the 7750 SR source port, which is the SR DWDM tunable power control enabled transponder port that can encode wave keys, and the 1830 PSS target port, which is the cross-connected egress amplifier port that can decode wave keys for a channel in A→Z or Z→A directions.

1. Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.
2. Choose Optical Transport Service from the object type drop-down menu and click Search. A list of managed optical transport services is displayed.
3. Choose a service and click Properties. The Optical Transport Service (Edit) form opens.
4. Choose Service Paths→Service Path. The Service Path properties form opens.
5. Click Search in the Auto Power Adjustment Rules panel. A list of rules is displayed.
6. Choose a rule and click Properties. The Power Adjustment Rule (Edit) form opens.
7. Configure the required parameters:
8. Save your changes and close the form.
9. Click Power A to Z or Power Z to A in the Optical Transport Service (Edit) form. The Discovered Service Power A to Z or Z to A form opens.
10. Click Auto Power Adjustment to implement automatic power adjustment. A dialog box appears.

11 Click Yes. The automatic power adjustment process starts and the status changes from Not executed to In Progress.

12 If you need to terminate the automatic power adjustment process:

i Click Auto Power Adjustment. A dialog box appears.

ii Click Yes. The automatic power adjustment process stops. The status changes from In Progress to Aborted.

Procedure 19-4 To perform an automatic power adjustment on an 1830 PSS

The 5620 SAM supports egress and ingress power adjustments for the following cards:

- A2325A
- A2P2125
- A4PSWG
- AHPHG
- AHPLG
- ALPHG
- RA2P
- AM2032A
- AM2125A
- AM2125B
- AM2318A
- AM2625A
- ASWG

The 5620 SAM supports add and drop power adjustments for the following cards:

- WR8-88A
- WR8-88AF

The power adjustment support on a card depends on the current topology. If the Power Management Type parameter of the amplifier card is set to Manual on the Port Specifics→General tab of the Physical Port (Edit) form, the card does not support ingress or egress power adjustment.

The following types of power adjustments are supported on the Card Specifics→Power Adjustment tab of the Card Slot (Edit) form:

- Linear—for linear topologies and requires forced cross-connects
- Ring—for ring topologies and is also called ASE adjustment
- Dynamic Tilt—based on the tilt adjustment parameters on the node

The automatic power adjustment is supported for linear topologies from the power graph.

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose Optical Transport Service from the object type drop-down menu and click Search. A list of managed optical transport services is displayed.

3 Choose a service and click Properties. The Optical Transport Service (Edit) form opens.

4 Choose Service Paths→Service Path. The Service Path properties form opens.

5 Click Power A to Z or Power Z to A. The Service Path Power A to Z or Z to A form opens.

6 Drag the horizontal split bar to view the Power Control form that lists the power adjustment configurations of the termination points for the service.

7 Choose a power adjustment point and click Properties. The Power Adjustment (Edit) form opens.

8 Configure the required parameters in the Power Attributes panel and click OK.

9 Click Start Power Adjust or right-click on the Power Graph and choose Start Power Adjust to start automatic power adjustment in the Service Path Power A to Z or Z to A form.

Note — Click Stop Power Adjust or Abort Power Adjust to stop or abort a power adjustment, respectively.

10 Click Resync on the Power Control form to view the current status and results.

11 Save your changes and close the forms.

Procedure 19-5 To manage the expected power level and deviation at a Wavelength Tracker detection point

1 On the navigation tree, expand Network→NE→Shelf→Card→Port.

2 Right-click on a port and choose Properties. The Physical Port (Edit) form opens. Table 19-6 lists the ports that support the Wavelength Tracker.

Table 19-6 Wavelength Tracker-enabled ports

Card	Port	Direction
Decoder Ports		
A2325A AHPHG AHPLG ALPHG AM2017B AM2325B	LINE	IN, OUT
	SIG	OUT
	DCM	OUT
AM2125A	LINEIN	IN
	LINEOUT	OUT

(1 of 2)

Card	Port	Direction
CWR8 CWR8-88	SIG	IN, OUT
	THRU	OUT
	OMD	IN
	CLS (1 to 8)	IN, OUT
OPSA, Protection Mode = OCHP or OMSP only	SIG	IN
	A	IN
	B	IN
Encoder Ports		
112SCA1	L1	OUT
112SCX10	L1	OUT
11DPE12 11DPE12E	VA (1 to 2)	OUT
11QPA4	VA (1 to 4)	OUT
11STAR1	L1	OUT
11STAR1A	L1	OUT
11STGE12	L1	OUT
11STMM10	L1	OUT
43SCX4 43SCX4E	L1	OUT
43STA1P	L1	OUT
43STX4 43STX4P	L1	OUT
4DPA4	VA (1 to 2)	OUT
MVAC	G (1 to 8)	OUT
SVAC	L1	OUT
Other Ports		
WTOCM	IN (1 to 4)	IN

(2 of 2)

3 Resynchronize all wave keys.

i Click on the Port Specifics tab of the Physical Port (Edit) form, then on the Wave Keys tab.

ii Click Resync All Wave Keys.

4 Perform one of the following:

a Click Power Management In to view the detection point power levels for the inbound optical light path. The Port Power Management power chart for the inbound optical light path opens.

b Click Power Management Out to view the detection point power levels for the outbound optical light path. The Port Power Management power chart for the outbound optical light path opens.

5 To set the expected power level for a channel:

i Right-click on the power chart and choose Properties. A dialog box appears.

ii Click OK. The Wave Keys (Edit) form opens.

iii Configure the required parameters in the General tab.

iv Save your changes and close the form.

6 Right-click on the power chart and choose Set Power Deviation. The Set Power Deviation for channel form opens.

7 Perform one of the following to set the power deviation.

a Enter a deviation value between 0 and 5 and click Apply.

b Drag the slide bar left or right to choose a deviation value and click Apply.

The Set Power Deviation for channel form closes and the size of the Z bar increases or decreases based on the configured deviation value.

8 Close the power chart.

Procedure 19-6 To export optical power chart data to a CSV file

1 On the navigation tree, expand Network→NE→Shelf→Card→Port.

2 Right-click on a port and choose Properties. The Physical Port (Edit) form opens.

3 Perform one of the following:

a Click Power Management In to view the detection point power levels for the inbound optical light path. The Port Power Management power chart for the inbound optical light path opens.

b Click Power Management Out to view the detection point power levels for the outbound optical light path. The Port Power Management power chart for the outbound optical light path opens.

4 Click on the Export power values to CSV file icon. The Save As window opens.

5 Choose an appropriate location and click Save. The CSV file that contains the optical power level data is saved.

Procedure 19-7 To configure target power offset per direction

The following ports support target power offset:

- A2325A, AHPHG, AHPLG, and ALPHG LINE ports
- A2P2125, A4PSWG, AM2032A, AM2125A, AM2125B, AM2318A, AM2625A, ASWG, and RA2P LINEIN ports (ingress only)
- A2P2125, A4PSWG, AM2032A, AM2125A, AM2125B, AM2318A, AM2625A, ASWG LINEOUT ports (egress only)

The target power offset depends on the ingress and egress direction of the port.

See the *Alcatel-Lucent 1830 Photonic Service Switch 36/32/16 (PSS-36/PSS-32/PSS-16) User Provisioning Guide for more information.*

1 On the equipment navigation tree, expand Network→NE→Shelf→Card→Port.

2 Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

3 Click on the Port Specifics tab, then on the Target Power Offset tab.

4 Click Properties. The Power Offset (Edit) form opens.

5 Configure the Target Power Offset (dB) parameter.

6 Save your changes and close forms.

Procedure 19-8 To view and configure target power offset per channel

The 5620 SAM allows you to view and configure the ingress and egress target power attributes per optical channel.

1 On the navigation tree, expand Network→NE→Shelf→Card.

Note — The following ports support target power offset:

- A2325A, AHPHG, AHPLG, and ALPHG LINE ports
- A2P2125, A4PSWG, AM2032A, AM2125A, AM2125B, AM2318A, AM2625A, ASWG and RA2P LINEIN ports (ingress only)
- A2P2125, A4PSWG, AM2032A, AM2125A, AM2125B, AM2318A, AM2625A, ASWG LINEOUT ports (egress only)

2 Right-click on the Card Slot and choose Properties. The Card Slot (Edit) form opens.

3 Click on the Card Specifics tab, then on the Channel Target Power Offset tab. A list of ingress and egress target power attributes per optical channel appears.

Note — The Channel Target Power Offset tab appears on the form under the following conditions:

- The card is equipped and not pre-provisioned.
- Service is created between the line ports of the two amplifier cards.
- The Power Management Type parameter for the line port of the amplifier card, which is displayed in the Port Specifics→General form, is set to Auto.

4 Choose an entry for which the Applicable? parameter is set to Yes. Click on the Properties tab. The Target Power Offset (Edit) form opens.

5 Configure the User Offset (db) parameter.

6 Click OK.

7 Save your changes and close the form.

Procedure 19-9 To configure baseline types OPT and OPR on ports

The 5620 SAM allows you to create and configure the baseline types OPR (Optical Power Received on OT and OSC points) and OPT (Optical Power Transmitted on OT and OSC points).

1 On the navigation tree, expand Network→NE→Shelf→Card→Port.

2 Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

3 Click on the Port Specifics tab, then on the Performance and the Baseline tabs.

4 Click Create. The Baseline (Create) form opens.

5 Configure the required parameters and click OK.

6 Save your changes and close the forms.

Note — The value of the Reason parameter is modified under the Baseline tab of the Physical Port (Edit) form.

Procedure 19-10 To rekey wave key values of a service

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Choose Optical Transport Service from the object type drop-down menu and click Search. A list of managed optical transport services is displayed.

3 Choose a service and click Properties. The Optical Transport Service (Edit) form opens.

4 Click Rekey Service.

Note — Check the deployment status in the Wave Key panel in the OCH Cross Connects tab of the Optical Transport Service (Edit) form.

Procedure 19-11 To create an unreserved technology type

1 On the navigation tree, expand Network→1830 PSS.

2 Right-click on an 1830 PSS and choose Properties. The Network Element (Edit) form opens.

3 Click on the NE Specifics tab, then on the Technology Types tab.

4 Click Create. The Technology Type (Create) form opens.

5 Configure the required parameters.

6 Save your changes an close the forms.

Procedure 19-12 To set the technology type on OCH cross-connects on the 1830 PSS

1 On the navigation tree, expand Network→1830 PSS.

2 Right-click on the 1830 PSS and choose Properties. The Network Element (Edit) form opens.

3 Click on the OCH CrossConnects tab. A list of OCH cross-connects appears.

4 Choose a cross-connect and click Properties. The OCH Cross Connect (Edit) form opens.

5 Select the technology type in the User Technology AZ panel or the User Technology ZA panel and click OK.

6 Save your changes and close the forms.

Note — The Reserved Technology type is automatically received by the cross-connect only when the technology type is CWDM or DWDM.

Procedure 19-13 To configure an on-demand OSNR scan

1 On the navigation tree, expand Network→NE→Shelf→Card (WTOCMA)→Port.

2 Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

3 Click on the Port Specifics tab, then on the On Demand OSNR Scan tab.

4 Configure the OSNR Measurement Enabled parameter.

Note — The OSNR Scan Status parameter displays the scan status as Not In Progress.

5 Click on the Channels tab.

6 Choose a channel or channels to perform the OSNR scan.

7 Click Start OSNR Scan. The OSNR scan begins.

Note 1 — The OSNR Scan Status parameter displays the scan status as Waiting when the scanning starts and as In Progress during the scanning process.

Note 2 — Click Abort OSNR Scan to abort the scan.

8 Click View results, after the scan completes. The OSNR Scan Results form opens with a graphical view of the OSNR measurements.

9 Perform one of the following:

- **a** Manual refresh of OSNR measurement values:
  - **i** Click on the Refresh OSNR Results icon.
  - **ii** Choose the refresh time interval: 30 s, 60 s, or 90 s.
- **b** Automatic refresh of OSNR measurement values:
  - **i** Click on the Auto-refresh OSNR results icon.
  - **ii** To stop auto-refresh, click on the Stop auto-refresh icon.

10 Save your changes and close the forms.

Procedure 19-14 To configure an OTDR scan

OTDR scans can be configured on the OTDRRX or OTDRTX ports of the A4PSWG or ASWG cards. One of the ports P1 through P8 of the OTDR card must be connected to the appropriate OTDRRX or OTDRTX ports before you start the scan.

Before performing an out-of-service OTDR scan, ensure that the APR Mode parameter in the Port Specifics tab of the LINEIN or LINEOUT port is set as Force.

1 On the equipment tree, expand Network→NE.

2 Right-click on the NE and choose Properties. The Network Element (Edit) form opens.

3 Click on the NE Specifics tab, then on the OTDR Scan Transfer tab.

4 Configure the required parameters.

Note 1 — Ensure that you configure the File Retrieval Location parameter as Local or Remote. The 5620 SAM does not display the result of the OTDR scan if the File Retrieval Location parameter is configured with the default value, Unset.

Note 2 — Configure the File Transfer Protocol parameter as FTP and configure the User Id and Password parameters.

Note 3 — If the File Retrieval Location parameter is configured as Remote, configure the File Server IP Address and Retrieval destination Path parameters.

5 Save and close the form.

6 On the equipment tree, expand Network→NE→Shelf→Card (A4PSWG or ASWG)→Port (OTDRRX or OTDRTX).

7 Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

8 Click on the Port Specifics tab, then on the OTDR Scan Specifics tab.

9 Select the required profile, or click Clear beside the Profile ID parameter to clear a selected or default profile and if required, configure the required parameters to set a custom profile.

> **Note —** Before configuring the profile, you must know the required span length of the configuration, based on which you must select or configure a custom profile for the OTDR scan. For example, if the network span length is 40 km in one direction, and the connection is bidirectional, then the total span length is 80 km.

10 Click Apply, then click Start Scan.

11 Click on the OTDR Scan Results File when the scan is complete.

12 Choose a file and click Retrieve File.

> **Note 1 —** The result is displayed on the JDSU FiberTrace Viewer on the local machine.
>
> The JDSU FiberTrace Viewer can be installed from the link: http://ofs.updatemyunit.net/.
>
> The JDSU FiberTrace Viewer cannot be launched automatically from Firefox or Internet Explorer 8.
>
> **Note 2 —** The result file is stored in the following location: **/opt/5620sam/server/nms/tftp_home/otdrScan/<NE IP address>/**
>
> **Note 3 —** To retrieve all the OTDR scan results from an NE, including the EC card, choose Retrieve All OTDR Scan Result Files from the More Actions contextual menu of the Network Element (Edit) form.
>
> **Note 4 —** The 5620 SAM purges the result files after seven days.

1830 PSS fault management

20 — 1830 PSS fault management

20.1 Overview

The fault management function detects, isolates, and corrects faults in a telecommunication network. Alarm reporting is the notification sent to external management systems for internally detected faults. The fault processing and alarm reporting functions are part of the supervision function of the NE that monitors and manages the NE transmission resources (for example, logical or physical facilities and the associated equipment modules).

Fault management

The 1830 PSS-32 / 1830 PSS-16 is provisioned on a per-port basis to detect faults and report faults, failures, and performance information. Equipment faults can be diagnosed down to an FRU or interface.

A system default alarm profile contains all of the alarms or conditions supported in the system and their severity, that is, Critical, Major, or Minor. The user can change the severity of alarms on each port or facility independently or point to the system profile. The system profile can be modified or reset to the original defaults.

The 5620 SAM correlates the events and alarms against the managed equipment and configured services and policies. The 5620 SAM applies the alarms to the appropriate equipment and services. A correlated alarm is an alarm that causes fault conditions for many objects. For example, if an alarm occurs because a port goes down, all services that use the port receive a notification of the alarm.

You can view the alarm from the service configuration form or from the subscriber information form that lists the affected service. The object information forms contain a faults tab, which lists the alarms that affect the object. The alarms appear in the alarm list. See the *1830 Photonic Service Switch 36/32/16 Product Information and Planning Guide*, the *5620 SAM User Guide*, and the *5620 SAM Troubleshooting Guide* for more information about fault and alarm management. See the *5620 SAM Alarm Reference* for a list of the alarms that the 5620 SAM can generate against the 1830 PSS.

User activity logging

The 5620 SAM logs each GUI and OSS user action, such as 1830 PSS object configuration, in the 5620 SAM database. The User Activity form lists the recent actions; older actions are purged according to the configured retention limits. For more information about the user activity log and configuring the log retention, see the *5620 SAM System Administrator Guide*.

20.2 RCA audit

The 5620 SAM allows you to perform RCA audits on optical links for which the MTU of each endpoint can be determined. The RCA audit policy for physical ports of physical link needs to be configured before performing an RCA audit. See Procedure 20-1 for more information about configuring an RCA audit policy and Procedure 20-2 for more information about performing an RCA audit.

Procedure 20-1 To configure an RCA audit policy

1 Choose Policies→RCA Audits from the 5620 SAM main menu. The RCA Audits form opens.

2 Select Audit Policy (RCA) from the object drop down list and click Create. The Audit Policy (Create) form opens.

3 Configure the required parameters.

4 Select a policy type and click OK. The new RCA audit policy is listed in the RCA Audits form.

5 Choose the new RCA audit policy and click Properties. The Audit Policy (Edit) form opens.

6 Configure the required parameters.

7 Save your changes and close the forms.

Procedure 20-2 To perform an RCA audit of an optical link

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Select Optical Link (Optical Management) from the object drop down list and click Search. A list of optical links appears.

3 Choose an optical link and click Properties. The Optical Link (Edit) form opens.

> **Note —** Ensure that you choose an optical link for which the MTU (bytes) parameter is configured on the General tab of the Physical Port (Edit) forms for the endpoints.

4 Click on the RCA Audit button. The Select RCA Policy to run the audit form appears with a list of configured policies.

5 Choose a the policy that you configured in Procedure 20-1 and click OK.

The 5620 SAM perform the audit and the Info form opens with the audit results.

6 Click OK. The RCA Result tab appears only if there are any issues found during the audit.

7 Click on the RCA Result tab. The RCA audit information is displayed on the Related Problem tab.

8 If required, expand the Optical Link object in the problems tree to view the problems, the associated severity, and the cause.

9 Double-click on a problem object on the navigation tree, to display information about the problem. The Problem (Edit) form opens. The following information is displayed:

- Last Time Changed
- Probable Cause
- Severity
- Description
- Solution

10 Click on the Related Problem tab to view related problems.

Note — The 5620 SAM does not provide a solution for optical link configuration errors.

11 Click on the Caused By Objects tab to view a list of objects that are causing the problem.

12 Choose an object and click Properties. The properties form for the object opens.

13 Click on the tabs to view information about the configuration.

14 Configure the parameters, as required.

15 Save your changes and close the forms.

20.3 Alarm management

The alarm-based fault management system provides the following:

- correlation of alarms with equipment- and service-affecting faults
- updates to the managed-object operational status of equipment, services, and interfaces 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
- ability to log the actions performed to correct the associated fault by adding notes to the alarm
- alarm history for performing trend analysis

See the *5620 SAM User Guide*, the *5620 SAM Alarm Reference*, and *1830 Photonic Service Switch 36/32/16 User Provisioning Guide* for more information.

Alarm suppression

The 5620 SAM does not generate alarms if several SNMP traps are sent in quick succession for the same type of event. The alarms are not generated to prevent 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 1830 PSS continues 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 generated, 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 display how often the alarm was generated. See the *5620 SAM User Guide* for more information.

Additional text

The 5620 SAM displays the alarm description and entity type in the additional text field for the 1830 PSS alarms.

View alarmed object

Alarms generated for network objects allow you to view faults on the 1830 PSS devices in the network down to the service, path, or port level. The 5620 SAM analyzes incoming alarms to ensure that the alarms are listed for the appropriate equipment or service. You can troubleshoot an equipment or service problem using the information. Click on the View Alarmed Object button in the Alarm Info form to navigate to the properties form of the alarmed object. See “Alarm management procedures” in the *5620 SAM User Guide* for more information.

Timestamp

The First Time Detected and Last Time Detected parameters on the Alarm Info form displays the timestamp of the first and last detections of the alarm on the 1830 PSS device.

Resynchronization of alarms

The 5620 SAM allows you to resynchronize the active alarms by choosing Resync All Active Alarms from the Resync contextual menu option at the NE level.

Environmental alarms

The 5620 SAM supports the configuration of the environmental alarm parameters on the User Interface Panel card for the 1830 PSS-32 or 1830 PSS-16 devices and on the PF card for 1830 PSS-4 devices.

Procedure 20-3 To configure environmental alarms

1 Perform one of the following depending on the 1830 PSS device:

  a On the equipment tree expand, Network→1830 PSS→Shelf→Card Slot (PF)

  b On the equipment tree expand, Network→1830 PSS→Shelf→Card Slot (User Interface Panel)

Note 1 — Choose the PF card for the 1830 PSS-4 devices.

Note 2 — Choose the USRPNL card for the 1830 PSS-32, 1830 PSS-16, and 1830 PSS-8 devices.

2 Right-click on a Card Slot and choose Properties. The Card Slot (Edit) form opens.

3 Click on the Environmental Alarms tab. The Environmental Alarms Configuration tab appears with the ports displayed.

Note — The number of ports displayed depends on the device type:

- 1830 PSS-32—eight ports
- 1830 PSS-16—six ports
- 1830 PSS-8—six ports
- 1830 PSS-4—three ports

4 Choose a port and click Properties. The Control Point Input (Edit) form opens.

5 Configure the required parameters.

Note — The change in the alarm message immediately changes the alarm description text of the generated alarms.

6 Save your changes and close the forms.

20.4 Alarm profile management

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 generated for a specific object and to view the aggregated alarm status. The status is also available on the Faults tab of an object property form. Alarm severity profiles can be configured at the NE, shelf, card slot, and interface level. See “Alarm status, severity, and aggregation” in the *5620 SAM User Guide* for more information.

The 5620 SAM displays the severity of an alarm based on the severity on the 1830 PSS device. The default severity of an alarm is Indeterminate on the 5620 SAM. When the severity of an alarm changes on the 1830 PSS device, the alarm with the previous severity is cleared and an alarm is generated on the 1830 PSS device with a new severity. Similarly, the 5620 SAM also clears the alarm and generates an alarm with the severity that matches the severity of the alarm displayed on the 1830 PSS device. The alarm severity update occurs because the Initial Severity Assignment parameter in the Policies tab of the Alarm Settings form is set to Indeterminate.

The alarms generated on the 1830 PSS device with severity as Not Alarmed have a severity of Warning on 5620 SAM. The 5620 SAM allows you to hide and display the alarms raised on the 1830 PSS device with severity as Not Alarmed. To display the alarms in the alarm list of the 5620 SAM, select the Enable NA Alarms check box on the Alarm Setting panel of the NE Specifics tab in the Network Element properties form. To hide the alarms, deselect the Enable NA Alarms parameter. The Enable NA Alarms parameter does not hide or display the historical alarms.

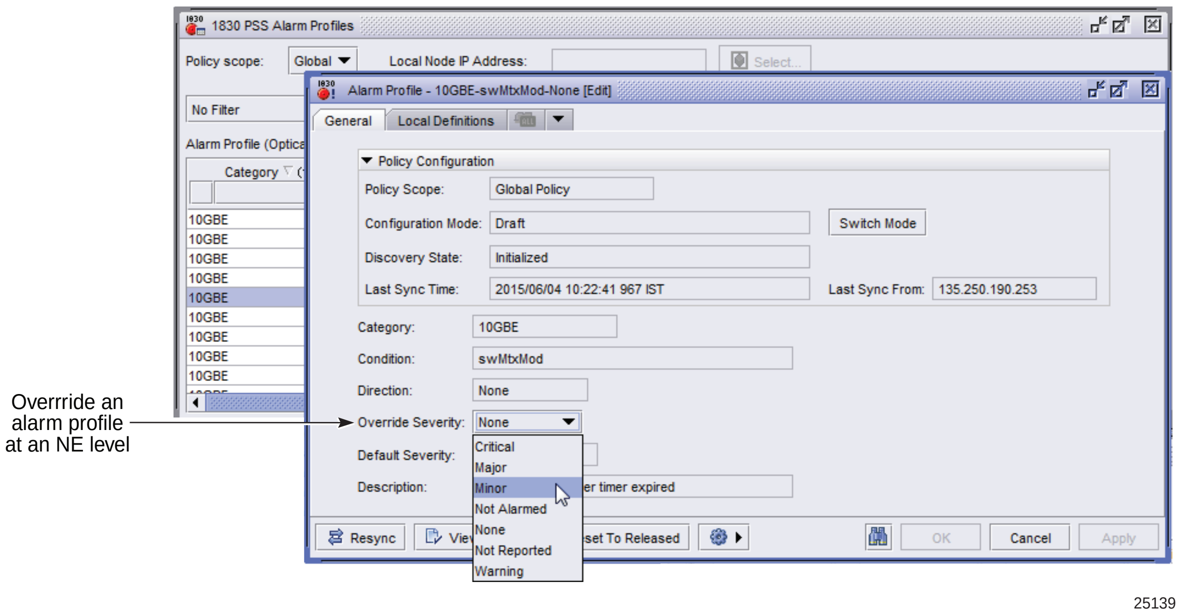
You can change the alarm severity on an 1830 PSS device in one of the following ways:

- NE level; see Procedure 20-4.
- Equipment level; see Procedure 20-5.
- Object level; see Procedure 20-6.

Overriding an alarm severity allows you to have different alarm severities at the NE, equipment, or the object level. For example, an alarm profile with Category of EQPT and Condition of mismatch, can have a severity of Critical at the NE level. At the same time, it can have alarm severity of Major on a shelf instance.

Procedure 20-4 To override an alarm severity at the NE level

Figure 20-1 Override alarm severity at the NE level



This procedure describes how to override an alarm severity at a NE level and distribute it to the required local devices.

1 Choose Tools→1830 Alarm Profiles→1830 PSS Alarm Profiles from the 5620 SAM main menu. The 1830 PSS Alarm Profiles form opens.

2 Click Search. A list of alarm profiles appears.

3 Choose an alarm profile for which you want to override the severity and click Properties. The Alarm Profile (Edit) form opens.

4 Configure the Override Severity parameter click Apply.

5 Click Switch Mode beside the Configuration Mode parameter. The Switch Distribution Mode form opens.

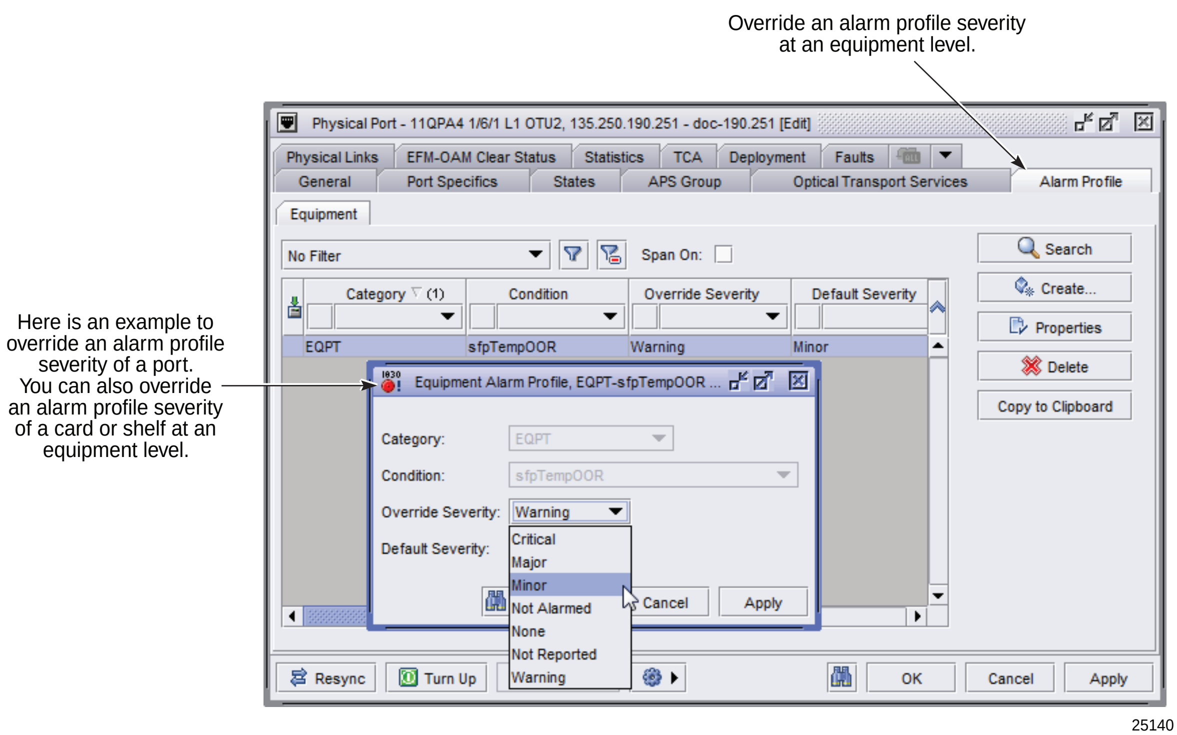
6 Choose the sites from the Available Local Policies list and click on the right-arrow button. The sites are listed in the Selected Local Policies list.

7 Click Distribute. The Status field in the Selected Objects list provides the status of the distribution.

8 Save your changes and close the forms.

Procedure 20-5 To override an alarm severity at the equipment level

Figure 20-2 Override alarm severity at the equipment level



You can override the severity of an alarm profile on the following objects:

- shelf
- card
- port

This procedure describes how to override an alarm severity at the object level.

1 Perform one of the following on the equipment navigation tree:

a Expand to the required shelf level, right-click on the shelf object, and choose Properties. The Shelf (Edit) form opens.

b Expand to the required card level, right-click on the card object, and choose Properties. The Card Slot (Edit) form opens.

c Expand to the required port level, right-click on the port object, and choose Properties. The Physical Port (Edit) form opens.

2 Click on the Alarm Profile tab and click Create. The Select Alarm Category form opens.

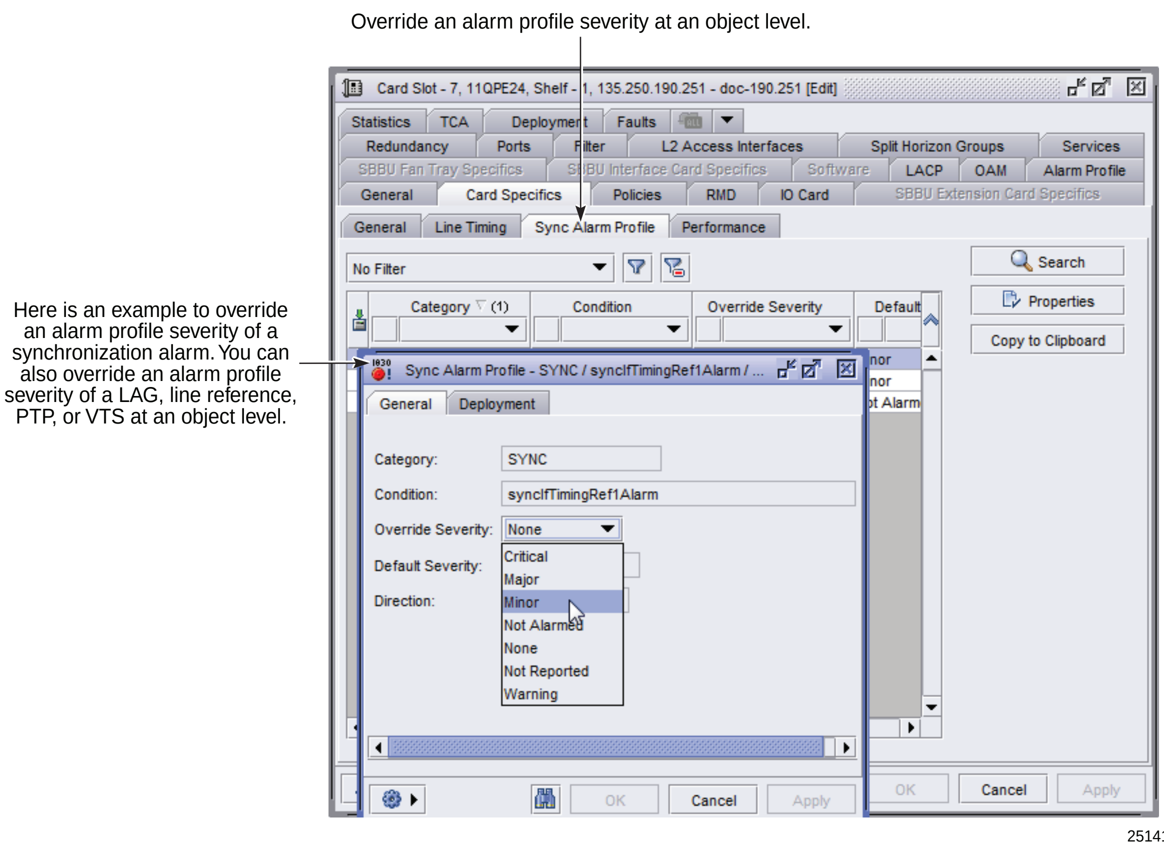
3 Choose a category and click OK. The Equipment Alarm Profile (Create) form opens.

4 Configure the Override Severity parameter and click OK.

5 Save your changes and close the forms.

Procedure 20-6 To override an alarm severity at the object level

Figure 20-3 Override alarm severity at the object level



You can override the severity of an alarm profile on the following objects:

- LAG
- Synchronization
- Line reference
- PTP
- VTS

This procedure describes how to override an alarm severity at the object level.

1 Perform one of the following on the equipment navigation tree:

a Expand to the required 11DPE12A or 11QPE24 card on which a LAG is configured and perform the following:

i Choose LAGs→LAG from the navigation tree.

ii Right-click on the LAG object and choose Properties. The LAG (Edit) form opens.

iii Go to step 2.

b Expand to the 11DPE12A, 11DPE12E, 11QPE24, or PTPCTL card on which SyncE is enabled and perform the following:

i Right-click on the card object and choose Properties. The Card Slot (Edit) form opens.

ii Click on the Card Specifics tab.

iii Click on the Sync Alarm profile tab. A list of alarm profiles appears.

iv Go to step 3.

c Expand to the 11DPE12A, 11DPE12E, 11QPE24, or PTPCTL card on which SyncE is enabled and perform the following:

i Right-click on the card and choose Properties. The Card Slot (Edit) form opens.

ii Click on the Card Specifics tab.

iii Click on the Line Timing tab. A list of line references appears.

iv Choose a line reference from the list and click on Properties. The LineReference (Edit) form opens.

v Go to step 2.

d Expand to the 11DPE12A or PTPCTL card on which PTP clock is enabled and perform the following:

i Right-click on the card and choose Properties. The Card Slot (Edit) form opens.

ii Click on the PTP tab.

iii Click on the Clock tab. A list of clocks appears.

iv Choose a clock from the list and click on Properties. The IEEE 1588 PTP Clock (Edit) form opens.

v Go to step 2.

e Expand to the 11DPE12, 11DPE12A, or 11DPE12E card on which VTS map is configured and perform the following:

i Right-click on the port and choose Properties. The Physical Port (Edit) form opens.

ii Click on the Alarm Profile tab.

iii Click on the VTS tab. A list of VTS alarm profiles appears.

iv Go to step 3.

2 Click on the Alarm Profile tab. A list of alarm profiles appears.

3 Choose an alarm profile for which you want to override the severity and click Properties. The Alarm Profile (Edit) form opens.

4 Configure the Override Severity parameter and click OK. The Alarm Profile (Edit) form closes and the Override Severity column is updated with the configured value in the object properties form.

5 Save your changes and close the forms.

Alarm severity assignment profiles

A condition is a generic term used to refer to a problem or status that is detected or exists on a device. When a device declares a condition, the device determines if the condition is service-effecting, using internal rules. The device provides the corresponding severity from the provisioning data. There are two types of conditions: alarms and events. See the *Alcatel-Lucent 1830 Photonic Service Switch Product Information and Planning Guide* for more information about alarms and events.

Condition severities are managed by alarm severity assignment profiles (ASAPs). The 5620 SAM allows you to modify the severity of an alarm profile. However, you cannot modify the severity of the default alarm profiles that are available on the 1830 PSS-36 and 1830 PSS-64 devices.

Procedure 20-7 To configure an OCS alarm profile

Create an OCS alarm profile

1 Choose Tools→1830 Alarm Profiles→1830 OCS Alarm Profiles from the 5620 SAM main menu. The 1830 OCS Alarm Profiles form opens.

2 Click Create. The OCS Alarm Profile (Create) form opens.

3 Configure the required parameters:

Note 1 — The User Label parameter must not start with the prefix LBL-.

Note 2 — The ASAP Profile ID is not configurable if Auto-Assign ID is selected.

4 Click Apply. The form name changes from OCS Alarm Profile (Create) to OCS Alarm Profile (Edit). Additional tabs appear on the OCS Alarm Profile (Edit) form depending on the value configured for the ASAP Entity Type parameter in step 3.

Distribute an OCS alarm profile

5 Choose Tools→1830 Alarm Profiles→1830 OCS Alarm Profiles from the 5620 SAM main menu. The 1830 OCS Alarm Profiles form opens.

6 Choose the newly created alarm profile and click Switch Mode beside the Configuration Mode parameter. A dialog box appears.

7 Click Yes. The Release - 1830 OCS Alarm Profile form opens.

8 Choose the sites from the Available Objects list and click on the right-arrow button. The sites are listed in the Selected Objects list.

9 Click Distribute. The Status field in the Selected Objects list provides the status of the distribution.

10 Close the Release - 1830 OCS Alarm Profile form. The OCS Alarm Profile (Edit) form reappears with the Configuration Mode parameter updated as Released.

Configure the alarm severity

11 Click on the OCS ASAP Condition tab. A list of available conditions appears.

12 Choose a condition from the list and click Properties. The OCS ASAP Condition (Edit) form opens.

13 Configure the Severity parameter.

14 Click OK. The OCS ASAP Condition (Edit) form closes and the OCS Alarm Profile (Edit) form reappears.

15 Click OK. The OCS Alarm Profile (Edit) form closes.

Procedure 20-8 To assign an OCS alarm profile to objects

Ensure that the OCS alarm profile is configured and distributed to the required device before assigning the profile to an object on the device. OCS alarm profiles can be configured on shelves, cards, ports, facility objects such as OMS, OTS, OMSOCHIF, OTUODUk, OTUk, and IP interfaces such as ES1 ports. Additionally, you can also configure the alarm profiles on the OT panels of the Port Specifics tab of the Physical Port (Edit) form.

1 Choose Equipment from the navigation tree view selector and expand to the required object on the navigation tree.

2 Right-click on the object and choose Properties. The properties form of the object opens.

3 Select an ASAP profile in the Alarm Profile panel.

Note — Depending on the type of object you are configuring the alarm profile on, the Alarm Profile parameter appears on different tabs or panels on the properties form.

4 Click OK. The properties form closes.

20.5 Alarm correlation

The 5620 SAM fault management application supports viewing the graphical representation of alarm correlation. Click on the Alarm List, right-click on the specific alarm in the list, and choose Show Impact from the drop-down menu to display the impact diagram.

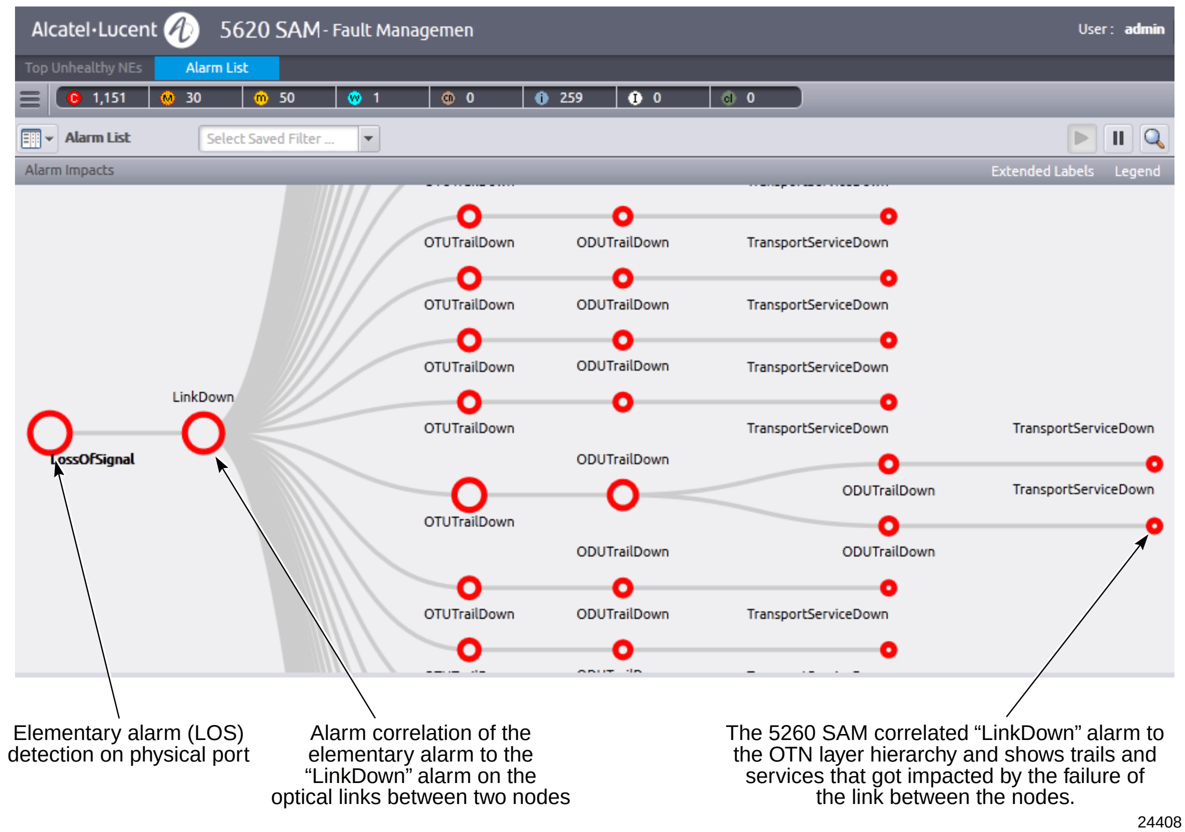
The 1830 PSS alarm correlation diagram provides the graphical representation of the impacted objects in the OTN layer when a fault occurs.

For example, when a port goes out of service due to an optical link failure, the LossOfSignal alarm is reported to the 5620 SAM on the port and the fault management application correlates the LossOfSignal alarm to the LinkDown alarm which in-turn correlates the alarm to the OTN layers above it (that is, OTU, OCH, or OTS). The process continues up to the transport service layer, if a transport service is configured.

The alarm correlation continues up to the L2 or L3 service if a specific SR port is involved in both optical transport service and L2 or L3 service.

In the Figure 20-4, one LinkDown alarm is correlated to multiple OTUTrailDown alarms because all of the OTU trails ride on the optical link.

Figure 20-4 Alarm correlation in 1830 PSS



1830 PSS policy management

21 — 1830 PSS QoS policy

21.1 QoS policy management on the 1830 PSS

You can create, modify, or delete local policies. You can perform the following configurations for global policies using the 5620 SAM policy framework:

- create and distribute the global policies to the 1830 PSS devices
- modify and distribute the modified global policies to the 1830 PSS devices
- delete global policies. If a global policy exists as a local policy on an 1830 PSS device, the local policy is also deleted.

The 5620 SAM supports configuration of QoS policies for the following cards:

- 11OPE8
- 11QCE12X
- 11QPE24

The global policy is distributed to all the supported cards on the 1830 PSS device. You cannot distribute to a specific card. See “NE routing and forwarding” and “QoS policies” in the *5620 SAM User Guide* for distribution information and QoS policy procedures.

The 5620 SAM supports enabling or disabling ingress and egress frame based accounting on the Network→NE→Shelf→Card Slot→Card Slot (Edit) form→Policies tab→Frame Based Accounting tab. When enabled, this feature allows QoS policies to account for the Ethernet frame overhead. When disabled, the queue rates and egress rates do not account for the Ethernet frame overhead. By default, frame based accounting is disabled for both ingress and egress.

QoS policies

The 5620 SAM supports the following types of 1830 PSS QoS policies:

- Access Ingress
- Port Access Egress
- Network
- Network Queue
- Port Scheduler
- Slope

For QoS global policy procedures, see “QoS policies procedures” in the *5620 SAM User Guide*.

Table 21-1 Policies references

Topics	Chapter	Document
Policies overview	Policies overview	*5620 SAM User Guide*
Policies procedures	Policies overview	*5620 SAM User Guide*
QoS policies overview	QoS policies	*5620 SAM User Guide*

Table 21-2 describes the types of 1830 PSS QoS policies.

Table 21-2 1830 PSS QoS policies

Policy type	Applied to	Menu option
7210 and 1830 SAP Access Ingress	Access SAP	Policies→QoS→SROS QoS→Access Ingress→7210 and 1830 SAP Access Ingress. See Procedure “To configure a 7210 and 1830 access ingress policy” in the *5620 SAM User Guide* for information about how to configure the global policy.
7210 and 1830 Port Access Egress	Access port SAP egress	Policies→QoS→SROS QoS→Access Egress→7210 and 1830 Port Access Egress. See Procedure “To configure a 7210 and 1830 port access egress policy” in the *5620 SAM User Guide* for information about how to configure the global policy.
7210 and 1830 Network	Network port Uplink port	Policies→QoS→SROS QoS→Network→7210 and 1830 Network. See Procedure “To configure a 7210 and 1830 network policy” in the *5620 SAM User Guide* for information about how to configure the global policy.
7210 and 1830 Network Queue	Uplink port	Policies→QoS→SROS QoS→Network Queue→7210 and 1830 Network Queue. See Procedure “To configure a 7210 and 1830 network queue policy” in the *5620 SAM User Guide* for information about how to configure the global policy.
7210 and 1830 Port Scheduler	Access and uplink ports	Policies→QoS→SROS QoS→Scheduler→7210 and 1830 Port Scheduler. See Procedure “To configure a 7210 and 1830 port scheduler policy” in the *5620 SAM User Guide* for information about how to configure the global policy.
7210 and 1830 Slope	Access and uplink ports	Policies→QoS→SROS QoS→Slope→7210 and 1830 Slope. See Procedure “To configure a 7210 and 1830 slope policy” in the *5620 SAM User Guide* for information about how to configure the global policy.

21.2 Procedures to configure 1830 PSS QoS local policies

The following procedures describe how to configure local 1830 PSS Qos local policies on the supported cards.

Procedure 21-1 To configure an 1830 PSS access ingress local policy

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 1830 PSS on which you need to configure the access ingress policy.

3 Expand the shelf object on which the card is located.

4 Right-click on the card object and choose Properties. The Card Slot (Edit) form opens.

5 Click on the Policies tab. The Frame Based Accounting tab is displayed.

6 Click on the Access Ingress tab.

7 Click Create. The SAP Access Ingress, Local Policy (Create) form opens.

8 Configure the required parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Number of QoS Classifiers
- Default FC
- MAC Match Criteria type
- IP Match Criteria type
- Allow any IPV6 Match
- IPV6 Match Criteria type

Note — If you need to configure the required parameters for the IP match criteria in step 11, set the IP Match Criteria type parameter to Any.

Configure meter

9 Click on the Meter tab.

i Click Create. The Meter, SAP Access Ingress, Local Policy (Create) form opens.

ii Configure the required parameters:

- ID
- Rate Mode
- MultiPoint

iii Click on the CIR/PIR tab and configure the required parameters:

- CIR Adaptation
- PIR Adaptation
- CIR (kbps)
- PIR (kbps)

Note — Select the MAX check box to configure the CIR and PIR parameters to MAX.

iv Click on the Burst Size tab and configure the required parameters:

- Admin Cbs (kbps)
- Admin Mbs (kbps)

Note — Select the MAX check box to configure the Admin Cbs and Admin Mbs parameters to MAX.

v Click OK to save the changes. A dialog box appears.

vi Click OK button. The Meter, SAP Access Ingress Local Policy (Create) form closes.

Configure forwarding class

10 Click on the Forwarding Classes tab.

i Click Create. The Forwarding Class, SAP Access Ingress, Local Policy (Create) form opens.

ii Configure the required parameters:

- Forwarding Class
- Queue ID
- Meter ID
- Multicast Meter ID
- Broadcast Meter ID
- Unknown Meter ID

iii Click OK to save the changes. A dialog box appears.

iv Click OK. The Forwarding Class, SAP Access Ingress, Local Policy (Create) form closes.

Configure IP, MAC, or IPv6 match criteria

11 Perform one of the following:

a Click on the IP Match Criteria tab.

i Click Create. The IP Match, SAP Access Ingress, Local Policy (Create) form opens.

ii Configure the required parameters:

Note — If you need to configure the required parameters for the IP match criteria, set the IP Match Criteria type parameter to Any in step 8.

- ID
- Displayed Name
- Description
- Forwarding Class
- Protocol
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- Fragment
- Source Port
- Port Src
- Destination Port
- Port Dst
- DSCP

Note — The Protocol parameter must be set to TCP or UDP to configure the required parameters in the Port Properties panel.

iii Click OK to save the changes. A dialog box appears.

iv Click OK. The IP Match, SAP Access Ingress, Local Policy (Create) form closes.

b Click on the MAC Match Criteria tab.

i Click Create. The MAC Match, SAP Access Ingress, Local Policy (Create) form opens.

ii Configure the required parameters:

- ID
- Displayed Name
- Description
- Forwarding Class
- Source MAC
- Source Mask
- Destination MAC
- Destination Mask
- Dot1p
- Dot1p Mask
- Ether Type

iii Click OK to save the changes. A dialog box appears.

iv Click OK. The MAC Match, SAP Access Ingress, Local Policy (Create) form closes.

c Click on the IPv6 Match Criteria tab.

i Click Create. The IPv6 Match, SAP Access Ingress, Local Policy (Create) form opens.

ii Configure the required parameters:

Note — If you want to configure the required parameters for IPv6 Match Criteria, set the Allow any IPV6 Match parameter to true and the IPV6 Match Criteria type to Any in step 8.

- ID
- Displayed Name
- Description
- Forwarding Class
- Protocol
- Source IP
- Src Mask
- Destination IP
- Dst Mask
- Source Port
- Port Src
- Destination Port
- Port Dst
- DSCP

Note — The Protocol parameter must be set to TCP or UDP to configure the required parameters in the Port Properties panel.

iii Click OK to save the changes. A dialog box appears.

iv Click OK. The IPv6 Match, SAP Access Ingress, Local Policy (Create) form closes.

12 Click OK to save the policy. The SAP Access Ingress, Local Policy (Create) form closes.

13 Close the Card Slot (Edit) form.

Procedure 21-2 To configure an 1830 PSS network local policy

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 1830 PSS on which you need to create the network policy.

3 Expand the shelf object on which the card is located.

4 Right-click on the card object and choose Properties. The Card Slot (Edit) form opens.

5 Click on the Policies tab. The Access Ingress tab is displayed.

6 Click on the Network tab.

7 Click Create. The Network Policy, Local Policy (Create) form opens.

8 Configure the required parameters:

- Nw Mgr ID
- Auto-Assign ID
- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Default FC
- Default FC Profile
- Remarking

9 Click on the Egress Forwarding Classes tab.

10 Choose a forwarding class and click Properties. The Egress Forwarding Class, Network Policy (Create) form opens.

11 Configure the required parameters:

- Dot1p In Profile
- Dot1p Out Profile

12 Click OK. The Egress Forwarding Class, Network Policy (Create) form closes and a dialog box appears.

13 Click OK.

14 Map the dot1p tag of the ingress traffic to the ingress queue ID, if required.

i Click on the Ingress Dot1p tab.

ii Click Create. The Network Ingress Dot1p, Network Policy (Create) form opens.

iii Configure the required parameters:

- Dot1p
- Forwarding Class
- Profile

iv Click OK to close the form. The policy form reappears with the newly created object displayed.

v Repeat step 14 for each new rule that you need to add. You can configure up to eight rules.

15 Create network ingress meters.

i Click on the Ingress Meter tab.

ii Click Create. The Network Ingress Meter (Create) form opens.

iii Configure the required parameters:

- ID

Note — You cannot enter the values 1 and 9 for the ID parameter because they are created by default and cannot be deleted. Enter any value up to 12 other than 1 and 9.

- MultiPoint

  Set the parameter to true for multicast meters or false for unicast meters.

iv Click on the CIR/PIR tab.

v Configure the required parameters:

- CIR Adaptation
- PIR Adaptation
- CIR (kbps)
- PIR (kbps)

vi Click on the Burst Size tab.

vii Configure the required parameters:

- Committed Burst Size (kbps)
- Maximum Burst Size (kbps)

viii Click Apply. A dialog box appears.

ix Click OK. The Network Ingress Meter (Create) form closes and the Ingress Meter tab appears.

x Repeat steps ii to ix to create additional network ingress meters. You can create up to nine network ingress meters.

16 Assign the forwarding classes to specific network ingress meters.

i Click on the Ingress FCMeter tab.

ii Click Create. The Network Ingress Forwarding Class (Create) form opens.

iii Configure the required parameters:

- Forwarding class
- Meter (for unicast meters)
- MultiCast-Meter (for multicast meters)

iv Click OK. A dialog box appears.

v Click OK. The Network Ingress Forwarding Class (Create) form closes and the Ingress FCMeter tab appears.

vi Repeat steps ii to v to assign additional forwarding classes to the network ingress meters.

17 Click OK.

18 Click OK to save the policy. The Network Policy, Local Policy (Create) form closes.

19 Close the Card Slot (Edit) form.

Procedure 21-3 To configure an 1830 PSS port access egress local policy

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 1830 PSS on which you need to create the port access egress policy.

3 Expand the shelf object on which the card is located.

4 Right-click on the card object and choose Properties. The Card Slot (Edit) form opens.

5 Click on the Policies tab. The Access Ingress tab is displayed.

6 Click on the Port Access Egress tab.

7 Click Create. The Port Access Egress Policy, Local Policy (Create) form opens.

8 Configure the required parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Scope
- Egress Remark

9 Click on the Queues tab.

10 Choose a queue and click Properties. The PortAccessEgressQueue (Edit) form opens.

11 Configure the required parameters:

- ID
- Displayed Name
- Description

12 Click on the CIR/PIR tab and configure the required parameters:

- CIR Adaptation
- PIR Adaptation
- CIR (kbps)
- PIR (kbps)

13 Click OK. A dialog box appears.

14 Click OK. The PortAccessEgressQueue (Edit) form closes.

15 Repeat steps 10 to 14 to configure additional queues.

16 Click on the Forwarding Classes tab.

17 Click Create. The Network Egress Forwarding Class (Create) form opens.

18 Configure the required parameters:

- Forwarding Class
- In Profile
- Out Profile

19 Click OK. A dialog box appears.

20 Click OK. The Network Egress Forwarding Class (Edit) form closes.

21 Click OK. The Port Access Egress Policy, Local Policy (Create) form closes and a dialog box appears.

22 Click OK.

23 Close the Card Slot (Edit) form.

Procedure 21-4 To configure an 1830 PSS port scheduler local policy

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 1830 PSS on which you need to create the port scheduler policy.

3 Expand the shelf object on which the card is located.

4 Right-click on the card object and choose Properties. The Card Slot (Edit) form opens.

5 Click on the Policies tab. The Access Ingress tab is displayed.

6 Click on the Port Scheduler tab.

7 Click Create. The Port Scheduler, Local Policy (Create) form opens.

8 Configure the required parameters:

- Displayed Name
- Description
- Mode

9 Click OK. The Port Scheduler, Local Policy (Create) form closes and a dialog box appears.

10 Click OK.

11 Close the Card Slot (Edit) form.

Procedure 21-5 To configure an 1830 PSS network queue local policy

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 1830 PSS on which you need to create the network queue policy.

3 Expand the shelf object on which the card is located.

4 Right-click on the card object and choose Properties. The Card Slot (Edit) form opens.

5 Click on the Policies tab. The Access Ingress tab is displayed.

6 Click on the Network Queue tab.

7 Click Create. The Network Queue, Local Policy (Create) form opens.

8 Configure the required parameters:

- Displayed Name
- Description

9 Click on the Queues tab.

10 Choose a queue and click Properties. The NQueueEntry (Edit) form opens.

11 Configure the required parameters:

- ID
- Displayed Name
- Description

12 Click on the Select button in the Queue Management Policy panel. The Select Queue Management Policy form opens.

13 Choose a queue management policy and click OK. The Select Queue Management Policy form closes and the queue policy information is displayed.

14 Configure the required parameters in the Port Parent panel:

- Port Parent
- Weight
- CIR Level

15 Click on the CIR/PIR tab and configure the required parameters:

- CIR Adaptation
- PIR Adaptation
- CIR (kbps)
- PIR (kbps)

16 Click OK. A dialog box appears.

17 Click OK. The NQueueEntry (Edit) form closes.

18 Repeat steps 10 to 17 to configure additional queues.

19 Click OK. A dialog box appears.

20 Click OK. The Network Queue, Local Policy (Create) form closes and a dialog box appears.

21 Click OK.

22 Close the Card Slot (Edit) form.

Procedure 21-6 To configure an 1830 PSS WRED slope local policy

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the 1830 PSS on which you need to create the slope policy.

3 Expand the shelf object on which the card is located.

4 Right-click on the card object and choose Properties. The Card Slot (Edit) form opens.

5 Click on the Policies tab. The Access Ingress tab is displayed.

6 Click on the Slope tab.

7 Click Create. The Slope Policy, Local Policy (Create) form opens.

8 Configure the required parameters:

- Displayed Name
- Description

9 Click on the Queue Slope tab. Eight default queues appear on the form.

When a slope policy is created, the policy uses the parameters of the default policy. You can modify the parameters on the new policy.

10 Choose a queue and click Properties. The QueueSlope, Slope Policy (Create) form opens.

11 Configure the Time Average Factor parameter.

12 Configure the required parameters in the High Slope panel:

- Administrative State
- Start Average
- Max Average
- Max Probability

13 Configure the required parameters in the Low Slope panel:

- Administrative State
- Start Average
- Max Average
- Max Probability

14 Configure the required parameters in the Non Tcp Slope panel:

- Administrative State
- Start Average
- Max Average
- Max Probability

15 Click OK. A dialog box appears.

16 Click OK. The QueueSlope, Slope Policy (Create) form closes and a Queue Slope tab appears.

17 Click OK. The Slope, Local Policy (Create) form closes and the Slope tab on the Card Slot (Edit) form appears.

18 Close the Card Slot (Edit) form.

Procedure 21-7 To associate a slope policy with a port

Before you perform the procedure, ensure that the assigned rate is configured on the port.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→NE→Shelf→Card Slot→Port.

3 Right-click on the Port icon and choose Properties. The Physical Port (Edit) form opens.

4 Click on the QoS Pool tab. The QoS buffer pools appear on the form.

5 Choose an entry and click on the Properties tab. The QoS Pool (Edit) form opens.

6 Click on the Select button in the Slope Policy panel. The Select Slope Policy form opens with a list of slope policies.

7 Choose a slope policy and click OK. The Select Slope Policy form closes and the QoS Pool (Edit) form appears.

8 Click OK. The QoS Pool (Edit) form closes and the Physical Port (Edit) form appears.

9 Click OK. A dialog box appears.

10 Click Yes to apply the changes.

22 — 1830 PSS ACL IP filter

22.1 1830 PSS ACL IP filter overview

ACL filters are used by routers and switches to allow or deny data into or out of a network interface. When an ACL is configured on an interface, the network device analyzes the data that passes through the interface, compares it to the configuration set in the ACL pattern, and allows or denies the data into or out of the interface.

The 5620 SAM supports the creation and management of the ACL IP filters. The main elements of the 1830 PSS ACL IP filtering process are patterns, filters, and port-to-ACL-filter associations. Patterns contain the criteria for traffic filtering, such as source IP, source port, destination IP, destination port, protocol, and so on. ACL filters are the ordered lists of ACL patterns. You can assign a maximum of two filters to each ACL-applicable port, one in the receive direction and one in the transmit direction.

Table 22-1 lists the cards and ports that support ACL IP filtering.

Table 22-1 Cards and ports that support ACL IP filtering

Cards	Ports [1]
OT ports with GCC enabled	Ports supporting GCC
A2325A, AHPHG, AHPLG, ALPHG, AM2017B, AM2325B	OSC
EC (PSS-4)	OAMP
MTC1T9, MXEC320H	E1, E2, OAMP
USRPNL	E1, E2, OAMP, VOIP

Note

(1) If a port is unassigned, the ACL IP Filters tab does not appear in the Physical Port (Edit) form.

22.2 Workflow to configure 1830 PSS WDM ACL IP filtering

1. Enable ACL configuration on an 1830 PSS device. See Procedure 22-1.
2. Create an ACL IP pattern. See Procedure 22-2.
3. Create an ACL IP filter. See Procedure 22-3.
4. Assign an ACL IP filter to a port. See Procedure 22-4.

22.3 1830 PSS WDM ACL IP filter procedures

The following procedures describe how to create and assign an ACL IP filter to a port that supports filtering.

Procedure 22-1 To enable ACL configuration on an 1830 PSS

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Right-click on the 1830 PSS on which you need to enable ACL configuration and choose Properties. The Network Element (Edit) form opens.

3 Click on the ACL tab.

4 Configure the required parameters:

- Receive Action
- Transmit Action

5 Select the ACL Configuration via SNMP Enabled check box.

6 Click Apply. A dialog box appears.

7 Click Yes.

8 Close the Network Element (Edit) form.

Procedure 22-2 To create an 1830 PSS ACL IP pattern

1 Choose Policies→Filter→PSS ACL IP Filter from the 5620 SAM main menu. The PSS ACL Filter Policies form opens.

2 Click Create and choose Create ACL IP Pattern. The ACL Pattern, Global Policy (Create) form opens.

3 Configure the required parameters:

- Pattern ID
- Action
- ICMP Error Reporting Enabled
- Source IP Address
- Source IP Mask Prefix
- Destination IP Address
- Destination IP Mask Prefix
- Internet Protocol
- IP Fragmentation

4 Configure the required parameters based on the value configured for the Internet Protocol parameter in step 3:

- TCP/UDP Source Port
- TCP/UDP Destination Port
- ICMP Type
- ICMP Code
- TCP Established

5 Click Apply. The ACL Pattern, Global Policy (Edit) form appears.

6 Click Switch Mode beside the Configuration Mode parameter. A dialog box appears.

7 Click Yes. The Release - 1830 PSS ACL IP Pattern form appears.

8 Choose the sites from the Available Objects list and click on the right-arrow button. The sites are listed in the Selected Objects list.

9 Click Distribute. The Status field in the Selected Objects list provides the status of the distribution.

10 Close the Release - 1830 PSS ACL IP Pattern form. The ACL Pattern, Global Policy (Edit) form reappears with the Configuration Mode parameter set as Released.

11 Close the ACL Pattern, Global Policy (Edit) form. The PSS ACL Filter Policies form reappears.

12 Choose ACL Pattern (Optical Access Control Lists) from the object drop-down menu and click Search. The list of ACL patterns appears.

13 Close the PSS ACL Filter Policies form.

Procedure 22-3 To create an 1830 PSS ACL IP filter

1 Choose Policies→Filter→PSS ACL IP Filter from the 5620 SAM main menu. The PSS ACL Filter Policies form opens.

2 Click Create and choose Create ACL IP Filter. The ACL Filter, Global Policy (Create) form opens.

3 Configure the Filter Name parameter and click on the Apply button. The ACL Filter, Global Policy (Edit) form appears.

4 Click on the ACL Pattern Binding tab.

5 Click on the Add Pattern button. The ACL Pattern Binding (Create) form opens.

6 Click on the Select button beside the Pattern ID parameter. The Select Pattern - ACL Pattern Binding form opens with a list of ACL patterns.

7 Choose an ACL pattern from the list and click OK. The Select Pattern - ACL Pattern Binding form closes and the ACL Pattern Binding (Create) form reappears.

8 Configure the Pattern Index parameter.

9 Click OK. The ACL Pattern Binding (Create) form closes and the filter is listed under the ACL Pattern Binding tab in the ACL Filter (Edit) form.

10 Click on the General tab.

11 Click Switch Mode beside the Configuration Mode parameter. A dialog box appears.

12 Click Yes. The Release - 1830 PSS ACL IP Filter form opens.

13 Choose sites from the Available Objects list and click on the right-arrow button. The sites are listed in the Selected Objects list.

14 Click Distribute. The Status field in the Selected Objects list provides the status of the distribution.

15 Close the Release - 1830 PSS ACL IP Filter form. The ACL Filter, Global Policy (Edit) form reappears with the Configuration Mode parameter set as Released.

16 Close the ACL Filter, Global Policy (Edit) form. The PSS ACL Filter Policies form reappears.

17 Choose ACL Filter (Optical Access Control Lists) from the object drop-down menu and click Search. The list of ACL filters appears.

18 Close the PSS ACL Filter Policies form.

Procedure 22-4 To assign an ACL IP filter to a port

Ensure that the Administrative State of the port to which an ACL IP filter is assigned is configured either as Up or Maintenance. Table 22-1 lists the cards and ports that support ACL IP filtering.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand an 1830 PSS device icon to the port level.

3 Right-click on the port for which you want to assign an ACL IP filter, and choose Properties. The Physical Port (Edit) form opens.

4 Click on the ACL IP Filters tab.

Note 1 — Unassigned ports do not display the ACL IP Filters tab.

Note 2 — The ACL IP Filters tab is hidden by default. To view the tab, click on the Show All Tabs icon on the right side of the form.

5 Click Create. The IP Filter Cfg (Create) form opens.

6 Configure the Direction parameter.

7 Click on the Select button beside the Filter Name parameter. The Select Filter ID - IP Filter Cfg form opens with a list of available IP filters.

8 Choose a filter from the list and click OK. The Select Filter ID - IP Filter Cfg form closes and the IP Filter Cfg (Create) form reappears.

9 Select the Filter Enabled check box.

10 Click OK. A dialog box appears and the IP Filter Cfg (Create) form closes.

11 Click OK. The assigned filter is listed under the ACL IP Filters tab.

12 Click OK. A dialog box appears.

13 Click Yes. The Physical Port (Edit) form closes.

22.4 1830 PSS OCS ACL IP filter

The 5620 SAM allows you to view and modify the 15 default ACL IP filters on an 1830 PSS OCS device.

Procedure 22-5 To configure an 1830 PSS OCS ACL IP filter

1 Choose Policies→Filter→PSS ACL IP Filter from the 5620 SAM main menu. The PSS ACL Filter Policies form opens.

2 Choose OCS ACL IP Filter (Optical Access Control Lists) from the object drop-down menu and click Search. A list of the default OCS ACL IP filters appears.

3 Choose a filter that you need to modify and click Properties. The OCS ACL IP Filter (Edit) form opens.

4 Click on the IP Filter Entries tab. A list of existing entries for the filter appears.

5 Click Create. The IP Filter Entry (Create) form opens.

6 Configure the required parameters:

- Entry ID
- Auto-Assign ID
- Action
- Incoming Interface
- Incoming Interface ID
- Source IP Address
- Source IP Mask
- Destination IP Address
- Destination IP Mask

7 Perform one of the following additional actions depending on the filter chosen in step 3:

a If you chose ICMP filter in step 3, configure the required parameters:

- ICMP Type
- ICMP Code

b If you chose IP Forwarding filter in step 3, configure the required parameters:

- Internet Protocol
- Fragment
- Connection State

Note 1 — If you configured the Internet Protocol parameter as ICMP, configure the ICMP Type and ICMP Code parameters.

Note 2 — If you configured the Internet Protocol parameter as TCP or UDP, configure the Source Port Type and Destination Port Type parameters.

Note 3 — If you configured the Internet Protocol parameter as Others, enter the value in the text box next to the Internet Protocol parameter.

c If you chose any other filter in step 3, configure the Source Port Type parameter in the Ports panel.

Note — If the Source Port Type parameter is configured as Others, enter the value in the text box next to the Source Port Type parameter.

8 Click OK. The IP Filter Entry (Create) form closes and a dialog box appears.

9 Click OK. The new IP filter entry is added to the list under the IP Filter Entries tab in the OCS ACL IP Filter (Edit) form.

10 Click OK. A dialog box appears.

11 Click Yes. A dialog box appears.

12 Click Yes. The OCS ACL IP Filter (Edit) form closes and the PSS ACL Filter Policies form reappears.

13 Close the PSS ACL Filter Policies form.

1830 PSS network management

23 — 1830 PSS Ethernet OAM

23.1 Ethernet OAM overview

The 5620 SAM supports Ethernet OAM on the following cards on the Ethernet optical transport services, such as 802.1ag, Y.1731, and 802.3ah:

- 11DPE12A
- 11DPE12E
- 11OPE8
- 11QCE12X
- 11QPE24

Ethernet OAM defines the OAM sublayer, which is used for monitoring link operations such as remote fault indication and remote loopback control. The network operators can monitor the health of the network and determine the location of failing links or fault conditions. The EFM OAM provides data link layer mechanisms to complement applications that may reside in higher layers.

The OAM information is transported in slow protocol frames which are called OAMPDUs. The OAMPDUs contain the appropriate control and status information to monitor, test and troubleshoot EFM OAM-enabled links. The OAMPDUs traverse a single link that is passed between peer OAM entities, and are not forwarded by MAC clients (such as bridges or switches), unless they are configured.

The following EFM OAM functions are supported on the 11DPE12A, 11DPE12E, 11OPE8, 11QCE12X, and 11QPE24 cards:

- EFM OAM capability discovery
- active and passive modes
- remote failure indication
- local and remote loopbacks
- EFM OAMPDU tunneling
- high-resolution EFM OAM timers (500 ms interval)

Ethernet CFM

Ethernet CFM supports end-to-end service management in an L2 network. The CFM tools provide path discovery and fault detection, isolation and notification.

Table 23-1 lists the supported Ethernet CFM test types and the objects for which the tests can be performed.

Table 23-1 Ethernet CFM test types and test objects in the Ethernet network level

Test type	Network object or service component for test
CFM Loopback - Procedure 23-3	SAP or Ethernet Ring Path End Point
CFM Link trace - Procedure 23-4	
CFM One Way Delay - Procedure 23-5	
CFM Two Way Delay - Procedure 23-6	
CFM Two Way Synthetic Loss Measurement (SLM) - Procedure 23-7	
CFM Loss Measurement (LM) - Procedure 23-8	

CFM diagnostics tests

The following CFM diagnostic tests detect connectivity failure.

CFM loopback

The 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 MIP can reply to a loopback message if the destination MAC address matches the MAC address of the MEP or MIP. The CFM loopback tests verify connectivity to a specific MEP or MIP.

CFM link trace

The 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. The frame delay is 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 two-way SLM

The CFM two-way SLM test measures the synthetic loss which is used to check for packet loss.

CFM LM

The CFM LM test measures the counter values applicable for ingress and egress service frames where the counters maintain a count of transmitted and received data frames between a pair of MEPs.

23.2 Components of Ethernet CFM

Maintenance domain (MD) or maintenance entity (ME)

A maintenance domain or maintenance entity defines the boundaries for connectivity fault management. The 5620 SAM supports none, DNS, MAC, and string formats for a maintenance domain. The value of MD value for which varies from 0 to 7. The level of an MD distinguishes the administrators involved in monitoring a service and provides a hierarchy among them. The hierarchy prevents CFM traffic from flowing from a low level to flow to a high level.

Maintenance association (MA) or maintenance entity group (MEG)

A maintenance association or maintenance entity group includes a set of maintenance end points. Each MEG in a network is identified by its ID which is composed of the MD name and the MEG name of a particular format. The name of a MEG is 13 characters long if the name format is icc-based.

Maintenance end points (MEP)

A maintenance end point initiates, processes, and terminates Ethernet CFM functions. A MEP has two directions, up or down. The Up-MEP directs the traffic towards the switch fiber and the Down-MEP directs the traffic towards the SAPs, away from the switch fiber.

The 5620 SAM supports configuration of both Up-MEPs and Down-MEPs using Ethernet cards. The Up-MEPs are configured on client ports to monitor services. The Up-MEPs supports the configuration with an interval of one second or longer. Down-MEPs monitor links and require a short interval like 3.3 ms. A Down-MEP is configured on each path of an Ethernet ring.

23.3 Ethernet CFM procedures

Procedure 23-1 To configure Ethernet CFM

Configure the Flow Continuity Monitoring parameter as CCM under the Card Specifics→General tab of the 11DPE12A and 11DPE12E Card Slot (Edit) form, before configuring the Ethernet CFM.

Configure MD and distribute to 1830 PSS

1 Choose Tools→Ethernet CFM→Maintenance Domain Policies from the 5620 SAM main menu. The Maintenance Domain Policies form opens.

2 Perform one of the following:

a Modify an existing MD.

i Configure a filter if required and click Search. A list of MDs appears.

ii Choose an MD and click Properties. The Maintenance Domain Global Policy (Edit) form opens.

b Create an MD.

i Click Create. The Maintenance Domain - Global Policy (Create) form opens.

ii Configure the required parameters:

- MD Mgr Object ID
- Maintenance Domain ID
- Name Type
- Name
- Description
- Level

Note 1 — Configure Name Type parameter as none for creating a MEG with icc-based Name Format parameter in step 11.

Note 2 — The MD Mgr Object ID and Maintenance Domain ID parameters need not be configured if the respective Auto-Assign ID check box is selected.

iii Click Apply. The form displays additional tabs, and the form name changes to Maintenance Domain Global Policy (Edit).

3 Click Switch Mode in the Policy Configuration panel. A dialog box appears.

4 Click Yes. The Release - Maintenance Domain form opens with the list of 1830 PSS devices available for distribution in the Available Objects list.

5 Choose one or more devices and click on the right arrow button. The device or devices move to the Selected Objects list on the right side of the form.

6 Click Distribute. The 1830 PSS policy is distributed to the 1830 PSS device or devices.

7 Close the Release - Maintenance Domain, Maintenance Domain (Edit), and Maintenance Domain Policies forms. The Maintenance Domain Policies form reappears with the newly configured MD.

Add global MEG to MD

8 Choose the newly configured MD and click Properties. The Maintenance Domain - Global Policy (Edit) form opens.

9 Click on the Global Maintenance Entity Group tab.

10 Click Create. The Global Maintenance Entity Group (Create) form opens.

11 Configure the required parameters:

- Auto-Assign ID
- Name
- Description
- Administrative State

12 Configure the Name Format and Name parameters in the Maintenance Entity Group panel. If you set the Name Format parameter to icc-based, the associated name must be 13 characters long.

Note — Configure Name Type parameter in step 2 as none for creating a MEG with icc-based Name Format.

13 Configure the required parameters in the Initial MEG Configuration panel:

- Initial CCM Interval
- Initial MHF-Creation
- Initial MIP LTR Priority

14 Click OK. The Global Maintenance Entity Group (Create) form closes, and the Maintenance Domain - Global Policy (Edit) form reappears with the newly configured global MEG.

Associate 1830 PSS and service with global MEG

15 Choose a the newly configured global MEG and click Properties. The Global Maintenance Entity Group (Edit) form opens.

16 Click on the NE Maintenance Entity Group tab.

17 Click Create. The NE Maintenance Entity Group (Create) form opens.

18 Click on the Select button in the Site panel. The Select Site form opens.

19 Click Search. A list of sites is displayed.

20 Choose an 1830 PSS device and click OK. The Select Site form closes, and the site information is displayed on the NE Maintenance Entity Group (Create) form.

21 Click on the Select button in the Card/RMD panel. The Select Card/RMD form opens.

22 Click Search. A list of supported OT cards is displayed.

23 Choose an OT card and click OK. The Select Card/RMD form closes, and the card information is displayed on the NE Maintenance Entity Group (Create) form.

24 Click on the Service tab.

25 Click Create. The MEG Service (Create) form opens.

26 Configure the required parameters:

- Service ID
- MHF-Creation
- VLAN ID

Note — Only the parameters that are supported on the selected card are displayed when you open the MEG Service (Create) form.

27 Click OK. The MEG Service (Create) closes, and the service information is displayed on the NE Maintenance Entity Group (Create) form.

28 Click OK to save the changes. The newly configured NE MEG appears in the NE Maintenance Entity Group tab of the Global Maintenance Entity Group (Edit) form.

Configure MEP

Note 1 — Ensure that you create an optical SubGigE service and associate it to the MEG before creating a MEP, while using the 11DPE12A card.

Note 2 — Ensure that you create a VPLS service and associate it to the MEG before creating a MEP, while using the 11QPE24, 11OPE8, and 11QCE12X cards.

29 Click on the Managed MEP tab.

30 Click Create. The MEP (Create) form opens.

31 Configure the ID parameter.

32 Click on the Select button beside the Maintenance Domain OD parameter and choose the newly configured MD.

33 Configure the required parameters:

- Direction
- Administrative State
- MAC Address
- Type
- Interface Type

Note — The values for the Interface Type parameter are:

- Port and LAG for 11DPE12A card
- SAP and Ethernet Ring Path End Point

34 Configure the port, SAP, LAG, or Ethernet ring path endpoint in the respective panels based on the value configured for the Interface Type parameter.

35 Choose an entry and click OK. The Select MEP form closes and the MEP (Create) form reappears.

36 Click OK. The MEP (Create) form closes and the NE Maintenance Entity Group (Edit) form reappears with the newly configured MEP.

Add remote MEP to NE MEG

37 Click on the Remote MEP tab in the NE Maintenance Entity Group (Edit) form. and click Create. The Remote MEP (Create) form opens.

38 Configure the MEP ID parameter. The Remote MEP (Create) form closes and the NE Maintenance Entity Group (Edit) form reappears.

39 Click Apply to save the configuration.

23.4 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 according to SLAs. 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.

You can create and schedule the execution of OAM tests using the 5620 SAM Service Test Manager, or STM. The prerequisites for running the CFM tests are:

- Choose CCM option for the Flow Continuity Monitoring parameter on the Card Specifics→General tab of the Card Slot (Edit) form.
- Configure an Ethernet CFM MD and subordinate objects associated with the MD such as a Global MEG, MEG, and MEP. See Procedure 23-1.

Proactive OAM tests are carried out for proactive reporting of fault or performance results. On-demand OAM tests are initiated by manual intervention for a limited time to carry out diagnostics. On-demand OAM can result in single or periodic OAM actions during the diagnostics time interval. The Proactive OAM tests are configured in the 5620 SAM by enabling the NE Schedulable parameter on the CFM test (Create) forms.

Table 23-2 Proactive OAM tests and supported cards

CFM tests	Supported cards
CFM two-way delay	11DPE12A 11OPE8 11QCE12X 11QPE24
CFM two-way SLM	11DPE12A 11OPE8 11QCE12X 11QPE24

Table 23-3 On-demand OAM tests and supported cards

CFM tests	Supported cards
CFM loopback	11DPE12A 11OPE8 11QCE12X 11QPE24
CFM link trace	11OPE8 11QCE12X 11QPE24
CFM one way delay	11DPE12A
CFM two way delay	11DPE12A 11OPE8 11QCE12X 11QPE24
CFM two way SLM	11DPE12A 11OPE8 11QCE12X 11QPE24
CFM LM	11DPE12A

23.5 OAM diagnostic test procedures

Use the following procedures to create and run OAM diagnostic tests.

Procedure 23-2 To configure Ethernet OAM fault management mode

Perform the following procedure to configure the Ethernet OAM fault management mode and the Ethernet CFM redundancy on the following cards:

- 11OPE8
- 11QCE12X
- 11QPE24

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the equipment view.

2 Expand to the level of the required card.

3 Right-click on the card and choose Properties. The Card Slot (Edit) form opens.

4 Click on the OAM tab.

5 Configure the required parameters on the Ethernet CFM Redundancy panel, as required:

- MC LAG Standby Inactive
- MC LAG Prop hold Time (seconds)

6 Configure the Fault Management Mode parameter on the Ethernet OAM Fault Management panel.

Note — Select IEEE for configuring the IEEE 802.1ag compliant fault management mode. Select ITU-T for configuring the ITU-T G.8021 compliant fault management mode.

7 Click OK. The Card Slot (Edit) form closes.

Procedure 23-3 To create and run an on-demand CFM loopback test

Perform this procedure to manually create and run a CFM loopback test. You can create multiple CFM loopback tests for an originating MEP.

Note — The maximum number of continuous CFM loopback tests that can be run is 300, provided that the SAA packet per second rate of 200 pps is not exceeded. The total number of continuous tests must share this maximum rate of 200 pps.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click Create.

3 Choose Ethernet CFM→CFM Loopback. The CFM Loopback Test (Create) form opens.

4 Configure the required parameters:

- Auto-Assign ID
- Name
- Description
- Administrative State

5 Deselect the NE Schedulable check box.

6 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG form opens.

7 Specify a search filter, if required, and click Search. A list of global MEGs is displayed.

8 Select an entry and click OK. The Select Global MEG form closes, and the CFM Loopback Test (Create) form displays the global MEG.

9 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Loopback form opens.

10 Specify a search filter, if required, and click Search. A list of MEPs is displayed.

11 Select a MEP in the list and click OK. The Select Originating MEP - CFM Loopback form closes, and the CFM Loopback Test (Create) form displays the MEP information.

12 Perform one of the following:

a To select a MEP as the test destination:

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 Choose a MEP and click OK. The Select MEP - CFM Loopback form closes, and the CFM Loopback Test (Create) form refreshes.

b To select a MIP as the test destination:

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 Choose a MIP and click OK. The Select MIP - CFM Loopback form closes, and the CFM Loopback Test (Create) form refreshes.

c To select an unmanaged MEP as the test destination:

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 Choose an unmanaged MEP and click OK. The Select Unmanaged MEP - CFM Loopback form closes, and the CFM Loopback Test (Create) form refreshes.

13 Configure the required parameters in the MEP Transmit LBM Information panel:

- Data TLV Size or Padding
- Data Size
- VLAN Priority
- Number of Test Packets
- VLAN Drop Enable
- LBM Interval (deciseconds)
- LBM Timeout (seconds)

14 Click Apply to save the changes.

15 To run the test, click Execute.

16 Click on the Results tab to view the test results.

Procedure 23-4 To create and run an on-demand CFM link trace test

Note — The maximum number of continuous CFM link trace tests that can be run is 300, provided that the SAA packet per second rate of 200 pps is not exceeded. The total number of continuous tests must share this maximum rate of 200 pps.

However, it is recommended that number of continuous CFM link trace tests run should be kept well below the maximum allowed limit.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click Create.

3 Choose Ethernet CFM→CFM Link Trace from the Create contextual menu. The CFM Link Trace Test (Create) form opens.

4 Configure the required parameters:

- Auto-Assign ID
- Name
- Description
- Administrative State

5 Deselect the NE Schedulable check box.

6 Click on the Select button beside the Global ID field to choose a global MEG. The Select Global MEG - CFM Link Trace form opens.

7 Specify a search filter, if required, and click Search. A list of global MEGs is displayed.

8 Select an entry and click OK. The Select Global MEG - CFM Link Trace form closes, and the CFM Link Trace Test (Create) form displays the global MEG.

9 Click on the Select button beside the ID field to choose an originating MEP. The Select Originating MEP - CFM Link Trace form opens.

10 Specify a search filter, if required, and click Search. A list of MEPs is displayed.

11 Select a MEP in the list and click OK. The Select Originating MEP - CFM Link Trace form closes, and the CFM Link Trace Test (Create) form displays the MEP information.

12 Perform one of the following:

a To select a MEP as the test destination:

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 Choose a MIP and click OK. The Select MEP - CFM Link Trace form closes, and the CFM Link Trace Test (Create) form refreshes.

b To select a MIP as the test destination:

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 Choose a MIP and click OK. The Select MIP - CFM Link Trace form closes, and the CFM Link Trace Test (Create) form refreshes.

c To select an unmanaged MEP as the test destination:

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 Choose an unmanaged MEP and click OK. The Select Unmanaged MEP - CFM Link Trace form closes, and the CFM Link Trace Test (Create) form refreshes.

13 Configure the TTL parameter in the MEP Transmit LTM Information panel.

14 Click Apply to save the changes.

15 To run the test, click Execute.

16 Click on the Results tab to view the test results.

Procedure 23-5 To create and run an on-demand CFM one-way delay test

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click Create.

3 Choose Ethernet CFM→CFM One Way Delay Test. The CFM One Way Delay Test (Create) form opens.

4 Configure the required parameters:

- Auto-Assign ID
- Name
- Description
- Administrative State

5 Click on the Select button beside the Global ID parameter to choose a global MEG. The Select Global MEG form opens.

6 Specify a search filter, if required, and click Search. A list of global MEGs is displayed.

7 Choose an entry and click OK. The Select Global MEG form closes, and the CFM One Way Delay Test (Create) form displays the global MEG.

8 Click on the Select button beside the ID parameter 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 Search. A list of MEPs is displayed.

10 Choose a MEP and click OK. 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 in the MEP Transmit Information panel:

a Choose a MEP as the test destination.

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 Choose a MEP and click OK. The Select MEP - CFM One Way Delay form closes, and the CFM One Way Delay Test (Create) form refreshes.

b Choose a MIP as the test destination.

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 Choose a MIP and click OK. The Select MIP - CFM One Way Delay form closes, and the CFM One Way Delay Test (Create) form refreshes.

c Choose an unmanaged MEP as the test destination.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select Unmanaged MEP - CFM One Way Delay form opens.

ii Choose an unmanaged MEP and click OK. The Select Unmanaged MEP - CFM One Way Delay form closes, and the CFM One Way Delay Test (Create) form refreshes.

12 Configure the Priority parameter in the MEP Transmit DMM Information panel.

13 Click Apply. The form displays additional buttons and tabs.

14 Click Execute to run the test.

15 Click on the Results tab to view the test results.

Procedure 23-6 To create and run an on-demand and proactive CFM two-way delay test

Note — You can run up to 300 continuous CFM two-way delay tests when you do not exceed the SAA packet per second rate of 200 pps. The total number of continuous tests must share this maximum rate of 200 pps.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click Create.

3 Choose Ethernet CFM→CFM Two Way Delay Test. The CFM Two Way Delay Test (Create) form opens.

4 Configure the required parameters:

- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable

Note 1 — The NE Schedulable parameter is enabled for the proactive CFM two-way delay test.

Note 2 — When the NE Schedulable parameter is enabled, two additional tabs Test Parameters and Results Configuration appear in the form.

5 Click on the Select button beside the Global ID parameter to choose a global MEG. The Select Global MEG form opens.

6 Specify a search filter, if required, and click Search. A list of global MEGs is displayed.

7 Choose an entry and click OK. The Select Global MEG form closes, and the CFM Two Way Delay Test (Create) form displays the global MEG.

8 Click on the Select button beside the ID parameter 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 Search. A list of MEPs is displayed.

10 Choose a MEP and click OK. 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 in the MEP Transmit Information panel:

a Choose a MEP as the test destination.

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 Choose an entry and click OK. The Select MEP - CFM Two Way Delay form closes, and the CFM Two Way Delay Test (Create) form refreshes.

b Choose a MIP as the test destination.

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 Choose an entry and click OK. The Select MIP - CFM Two Way Delay form closes, and the CFM Two Way Delay Test (Create) form refreshes.

c Choose an unmanaged MEP as the test destination.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select Unmanaged MEP - Two Way Delay form opens.

ii Choose an entry and click OK. The Select Unmanaged MEP - CFM Two Way Delay form closes, and the CFM Two Way Delay Test (Create) form refreshes.

12 When the NE Schedulable parameter is enabled in step 4, go to step 15. Otherwise, go to step 13.

13 Configure the required parameters in the MEP Transmit DMM Information panel:

- VLAN Priority
- Data Size (octets)

14 Go to step 18.

15 Click on the Test Parameters tab and configure the required parameters in the Execution Details panel:

- Packet Interval (milliseconds)
- Packet Timeout (milliseconds)
- Forwarding Class
- Size (octets)

16 Click on the Results Configuration tab and click on the Select button in the Card TCA Profile panel. The Select Card TCA Profile - CFM Two Way Delay Test form opens.

17 Choose an entry and click OK. The Select Card TCA Profile - CFM Two Way Delay Test form closes and the CFM Two Way Delay Test (Create) form opens.

18 Click Apply to save the changes.

19 Click on the Results tab to view the test results.

Procedure 23-7 To create and run an on-demand and proactive CFM two-way SLM test

Note — You can run up to 300 continuous CFM two-way SLM tests when you do not exceed the SAA packet per second rate of 200 pps. The total number of continuous tests must share this maximum rate of 200 pps.

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click Create.

3 Choose Ethernet CFM→CFM Two Way SLM. The CFM Two Way SLM Test (Create) form opens.

4 Configure the required parameters:

- Auto-Assign ID
- Name
- Description
- Administrative State
- NE Schedulable

Note 1 — The NE Schedulable parameter is enabled for the proactive CFM two-way SLM test.

Note 2 — When the NE Schedulable parameter is enabled, two additional tabs Test Parameters and Results Configuration appear in the form.

5 Click on the Select button beside the Global ID parameter to choose a global MEG. The Select Global MEG form opens.

6 Specify a search filter, if required, and click Search. A list of global MEGs appears.

7 Choose an entry and click OK. The Select Global MEG form closes, and the CFM Two Way SLM Test (Create) form displays the global MEG.

8 Click on the Select button beside the ID parameter to choose an originating MEP. The Select Originating MEP - CFM Two Way SLM Test form opens.

9 Specify a search filter, if required, and click Search. A list of MEPs appears.

10 Choose a MEP and click OK. The Select Originating MEP - CFM Two Way SLM Test form closes, and the CFM Two Way SLM Test (Create) form displays the MEP information.

11 Perform one of the following:

a Choose a MEP as the test destination.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM Two Way SLM form opens.

ii Choose an entry and click OK. The Select MEP - CFM Two Way SLM form closes, and the CFM Two Way SLM Test (Create) form refreshes.

b Choose a MIP as the test destination.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM Two Way SLM form opens.

ii Choose an entry and click OK. The Select MIP - CFM Two Way SLM form closes, and the CFM Two Way SLM Test (Create) form refreshes.

c Choose an unmanaged MEP as the test destination.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select Unmanaged MEP - Two Way SLM form opens.

ii Choose an entry and click OK. The Select Unmanaged MEP - CFM Two Way SLM form closes, and the CFM Two Way SLM Test (Create) form refreshes.

12 When the NE Schedulable parameter is enabled in step 4, go to step 15. Otherwise, go to step 13.

13 Configure the required parameters in the MEP Transmit SLM Information panel:

- Priority
- Interval (seconds)
- Timeout (seconds)
- Data Size (octets)
- Number of Test Packets

14 Go to step 17.

15 Click on the Test Parameters tab and configure the required parameters in the Execution Details panel:

- Packet Interval (milliseconds)
- Packet Timeout (milliseconds)
- Forwarding Class
- Size (octets)

16 Click on the Results Configuration tab and click on the Select button in the Card TCA Profile panel. The Select Card TCA Profile - CFM Two Way SLM Test form opens.

17 Specify a search filter, if required, and click Search. A list of card TCA profiles appear.

18 Choose an entry and click OK. The Select Card TCA Profile - CFM Two Way SLM Test form closes and the CFM Two Way SLM Test (Create) form opens.

19 Click Apply to save the changes.

20 Click on the Results tab to view the test results.

Procedure 23-8 To create and run an on-demand CFM LM test

1 Choose Tools→Service Test Manager (STM) from the 5620 SAM main menu. The Service Test Manager form opens.

2 Click Create.

3 Choose Ethernet CFM→CFM LM Test. The CFM LM Test (Create) form opens.

4 Configure the required parameters:

- Auto-Assign ID
- Name
- Description
- Administrative State

5 Deselect the NE Schedulable check box.

6 Click on the Select button beside the Global ID parameter to choose a global MEG. The Select Global MEG form opens.

7 Specify a search filter, if required, and click Search. A list of global MEGs is displayed.

8 Choose an entry and click OK. The Select Global MEG form closes, and the CFM LM Test (Create) form displays the global MEG.

9 Click on the Select button beside the ID parameter to choose an originating MEP. The Select Originating MEP - CFM LM Test form opens.

10 Specify a search filter, if required, and click Search. A list of MEPs appear.

11 Choose a MEP and click OK. The Select Originating MEP - LM Test form closes, and the CFM LM Test (Create) form displays the MEP information.

12 Perform one of the following in the MEP Transmit Information panel:

a Choose a MEP as the test destination.

i Click on the Select MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select MEP - CFM LM Test form opens.

ii Choose a MEP and click OK. The Select MEP - CFM LM Test form closes, and the CFM LM Test (Create) form refreshes.

b Choose a MIP as the test destination.

i Click on the Select MIP button beside the Target MAC Address parameter to choose the destination MIP. The Select MIP - CFM LM Test form opens.

ii Choose a MIP and click OK. The Select MIP - CFM LM Test form closes, and the CFM LM Test (Create) form opens.

c Choose an unmanaged MEP as the test destination.

i Click on the Select Unmanaged MEP button beside the Target MAC Address parameter to choose the destination MEP. The Select Unmanaged MEP - CFM LM Test form opens.

ii Choose an unmanaged MEP and click OK. The Select Unmanaged MEP - CFM LM Test form closes, and the CFM LM Test (Create) form opens.

13 Configure the required parameters in the MEP Transmit LM Information panel:

- Priority
- Interval
- Number of Test Packets

14 Click Apply to save the changes.

15 Click Execute to run the test.

16 Click on the Results tab to view the test results.

23.6 Smart SFP-RMD overview

An Ethernet demarcation point is required at the edge of a network to separate the operator domain from the end user. The demarcation point implemented as an Ethernet switch, which is known as an NID, supports a network interface and one or more customer facing ports. The NID provides Ethernet OAM functions to help the operator monitor, troubleshoot, and localize faults.

An RMD is an NID that is installed in the customer equipment and managed by the OT cards. The 5620 SAM supports the configuration of the Smart SFP-RMD on the 11QPE24 and 11QCE12X cards.

The 5620 SAM supports configuration of the following device types:

- CFM-capable 1000Base-X SFP
- EFM-capable 1000Base-X SFP
- cEDD NID
- TSoP-OC3
- TSoP-OC12

You can configure an RMD access interface using the C and X ports of the cards for device types CFM, EFM, and cEDD and using the C ports for device types TSoP-OC3 and TSoP-OC12. Only one access interface can be created per port. The accessible RMD device with a specific OUI is discovered and a management instance is created for the discovered device by specifying the device type and MAC address.

See Procedure 23-9 for more information about configuring an RMD. See Procedure 23-10 for more information about automatic configuration of an RMD.

Note — The 5620 SAM does not support automatic configuration of RMD for device types TSoP-OC3 and TSoP-OC12.

The 5620 SAM also supports the configuration of Ethernet CFM on the RMD. The supported device types are CFM and cEDD. See Procedure 23-13 for more information about configuring Ethernet CFM on RMD.

23.7 Configuring RMD

Procedure 23-9 To manually configure an RMD on a card

Before you perform the following procedure, ensure that you configure the following:

- set the Assigned Rate parameter on the Port Specifics→General tab of the Physical Port (Edit) form for the C or X port of the card for device types CFM, EFM, and cEDD
- turn up the port and set the operational state to Up
- configure the SyncE Support parameter on the Card Specifics→General tab of the Card Slot (Edit) form to Enable for the device types TSoP-OC3 and TSoP-OC12
- configure the Assigned Rate parameter for client ports on the Port Specifics→General tab of the Physical Port (Edit) form to 1GbE for the device types TSoP-OC3 TSoP-OC12
- configure the Pluggable Module Type parameter for client ports on the Port Specifics→General tab of the Physical Port (Edit) form to the following for the device types TSoP-OC3 or TSoP-OC12:
    - TSoP-OC3—SG-S-1.1 or SG-L-1.1
    - TSoP-OC12—SG-L-4.1 or SG-S-4.1

Note — After the Pluggable Module Type parameter is configured and the RMD device is configured on a specific port, the pluggable module type of the participating port cannot be changed to a module type that is not supported by the RMD device type.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→NE→Shelf→Card Slot.

3 Right-click on the Card Slot and choose Properties. The Card Slot (Edit) form opens.

4 Click on the RMD tab. The Discovery tab appears.

Configure RMD access interface

5 Click on the Access Interface tab and click Create. The RMD Access Interface (Create) form opens.

6 Configure the Interface ID parameter. Alternatively, you can select the Auto-Assign ID check box.

7 Click on the Select button to select the port to be used to manage the RMD. The Select Port form opens with the list of ports.

8 Choose a port. You can choose a port that is a member of a LAG for the EFM and cEDD device types. click OK. The Select Port form closes and the RMD Access Interface (Create) form reappears.

9 Click OK. A dialog box appears.

10 Click OK. The Card Slot (Edit) form opens. Go to step 18 if the device types that you need to configure are TSoP-OC3 or TSoP-OC12.

Assign access interface to RMD

11 Click on the Discovery tab.

12 Configure the OUI parameter.

Note — The OUI parameter is configured to 00-19-3A by default. The OUI parameter configuration is required only if the RMD has an OUI that differs from the default value.

13 To assign the RMD access interface to the RMD, click on the Select button. The Select RMD Interface form opens with a list of access interface.

14 Choose an access interface and click OK. The Select RMD Interface form closes and the Discovery tab appears. The access interface is assigned to the RMD.

15 Click on the Initiate button beside the Auto Discovery parameter to send a request to the 1830 PSS to discover the RMD attached to the RMD access interface.

16 Click OK.

17 After 10 s, click on the Discovered Devices tab. The RMD discovered by the 1830 PSS RMD discovery mechanism appears with the properties displayed.

Configure RMD

18 To manually configure the RMD, click on the Devices tab and click Create. The Remote Managed Device (Create) form opens.

19 Click on the Select button. The Select RMD Access Interface form opens with a list of RMD interface.

20 Choose an RMD interface and click OK. The Select RMD Interface form closes and the Remote Managed Device (Create) form reappears.

21 Configure the required parameters:

- Device ID
- Device Type
- Description
- MAC Address
- Forwarding Mode

Note — You can use the device type and MAC address information from the Discovered Devices tab that displays the RMD properties of the RMD discovered in step 17.

22 Click OK. The Remote Managed Device (Create) form closes and the Devices tab appears displaying the configured RMD.

23 Click Apply to save the changes.

Procedure 23-10 To automatically configure an RMD on a card

Before you perform the following procedure, ensure that:

- the Assigned Rate parameter on the Port Specifics→General tab of the Physical Port (Edit) form is configured for the C or X port of the card
- the port is turned up and the operational state is Up

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→NE→Shelf→Card Slot.

3 Right-click on the Card Slot and choose Properties. The Card Slot (Edit) form opens.

4 Click on the Ports tab. The ports are listed.

5 Choose any of the C and X ports to configure an RMD access interface.

6 Click on the Discover RMD Device button to create an RMD access interface to discover the RMD. A dialog box appears.

7 Click OK. The RMD access interface is created and the RMD is discovered.

8 Click on the RMD tab and click on the Access Interface tab to view the access interface and Discovered Devices tab to view the discovered RMD.

Note 1 — If the Auto Create Devices check box on the RMD→Discover tab of the Card Slot (Edit) form is enabled, the RMD devices are automatically created for the newly discovered devices.

Note 2 — If the Auto Create Devices check box on the RMD→Discover tab of the Card Slot (Edit) form is not enabled, the RMD device is not created. The automatic configuration of RMD is possible only for newly discovered devices and not for pre-existing discovered devices.

Procedure 23-11 To reset the RMD

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→NE→Shelf→Card Slot.

3 Right-click on the Card Slot and choose Properties. The Card Slot (Edit) form opens.

4 Click on the RMD tab. The Discovery tab appears.

5 Click on the Devices tab. The configured RMDs are listed.

6 Choose a device.

7 Click on the Reset Device button and choose one of the following options:

- Warm1
- Warm 2
- Warm 3
- Cold

A dialog box appears.

8 Click OK.

Procedure 23-12 To configure the RMD ports

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→NE→Shelf→Card Slot.

3 Right-click on the Card Slot and choose Properties. The Card Slot (Edit) form opens.

4 Click on the RMD tab. The Discovery tab appears.

5 Click on the Devices tab. The configured RMD is listed.

6 Choose the RMD and click Properties. The Remote Managed Device (Edit) form opens.

7 Click on the Ports tab. The RMD ports are listed.

8 Choose and entry and click Properties. The RMD Port (Edit) form opens.

9 Perform one of the following:

a Configure the network port (the port facing the service provider) parameters for EFM, CFM, or cEDD device types:

- Auto-Negotiation
  - Enabled
  - Fallback Enabled

b Configure the customer port (the port facing the customer equipment) parameters for cEDD device type:

- Traffic Enabled
- Duplex
- Speed (Mbps)
- Auto-Negotiation
  - Enabled
  - Fallback Enabled

Note 1 — When the device type is CFM or EFM, the Auto-Negotiation Fallback Enabled parameter cannot be modified.

Note 2 — When the device type is cEDD, the Auto-Negotiation Fallback Enabled parameter cannot be modified on a customer port.

Note 3 — When the device type is TSoP-OC3 or TSoP-OC12, the network port attributes are not applicable and are not displayed. The Traffic Enabled parameter is not applicable for customer ports. All other customer port attributes cannot be modified.

10 Click OK to save the configuration.

Procedure 23-13 To configure Ethernet CFM for an RMD

1 Perform steps 1 to 14 of Procedure 23-1 to:

- configure an MD and distribute it to an 1830 PSS
- add a global MEG to the MD

2 To associate an RMD with the MEG:

i Choose Tools→Ethernet CFM→Maintenance Domain Policies and choose an MD in the list.

ii Click Properties. The Maintenance Domain Global Policy (Edit) form opens.

iii Click on the Global Maintenance Entity Group tab and click Search. A list of global MEGs appears.

iv Choose a global MEG and click Properties. The Global Maintenance Entity Group (Edit) form opens.

v Click on the NE Maintenance Entity Group tab.

vi Click Create. The NE Maintenance Entity Group (Create) form opens.

vii Click on the Select button in the Site panel. The Select Site form opens.

viii Click Search. A list of sites is displayed.

ix Choose the 1830 PSS device where RMD is configured and click OK. The Select Site form closes, and the site information is displayed on the NE Maintenance Entity Group (Create) form.

x Click on the Select button in the Card/RMD panel. The Select Card/RMD form opens.

xi Choose Remote Managed Device (Remote Managed Device) from the Card Slot (Physical Equipment) drop-down menu.

xii Click Search. A list of supported RMDs is displayed.

xiii Choose an RMD and click OK. The Select Card - NE Maintenance Entity Group form closes, and the card information is displayed on the NE Maintenance Entity Group (Create) form.

xiv Configure the required parameters:

- When the device type is CFM, configure the CCM Interval parameter.
- When the device type is cEDD, configure:
  - CCM Interval (set to 1s)
  - MA Format (set to String)
  - MD Level (set to 0)
  - MD Format (set to String or DNS)

xv Click OK. The NE Maintenance Entity Group (Create) form closes and the The Global Maintenance Entity Group (Edit) form opens.

3 Perform one of the following to add a managed MEP to the MEG.

a From Tools→Ethernet CFM→Maintenance Domain Policies:

i Choose Tools→Ethernet CFM→Maintenance Domain Policies and choose an MD in the list.

ii Click Properties. The Maintenance Domain - Global Policy (Edit) form opens.

iii Click on the Global Maintenance Entity Group tab.

iv Choose the MEG and click Properties. The Global Maintenance Entity Group (Edit) form opens.

v Click on the Managed MEP tab.

vi Click Create. The MEP (Create) form opens.

vii Click on the Select button on the Remote Managed Device panel. The Select MEP form opens with the list of line ports displayed.

viii Choose an entry and click OK. The Select MEP form closes and the MEP (Create) form opens.

ix Click OK. The MEP (Create) form closes and the NE Maintenance Entity Group (Edit) form opens.

b From Network→NE→Shelf→Card Slot:

i Choose Network→NE→Shelf→Card Slot.

ii Right-click on the Card Slot and choose Properties. The Card Slot 11G Quad Port Pluggable GBE Mux (24 Clients) (Edit) form opens.

iii Click on the RMD tab. The Discovery tab appears.

iv Click on the Devices tab.

v Choose a device and click Properties. The Remote Managed Device (Edit) form opens.

vi Click on the Maintenance Domains tab and click Create. The Maintenance Domain - Local Policy (Create) form opens.

vii Configure the required parameters:

- MD Mgr Object ID
- Maintenance Domain ID
- Name Type
- Name
- Description
- Level

viii Click Apply.

Procedure 23-14 To configure TSoP device types

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→NE→Shelf→Card Slot.

3 Right-click on the Card Slot and choose Properties. The Card Slot (Edit) form opens.

4 Click on the RMD tab. The Discovery tab appears.

5 Click on the Devices tab. The configured RMD is listed.

6 Choose the RMD with the device type configured as TSoP-OC3 or TSoP-OC12, and click Properties. The Remote Managed Device (Edit) form opens.

7 Click on the TSoP tab. The TSoP parameters are listed.

8 Configure the Loopback Type parameter.

9 Click on the TSoP Channel tab.

10 Configure the required parameters:

- Destination MAC Address
- Encapsulation Enabled
- Encap EC ID
- Expected EC ID

11 Click Apply to save the changes.

24 — 1830 PSS IP routing

24.1 IP routing

The 1830 PSS devices support the following types of IP routing:

- OSPF version 2 according to RFC 2328 as IP routing algorithm
- IP static routing

24.2 Workflow to configure an OSPFv2 routing

OSPFv2 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. The 5620 SAM supports the configuration of the OSPFv2 routing on the 1830 PSS devices.

1 Configure a network interface on an 1830 PSS WDM or OCS devices.

See Procedures 24-1 and 24-2 for more information about configuring th network interfaces for WDM and OCS devices respectively

2 Configure a multi-area OSPFv2. The 1830 PSS devices have a default area that cannot be deleted.

See Procedures 24-3 and 24-4 for more information about configuring a multi-area OSPFv2 for WDM and OCS devices respectively.

See Procedures 24-5 and 24-6 for more information about modifying a multi-area OSPFv2 for WDM and OCS devices respectively.

See Procedures 24-7 and 24-8 for more information about deleting a multi-area OSPFv2 for WDM and OCS devices respectively.

3 Configure the OSPFv2 interface.

See Procedure 24-9 for more information about configuring an OSPFv2 interface for WDM devices.

See Procedure 24-10 for more information about modifying an OSPFv2 interface for OCS devices.

4 Configure an OSPFv2 area range. The OSPFv2 area range is used to summarize and filter out routes between OSPFv2 Areas. If an OSPFv2 area range is not specified, then all routes are sent out of the area as is. Up to three OSPFv2 area ranges can be configured per OSPFv2 area.

See Procedures 24-11 and 24-12 for more information about configuring an OSPFv2 area range for WDM and OCS devices respectively.

24.3 Procedures to configure OSPFv2 on WDM and OCS devices

Procedure 24-1 To configure a network interface on an 1830 PSS WDM device

Management and control information is carried to and from an 1830 PSS device using the following interfaces:

- IP interfaces
- network interfaces

An 1830 PSS WDM network interface can only have one associated facility object.

Perform this procedure to configure a network interface on an 1830 PSS, configure OSPF parameters, configure GCC type, and associate an ACL IP filter on the network interface.

1 Choose Routing from the navigation tree view selector.

2 Expand Network→1830 PSS→Routing Instance.

3 Right-click on the Routing Instance and choose Create Network Interface. The Select facility for the Network Interface form opens with a list of applicable cards and facility objects.

4 Choose an object from the list and click OK. The Select facility for the Network Interface form closes and the Network Interface (Create) form opens.

5 Configure the required parameters:

- Interface ID
- Auto-Assign ID
- Interface Status
- Packet Type
- MTU Size

Note — If the Packet Type parameter is configured as Non-Standard, the MTU Size parameter is set to 1473.

6 Click Apply. The form name changes to Network Interface (Edit).

7 Click on the OSPF tab.

8 Configure the required parameters:

- MD5 Authentication Enabled
- MD5 Key
- MD5 Key ID
- Hello Interval (seconds)
- Dead Interval (seconds)
- Cost Metric

9 Click on the Facility Binding tab. The associated network interface facility object appears.

10 Choose the object and click Properties. The Network Interface Facility Binding (Create) form opens.

11 Configure the Channel Type parameter if the facility object chosen in step 4 supports GCC1 or GCC2.

> **Note —** If the facility object chosen supports only GCC0, the Channel Type parameter cannot be configured.

12 Click on the ACL IP Filters tab.

13 Click Create. The IP Filter Cfg (Create) form opens.

14 Perform steps 6 to 11 of Procedure 22-4 to assign an ACL IP filter to the network interface.

> **Note —** Ensure that you have enabled ACL configuration through SNMP, created an ACL IP pattern, and created an ACL IP filter before assigning the ACL IP filter to the network interface. See Procedures 22-1, 22-2, and 22-3.

15 Click OK. A dialog box appears.

16 Click Yes. The Network Interface (Edit) form closes and the network interface object is added under the Routing Instance in the navigation tree.

Procedure 24-2 To configure a network interface on an 1830 PSS OCS device

You must configure the loopback IP address on the 1830 PSS device before you can configure the network interface.

Management and control information is carried to and from an 1830 PSS device using the following interfaces:

- IP interfaces
- network interfaces

IP interfaces include ports such as CIT and OAMP, which are configured by default. Both IP interfaces and network interfaces require the loopback address to be defined on the 1830 PSS device. See the *Alcatel-Lucent 1830 Photonic Service Switch Installation and System Turn-up Guide* for more information about defining the loopback address on an 1830 PSS device.

An 1830 PSS OCS network interface can have more than one associated facility objects.

1 Choose Routing from the navigation tree view selector.

2 Expand Network→1830 PSS OCS→Routing Instance.

3 Right-click on the Routing Instance and choose Create Network Interface. The Select facility for the Network Interface form opens with a list of applicable cards and facility objects.

4 Choose an object from the list and click OK. The Select facility for the Network Interface form closes and the Network Interface (Create) form opens.

5 Configure the required parameters.

6 Click on the Select button beside the Alarm Profile parameter. The Select alarmProfilePointer - Network Interface form opens with a list of available alarm profiles.

7 Choose a profile and click OK. The Select alarmProfilePointer - Network Interface form closes and the Network Interface (Create) form reappears.

8 Click on the Facility Binding tab. A list of associated facility objects appears.

9 Click Create. The Network Interface Facility Binding (Create) form opens.

10 Click on the Select button beside the Name parameter in the Facility pointer panel. The Select Facility pointer form opens with a list of available facility objects.

11 Choose an object and click OK. The Select Facility pointer form closes and the Network Interface Facility Binding (Create) form reappears.

12 Click OK. The Network Interface Facility Binding (Create) form closes and a dialog box appears.

13 Click OK. The facility object is listed under the Facility Binding tab in the Network Interface (Create) form.

14 Click OK. The Network Interface (Create) form closes and the network interface is listed in the navigation tree.

15 Expand the Network Interface object on the navigation tree to view the facility objects associated with the interface.

Procedure 24-3 To configure a multi-area OSPFv2 for WDM devices

The following procedure describes the steps to configure a multi-area OSPF for WDM devices.

Note — You need the 32-bit unique router ID before you can configure OSPF.

1 Choose Routing from the navigation tree view selector.

2 Choose Network→1830 PSS→Routing Instance→OSPFv2.

3 Right-click on the OSPFv2 object and choose Create Area. The Area Site (Create) form opens.

4 Configure the required parameters.

Note 1 — You can enable the DNS Opaque LSAs Distributed and Wave key Opaque LSAs Distributed parameters for only one OSPF area on the 1830 PSS WDM devices.

Note 2 — You cannot configure the Type parameter for a backbone area routing instance.

Note 3 — You can create up to three OSPF areas, in addition to the default backbone area (0.0.0.0).

5 Save your changes and close the forms.

Procedure 24-4 To configure a multi-area OSPFv2 for OCS devices

The following procedure describes the steps to configure a multi-area OSPF for OCS devices.

Note — You need the 32-bit unique router ID before you can configure OSPF.

1 Choose Routing from the navigation tree view selector.

2 Choose Network→1830 PSS OCS→Routing Instance→OSPFv2.

3 Right-click on the OSPFv2 object and choose Create Area. The Area Site (Create) form opens.

4 Configure the required parameters.

Note 1 — You can enable the DNS Opaque LSAs Distributed and Wave key Opaque LSAs Distributed parameters for only one OSPF area on the 1830 PSS WDM devices.

Note 2 — You cannot configure the Type parameter for a backbone area routing instance.

Note 3 — You can create up to three OSPF areas, in addition to the default backbone area (0.0.0.0).

5 Depending on the Type parameter value, the parameters in the Stub/NSSA tab are configurable for OCS devices.

6 Save your changes and close the forms.

Procedure 24-5 To modify a multi-area OSPFv2 for WDM devices

1 Choose Routing from the navigation tree view selector.

2 Choose Network→1830 PSS→Routing Instance→OSPFv2→Area.

3 Right-click on the Area object and choose Properties. The Area Site (Edit) form opens.

4 Modify the required parameters.

Note — You cannot modify the Type parameter for a backbone area routing instance.

5 Save the changes and close the form.

Procedure 24-6 To modify a multi-area OSPFv2 for OCS devices

1 Choose Routing from the navigation tree view selector.

2 Choose Network→1830 PSS OCS→Routing Instance→OSPFv2→Area.

3 Right-click on the Area object and choose Properties. The Area Site (Edit) form opens.

4 Modify the required parameters.

Note — You cannot modify the Type parameter for a backbone area routing instance.

5 Save the changes and close the form.

Procedure 24-7 To delete a multi-area OSPFv2 for WDM devices

1 Choose Routing from the navigation tree view selector.

2 Choose Network→1830 PSS→Routing Instance→OSPFv2→Area.

3 Right-click on the selected area and choose Delete. A dialog box appears.

4 Click Yes. The selected area is deleted.

Procedure 24-8 To delete a multi-area OSPFv2 for OCS devices

1. Choose Routing from the navigation tree view selector.
2. Choose Network→1830 PSS OCS→Routing Instance→OSPFv2→Area.
3. Right-click on the selected area and choose Delete. A dialog box appears.
4. Click Yes. The selected area is deleted.

Procedure 24-9 To configure a OSPF interface for WDM devices

The following procedure describes the steps to configure a OSPF interface for WDM devices.

1. Choose Routing from the navigation tree view selector.
2. Choose Network→1830 PSS OCS→Routing Instance→OSPFv2→Area.
3. Right-click on the Area object and choose Create Interface. The OSPF Interface (Create) form opens.
4. Select the specific interface in the Interface panel.
5. Save your changes and close the forms.

Procedure 24-10 To modify a OSPF interface for OCS devices

The following procedure describes the steps to configure a OSPF interface for WDM devices.

1. Choose Routing from the navigation tree view selector.
2. Choose Network→1830 PSS OCS→Routing Instance→OSPFv2→Area (Normal).
3. Right-click on the Interface object and choose Properties. The OSPF Interface (Edit) form opens.
4. Click on the Protocol Properties tab and configure the required parameters.
5. Save your changes and close the forms.

Procedure 24-11 To configure an OSPFv2 area range for WDM devices

1 Choose Routing from the navigation tree view selector.

2 Choose Network→1830 PSS→Routing Instance→OSPFv2→Area.

3 Right-click on an Area object and choose Create Area Range. The Area Range (Create) form opens.

4 Configure the required parameters.

5 Save your changes and close the form.

Procedure 24-12 To configure an OSPFv2 area range for OCS devices

1 Choose Routing from the navigation tree view selector.

2 Choose Network→1830 PSS OCS→Routing Instance→OSPFv2→Area.

3 Right-click on an Area object and choose Create Area Range. The Area Range (Create) form opens.

4 Configure the required parameters.

5 Save your changes and close the form.

25 — 1830 PSS service tunnels

25.1 Service tunnels overview

A service tunnel is an entity that is used to unidirectionally direct traffic from one device to another device. The service tunnel is provisioned to use a specific encapsulation method, such as GRE or MPLS, and the services are then mapped to the service tunnel.

On the Optical Transport Service (Edit) form, the Service Tunnels tab lists service tunnel objects (for example, SDPs, Ethernet rings, Ethernet tunnels, and other services) that are currently used by the service you are querying. When you click on the associated Discover Service Tunnels button, any previously discovered service tunnels on the service are removed and a manual rediscovery of the service tunnel is initiated, based on direct usage and current service configurations.

Note — The 11OPE8, 11QCE12X, and 11QPE24 cards support ERP. The ODU trails are added as tunnels for ERP. See Procedure 13-1 for more information about configuring ODU trails.

The Flow-through Services tab lists all other services that are currently using the object you are querying as a service tunnel. When you click on the associated Discover Flow-through Services button, any previously discovered flow-through services are removed and a manual rediscovery of the flow-through service is initiated, based on direct usage and current service configurations.

25.2 Ethernet (G.8032) ring protection

The 5620 SAM supports ERP for network protection of the Ethernet services using the 11OPE8, 11QCE12X, and 11QPE24 cards on the 1830 PSS-32, 1830 PSS-16, and 1830 PSS-4 devices. The 5620 SAM also supports:

- interconnection of multiple ERP rings to increase the span of the network
- ERP over LAG to increase link capacity on the ring

ERP overview

ERP switching offers ITU-T G.8032 specification compliance to achieve resiliency for carrier Ethernet networks. ERP keeps one link in the ring blocked to user traffic. You can run multiple ring sessions on the same physical ring with different blocked links in session. ERP enables load balancing on the ring when traffic patterns allow.

Ethernet rings use the G.8032 standard protocol for control, and participating nodes exchange protocol messages using Y.1731-defined OAM frames called R-APS. The R-APS frames are sent by MEPs that belong to an MA not associated with a service, and are positioned on ring paths. The frames are tagged and must be configured with a unique VID (that is, not shared with a service or other rings) when the ring port has dot1q encapsulation, and with a unique outer VID when the ring port has QinQ encapsulation. Ethernet rings are only on individual NNI ports that use QinQ encapsulation.

VPLS can use ERP. Epipes behave as two-node ERPs. All VPLSs may be protected by one Ethernet ring instance, or divided among several rings.

ERP on NNI and UNI ports

ERP can be configured on:

- UNI (1 GbE or 10 GbE) (access) ports configured using dot1q or QinQ encapsulation enabling support for Ethernet R-APS protected services on the service edge towards the customer site
- NNI (10 GbE) X (access uplink) ports configured using QinQ encapsulation enabling support for Ethernet R-APS protected services on the service within the Ethernet backbone
- NNI (1 GbE) C (access uplink) ports configured using QinQ encapsulation enabling support for Ethernet R-APS protected services on the service within the Ethernet backbone. The ports can be used to configure sub-rings interconnected with the main ring on the X ports.

ERP over LAG

LAG is used with ERP to increase link capacity on the ring. LAG ID must exist to add the endpoints for path A or B. When a sub-group is used on the LAG, only one sub group on a LAG can be configured for ERP over LAG. Both path A or B must be configured as LAGs of same signal rate, 1 GbE or 10 GbE. See Procedure 25-1 for more information about configuring ERP over LAG.

ERP sub-rings

Ethernet sub-rings provide a dual redundant way to interconnect with the main ring. The Ethernet cards support sub-rings connected to main rings and a sub-ring connected to a VPLS.

When sub-rings protect a link, the flush messages are propagated to the main ring. When main rings change topology, the flush messages are propagated around the main ring and do not continue to any sub-rings. The main rings are completely connected, but sub-rings are dependent on another ring or network for full connectivity. The topology changes need to be propagated to the other ring or network. The sub-rings offer the same capabilities as main rings in terms of control and data so that all link resources may be used.

The Ethernet cards support both the virtual channel and non-virtual channel for sub-ring control communication.

In the virtual channel mode, a dedicated VID, other than the main ring R-APS control channel is configured as a data instance on the main ring. An SHG needs to be configured in a virtual sub-ring to ensure that the sub-ring control messages from the main ring are passed only to the sub-ring control.

In the non-virtual channel mode, the sub-ring is only connected by the R-APS control channels on the sub-ring. This mode offers less redundancy in the R-APS messaging than the virtual channel mode because sub-ring R-APS messages are not propagated across the main ring. When a non-virtual link is configured, the protocol allows RPL messages over the sub-ring blocked link. See Procedure 25-2 for more information about configuring sub-rings.

Automatic Ethernet ring creation

The 5620 SAM automatically unites Ethernet ring elements in the network into Ethernet rings, and creates path objects to link endpoints within the ring. For the 5620 SAM to create an Ethernet ring, the following must exist:

- optical links between the participating ports. See Procedure 9-18 for more information about configuring optical links between ports.
- ODU trails between the participating ports. See Procedure 13-1 for more information about configuring ODU trails.
- at least two Ethernet ring elements with path endpoints. See Procedure 25-3 for more information about configuring Ethernet ring elements and Procedure 25-4 for more information about configuring an Ethernet ring element path.

Service provisioning on Ethernet (G.8032) rings

The 5620 SAM accelerates the provisioning of VPLS instances on Ethernet (G.8032) rings by automatically creating the control and data services on the rings. Services are configured on Ethernet (G.8032) rings in the same way as service tunnels. You can create Ethernet (G.8032) rings using the 5620 SAM GUI.

25.3 Ethernet ring configuration management

This section describes how to configure Ethernet ring elements, an Ethernet ring, and interconnections for Ethernet sub-rings on the Ethernet cards.

Procedure 25-1 To configure an Ethernet ring

The following are the prerequisites for configuring an Ethernet ring

- Select the L2Uplink check box on the Physical Port (Edit) form of the participating ports.
- Configure optical links between the participating ports.
- Configure ODU trails between the participating ports.
- Configure LAGs instead of ports for ERP over LAG.

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click Create and choose Ethernet Ring. The Ethernet Ring (Create) form opens.

3 Configure the required parameters:

- Mgr ID
- Auto-Assign ID
- Element ID
- Name
- Description
- Hold Time Down
- Hold Time Up (deciseconds)
- Revert Time (seconds)
- Guard Time (deciseconds)
- Compatible Version
- Auto Create Global MEG
- Maintenance Domain ID
- CCM Interval
- Run CCM On Create

Note 1 — If you enable the Auto Create Global MEG parameter, the ETH-CFM tab will display all associated Global MEGs created for this Ethernet Ring.

Note 2 — If path discovery generates Ethernet Ring paths, the Auto Create Global MEG, Maintenance Domain ID, CCM Interval, and Run CCM on Create parameters are not propagated to the per-path CFM Continuity Check tab configuration. Auto-generation of an MEG, or MEPs, or both can be configured on a per-path basis.

Alternatively, if path discovery is not operational (that is, no Ethernet Ring paths are populated into the Ethernet Ring), the General tab Path CFM Defaults parameters are propagated and an MEG, or MEPs, or both are generated upon manual creation of the Ethernet Ring paths.

4 Click Apply. The Ethernet Ring (Edit) form opens.

Configure Ethernet ring element

5 Click on the Components tab.

6 Right click on the Ring Elements object on the navigation tree and perform one of the following options:

a Create an Ethernet Ring Element

i Choose Ethernet Ring Element. The Select Network Elements form opens.

ii Choose the participating 1830 PSS devices from the list.

iii Click OK. The Select ELAN elements form opens.

iv Choose the participating cards from the list.

v Click OK. The Select ELAN elements form closes and the Ethernet Ring Element (Create) form opens.

vi Configure the required parameters:

- ID
- Description
- Administrative State
- Compatible Version
- Revert Time (seconds)
- Ring Node ID
- Sub-Ring
- Guard Time (deciseconds)

vii Click Apply. The changes are updated and the Ethernet Ring Element (Edit) form opens.

viii Close the Ethernet Ring Element (Edit) form. The Ethernet Ring (Edit) form opens with the Ethernet ring element objects on the navigation tree.

b Add an existing Ethernet Ring Element.

i The Select Element form opens.

ii Click Search and select an element.

iii Click OK. The element appears on the Components tab in Ethernet Ring form.

Configure owner and neighbor

7 Right-click on the Ethernet ring element object that you need to configure as owner and choose properties. The Ethernet Ring Element (Edit) form opens.

8 Configure the Ring Protection Link Type parameter as Owner.

9 Click OK. The Ethernet Ring Element (Edit) form closes and the Ethernet Ring (Edit) form reappears.

10 Right-click on the Ethernet ring element object that you need to configure as neighbor and choose properties. The Ethernet Ring Element (Edit) form opens.

11 Configure the Ring Protection Link Type parameter as Neighbor.

12 Click OK. The Ethernet Ring Element (Edit) form closes and the Ethernet Ring (Edit) form reappears.

Configure Ethernet ring path

13 Right-click on the Paths object on the navigation tree and choose Create Ethernet Ring Path to create a path. The Ethernet Path (Create) form opens.

Note — You must create a path for each element in the ring. Therefore each element (site) in the ring will have two endpoints (from two different paths) associated with it.

14 Configure the required parameters:

- Auto-Assign ID
- ID
- Description

15 Click on the Endpoints tab to configure the required parameters in the Endpoint A and Endpoint B panels:

- Path ID
- Ring Protection Link Type

  Configure the path of the Ethernet ring elements, configured as owner and neighbor, as the Ring Protection Link End.

  Configure all other paths as Normal.
- Administrative State
- R-APS Tag (Outer Encapsulation Value)
- R-APS Tag (Inner Encapsulation Value)

16 To configure the endpoints A and B:

i Click on the Select button in the Member Port section. The Select Member Port form opens.

ii Choose the participating ports as an endpoint.

iii Click OK. The endpoint parameters are automatically populated.

17 Click OK. The Ethernet Ring (Edit) form reappears.

18 Click Apply. A dialog box appears.

19 Click Yes. The dialog box closes and the new Path object appears on the navigation tree.

20 Repeat steps 13 to 19 to create other required paths.

Configure CFM continuity test

21 Right-click on the Path object on the navigation tree and choose Properties to create a path. The Ethernet Ring Path (Edit) form opens.

22 Click on the CFM Continuity Check tab.

23 Reconfigure the required parameters in the Global MEG Auto Creation panel, if required:

- Auto Create Global MEG
- Maintenance Domain ID
- CCM Interval
- Run CCM On Create

24 Click on the Select button. The Select CFM Test form opens.

25 Perform the following steps only if you need to choose the CFM test from the list.

i Choose the required CFM test.

ii Click OK. The Select CFM Test form closes and the Global ID and ID parameters for the selected test appear on the CFM Continuity Check tab.

26 Perform this step only if you need to create the required CFM test.

i Click Create to create the required CFM test. The Global Maintenance Entity Group (Create) form opens,.

ii Configure the required parameters:

- Auto-Assign ID
- Name
- Description
- Administrative State

iii Configure the Name Format and Name parameters in the Maintenance Entity Group panel.

Note — If you configure the Name Format parameter to icc-based, the associated name must contain 13 characters.

iv Configure the required parameters in the Initial MEG Configuration panel:

- Initial CCM Interval
- Initial MHF-Creation
- Initial MIP LTR Priority

v Click OK. The Global Maintenance Entity Group (Create) form closes, and the Select CFM Test form reappears with the new CFM test appearing in the list.

vi Choose the new CFM test.

vii Click OK. The Select CFM Test form closes and the Global ID and ID parameters for the selected test appear on the CFM Continuity Check tab.

27 Repeat steps 21 to 26 for all the configured paths.

28 Click Apply.

Turn up ring elements

29 Right-click on the Site object on the navigation tree and choose Turn Up. A dialog box appears.

30 Click Yes. The dialog box closes.

31 Repeat steps 29 to 30 for all the configured ring elements and paths.

Create control service

32 Click on the Create Control Service button. The Create Control Service form opens.

Note — See Procedure 15-1 for manual configuration of a VPLS service.

33 Click on the Select button beside the Customer field and select a customer from the Select Customer form.

34 Configure the required parameters, if required:

- Upper Ring Outer Encap
- Upper Ring Inner Encap

35 Click on the Select button beside the Control Service Template field, if required, and select a template from the Select Control Service Template form.

> **Note 1 —** Only use the Control Service Template if you need to customize the parameter fields associated with the sites or SAPs, such as the description or name.
>
> **Note 2 —** If you need to create a Control Service Template, choose Manage→Templates from the 5620 SAM main menu. Click on the Browse Example button and select the Ethernet Ring example. For more information about creating service tunnel templates, see "Managing templates" in the *5620 SAM Scripts and Templates Developer Guide*.
>
> **Note 3 —** If a template is not specified, all created objects will use their default property values.

36 Click OK. A dialog box opens.

37 Click Yes. The dialog box closes and the VPLS service (Edit) form opens.

38 Configure the Service Name parameter and click on the Apply button. The VPLS service is configured.

39 Click on the Topology view to view the topology of the Ethernet ring.

Procedure 25-2 To configure interconnect for Ethernet sub-rings

1 Configure two Ethernet rings such that the main ring is a closed ring and the sub-ring is not a closed ring. Perform Procedure 25-1 to configure the Ethernet rings.

2 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

3 Choose Ethernet Ring configured as sub-ring from the object drop-down menu and click Search.

4 Double-click on the Ethernet ring configured as the sub-ring. The Ethernet Ring (Edit) form opens.

5 Click on the Components tab.

6 Right-click on Interconnects and choose Create Ethernet Ring Interconnect. The Ethernet Ring Interconnect (Create) form opens.

7 Configure the required parameters:

- ID
- Description

8 Click on the Select button beside the ID parameter in the Element A panel. The Select Element - Ethernet Ring Interconnect form opens.

9 Choose the Ethernet ring element that you need to interconnect at the A end and click OK. The Select Element - Ethernet Ring Interconnect form closes and the Ethernet Ring Interconnect (Create) form reappears.

10 Configure the Type parameter.

11 Click on the Select button beside the Interconnected Ethernet Ring Element parameter in the Element A panel. The Select Ethernet Ring Element - Ethernet Ring Interconnect form opens.

12 Choose the Ethernet ring configured as the main ring and click OK. The Select Ethernet Ring Element - Ethernet Ring Interconnect form closes and the Ethernet Ring Interconnect (Create) form reappears.

13 Configure the required parameters, if required:

- VPLS
- Propagate Topology Change

14 Click on the Select button beside the ID parameter in the Element B panel. The Select Element - Ethernet Ring Interconnect form opens.

15 Choose the Ethernet ring element that you need to interconnect at the B end and click OK. The Select Element - Ethernet Ring Interconnect form closes and the Ethernet Ring Interconnect (Create) form reappears.

16 Configure the Type parameter.

17 Click on the Select button beside the Interconnected Ethernet Ring Element parameter in the Element B panel. The Select Ethernet Ring Element - Ethernet Ring Interconnect form opens.

18 Choose the Ethernet ring configured as the main ring and click OK. The Select Ethernet Ring Element - Ethernet Ring Interconnect form closes and the Ethernet Ring Interconnect (Create) form reappears.

19 Click OK. The Ethernet Ring Interconnect (Create) form closes. The interconnection is displayed in the navigation tree of the Ethernet Ring (Edit) form.

20 Click Apply to save the changes.

Procedure 25-3 To configure an Ethernet ring element

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Click Create.

3 Choose Ethernet Ring Element. The Select Network Elements form opens.

4 Choose the participating 1830 PSS devices from the list.

5 Click OK. The Select ELAN elements form opens.

6 Choose the participating cards from the list.

7 Click OK. The Select ELAN elements form closes and the Ethernet Ring Element (Create) form opens.

8 Configure the required parameters:

- Description
- Administrative State
- Compatible Version
- Guard Time (deciseconds)
- Revert Time (seconds)
- Ring Protection Link Type
- Ring Node ID
- Sub-Ring

9 Configure the sub-ring:

i Configure the Type parameter. The Ethernet Ring ID, VPLS, and Propagate Topology Change parameters appear if you configure the Type parameter as Virtual Link or Non Virtual Link.

ii Configure the required parameters, as required:

- Ethernet Ring ID
- VPLS
- Propagate Topology Change

10 Click Apply. The changes are updated and the Ethernet Ring Element (Edit) form opens.

11 Close the Ethernet Ring Element (Edit) form.

Procedure 25-4 To configure an Ethernet ring element path

1 Choose Manage→Service Tunnels from the 5620 SAM main menu. The Manage Service Tunnels search form opens.

2 Choose Ethernet Ring Element (Ethernet Ring) from the drop-down menu and click Search. The Ethernet ring elements are listed.

3 Choose the Ethernet ring element for which the path needs to be configured and click Properties. The Ethernet Ring Element (Edit) form opens.

4 Click on the Path Endpoints tab.

5 Click Create. The Ethernet Ring Path Endpoint (Create) form opens.

6 Configure the required parameters:

- Path ID
- Description
- Administrative State
- Path Endpoint Type

  Configure the path of the Ethernet ring elements, configured as owner and neighbor, as the Ring Protection Link End.

  Configure all other paths as Normal.

7 Click on the Port tab.

8 Click on the Select button and choose the port for the specific path (Path A or Path B).

9 Configure the required parameters:

- R-APS Tag (Outer Encapsulation Value)
- R-APS Tag (Inner Encapsulation Value)

10 Click OK. The Ethernet Ring Path Endpoint (Create) form closes and the Path Endpoints tab lists the configured path.

11 Click Apply.

12 Repeat steps 3 to 11 to configure the path A and B for all the Ethernet ring elements.

26 — 1830 PSS MC LAG group

26.1 MC LAG overview

A LAG is a group of 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 link and node-level redundancy using a switchover function.

MC LAG is an extension of the LAG concept that provides access link, card, and node level redundancy. An MC LAG configuration provides redundant L2 access connectivity that extends beyond link-layer protection by allowing two devices to share a common LAG endpoint. 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. The 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 are active at a time.

The 5620 SAM supports configuration of MC LAG groups on the following cards:

- 11OPE8
- 11QCE12X
- 11QPE24

MC LAG is supported on C ports with 1 GbE signal rate and on X ports with 10 GbE signal rate. The 5620 SAM supports configuration of the MC LAG source and the MC LAG peer at the node level and the card level. Only one MC LAG source can be configured per card. Four MC LAG peers can be configured per source.

26.2 MC LAG procedures

This section describes how to configure MC LAGs.

Procedure 26-1 To configure an MC LAG

Consider the following before you create an MC LAG group.

- Configure one or more LAGs on the participating cards. See Procedure 9-23 for more information about configuring LAGs.
- Configure VPLS service with MC LAG binding on the participating cards. See Procedure 15-1 for more information about configuring a VPLS service.

Configure MC LAG peer group

1 Choose Manage→Redundancy→Node Redundancy from the 5620 SAM main menu. The Manage Node Redundancy form opens.

2 Choose MC PSS Peer Group (Multi-Chassis) from the object drop-down menu.

3 Click Create. The MC PSS Peer Group (Create) form opens.

4 Click on the Select button beside the Name parameter in the Service Site sub-panel of the First Element panel to choose the first service site for the peer group. The Select Service Site - MC PSS Peer Group form opens.

5 Choose an NE in the list and click OK. The Select Service Site - MC Peer Group form closes, and the card slot and service site information are displayed on the MC PSS Peer Group (Create) form.

6 Configure the required parameters:

- Source ID
- Peer Name
- Description

7 Click on the Select button beside the Name parameter in the Second Element panel to choose the second service site for the peer group. The Select Service Site - MC PSS Peer Group form opens.

8 Repeat steps 5 and 6 for the Second Element panel.

9 Click Apply. The MC PSS Peer Group (Create) form refreshes with additional tabs.

Configure MC LAG group

10 Click on the Associated Groups tab.

11 Right-click on the MC LAG Group object in the navigation tree and choose Create MC PSS LAG Group. The MC PSS LAG Group (Create) form opens.

12 Configure the required parameters:

- LACP Key
- System ID
- System Priority
- Description

13 Specify the LAG for the first MC LAG site.

i Click on the Select button beside the LAG Name parameter in the First Site pane. The Select LAG - MC PSS LAG Group form opens.

ii Choose a LAG in the list and click OK. The Select LAG - MC PSS LAG Group form closes and the MC PSS LAG Group (Create) form displays the LAG information.

14 Specify the LAG for the second MC LAG site.

i Click on the Select button beside the LAG Name parameter in the Second Site panel. The Select LAG - MC PSS LAG Group form opens.

ii Choose a LAG in the list and click OK. The Select LAG - MC PSS LAG Group form closes and the MC PSS LAG Group (Create) form displays the LAG information.

15 Click OK. The MC PSS LAG Group (Create) form closes. The newly created MC LAG object is displayed below the MC LAG Group object in the navigation tree on the MC PSS Peer Group (Edit) form.

16 Repeat steps 10 to 15 to add more MC LAG groups.

17 Close the MC PSS Peer Group (Edit) form.

18 Close the Manage Node Redundancy form.

Procedure 26-2 To configure an MC LAG source on a card

Consider the following before you create an MC LAG group.

- Configure one or more LAGs on the participating card. See Procedure 9-23 for more information about configuring LAGs.
- Configure VPLS service with MC LAG binding on the participating cards. See Procedure 15-1 for more information about configuring a VPLS service.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→*NE*→Shelf→Card.

3 Right-click on the Card object and choose Properties. The Card Slot (Edit) form opens.

4 Click on the Redundancy tab. The Source tab appears.

5 Click Create. The MC Source (Create) form opens.

6 Configure the Source ID parameter.

7 Click on the Select button beside the Name parameter in the Service Site panel of service site for the peer group. The Select Service Site - MC Source form opens.

8 Choose a service in the list and click OK. The Select Service Site - MC Source form closes, and the service site information is displayed on the MC Source (Create) form.

9 Click Apply to save the changes.

Procedure 26-3 To configure an MC LAG peer on the card

Consider the following before you create an MC LAG peer:

- Configure one or more LAGs on the participating cards. See Procedure 9-23 for more information about configuring LAGs.
- Configure VPLS service with MC LAG binding on the participating cards. See Procedure 15-1 for more information about configuring a VPLS service.

Configure MC LAG peer group

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Choose Network→*NE*→Shelf→Card.

3 Right-click on the Card object and choose Properties. he Card Slot (Edit) form opens.

4 Click on the Redundancy tab. The Source tab appears.

5 Click on the MC Peer tab.

6 Click Create. The PSS MC Peer (Create) form opens.

7 Configure the required parameters:

- Peer ID
- Peer Name
- Description
- States

8 Click on the MC LAG tab. The General sub-tab appears.

9 Configure the required parameters:

- Keep-Alive Interval (deciseconds)
- Lost Connection Wait Interval
- Administrative State

10 Click on the Members sub-tab.

11 Click Create. The MC LAG (Create) form opens.

12 Configure the required parameters:

- LACP Key
- System ID
- System Priority

13 Specify the LAG for the MC LAG site.

i Click on the Select button beside the LAG Name parameter in the First Site panel. The Select LAG - MC PSS LAG Group form opens.

ii Choose a LAG in the list and click OK. The Select LAG - MC PSS LAG Group form closes and the MC PSS LAG Group (Create) form displays the LAG information.

14 Configure the required parameters:

- Remote LAG ID
- Flush Ethernet Ring Enabled

15 Click OK. The MC LAG (Create) form closes and the PSS MC Peer (Create) form reappears.

16 Click Apply. The MC LAG (Create) form closes and the PSS MC Peer (Edit) form appears with the newly created MC LAG.

17 Close the PSS MC Peer (Edit) form. The newly create MC LAG peer appears in the Card Slot (Edit) form.

Customer documentation and product support

Customer documentation

Customer Documentation Welcome Page

Technical Support

http://support.alcatel-lucent.com

Documentation feedback

documentation.feedback@alcatel-lucent.com