Alcatel-Lucent 5620

SERVICE AWARE MANAGER

NUAGE VIRTUALIZATION USER GUIDE

Alcatel·Lucent

All specifications, procedures, and information in this document are subject to change and revision at any time without notice. The information contained herein is believed to be accurate as of the date of publication. Alcatel-Lucent provides no warranty, express or implied, regarding its contents. Users are fully responsible for application or use of the documentation.

Disclaimers

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

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

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

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

Contents

Solution overview

Service management

Statistics management

Solution overview

1 — What's new?

1.1 What's new in 5620 SAM Release 13.0

This section highlights new data center management features for 5620 SAM Release 13.0 and provides pointers into the documentation for 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 features are introduced or the features introduced do not require documentation.

What's new in 5620 SAM Release 13.0 R3

Table 1-1 lists the data center management features added in 5620 SAM Release 13.0 R3 and described in 5620 SAM core customer documentation.

Table 1-1 5620 SAM Release 13.0 R3 features

Feature ID	Feature or function	Description	See
SAM-45601	V-Port to V-Port ACL and policy groups	The Data Center Manager displays policy group information for V-Ports that have an associated ACL policy group. The Virtual port redirect target tab on the V-Port properties form shows target redirect information.	Virtual port properties in Chapter 8
SAM-45964	SD-VPN Egress Shaping	The Data Center Manager displays forwarding class information for NSG gateways.	NSG management in Chapter 8
SAM-47162	Simple data center profiles	BGP profiles can be configured from the Inventory Management application. BGP profiles monitor prefix updates and either log or reject the prefix based on user-defined rules.	*5620 SAM Nuage Virtualization Solutions Guide* and Inventory Management application help tours.
SAM-53674	Persistent object deletion	Inactive persisted virtual service objects can be manually deleted from the database in the Service Navigator application	*5620 SAM Nuage Virtualization Solutions Guide*
SAM-55999	Data center profile management	The following profiles can be configured from the Profile View of the Inventory Management application: • BGP profiles • aging profiles • historical event profile • historical event partition profile	*5620 SAM Nuage Virtualization Solutions Guide* and Inventory Management application help tours.
SAM-57920	Enhanced DC historical viewer	The event information panel appears for selected events in the Historical Events tab of the Service Navigator application.	*5620 SAM Nuage Virtualization Solutions Guide*
SAM-58050	NSG lightweight discovery	You can use the Data Center Manager to see NSG V-Switches in the DC network.	NSG management in Chapter 8
SAM-62440	VSA-8 support	You can discover and manage the 7850 VSA-8 using the discovery manager.	Chapter 6

What's new in 5620 SAM Release 13.0 R1

There are no new data center management features for 5620 SAM Release 13.0 R1.

2 — 5620 SAM Nuage Virtualization overview

2.1 5620 SAM Nuage Virtualization overview

The Alcatel-Lucent 5620 Service Aware Manager (5620 SAM) Nuage Virtualization (NV) feature group provides the network management component for the Alcatel-Lucent Data Centers Service Delivery solution. The solution combines existing functionality from the 5620 SAM and the 5650 CPAM along with unique data center feature sets to provide end-to-end network management and service assurance for a data center network. This functionality allows you to:

- discover and manage a network of SROS-based NEs such as the 7850 VSG with full FCAPS EMS support
- discover and manage generic network elements with system management and MIB support
- provide IGP network infrastructure management
- monitor and manage virtual network objects with full visibility of associated network objects and services
- discover and manage data center services such as dVRS and EVPN services
- monitor service status and reachability with virtualization-aware service views and service mapping features
- manage alarms and identify the root cause or service impact of a network or service problem using historical event correlation
- proactively test service performance and monitor network status with service tests and threshold crossing alarms
- view performance, accounting, and server statistics and plot them into graphs
- provide OSS integration with external applications

2.2 5620 SAM deployment and packaging

The 5620 SAM is deployed and installed the same way as a 5620 SAM/5650 CPAM co-installation. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.

Application branding

If required, you can rebrand 5620 SAM applications for VSAP during a 5620 SAM main server installation, upgrade, or configuration operation. To rebrand the applications, you must specify an option when you open the 5620 SAM server installer, as shown in the following command example:

```
# ./ServerInstall_RHEL_SAM_R_r_revision.bin -DNUAGE=true ↵
```

where

R_r is the release identifier, in the form *MAJOR_minor*

revision is the revision identifier, such as R1, R3, or another descriptor

Nuage Virtualization features

While the Nuage Virtualization feature set is derived from the 5620 SAM and the 5650 CPAM, packaging is not the same. Some 5620 SAM capabilities which are not relevant to DC network management are excluded. For example, optical and LTE support is not included.

Features in the Nuage Virtualization feature set are offered in the following layers which reflect different sets of management capabilities.

- **EML Layer** — provides equipment management and FCAPS features for managed devices with SNMP/SFTP/FTP. Standard equipment management features for the 7850 VSG include backup and restore, statistics, alarms, and equipment configuration.
- **Infrastructure Layer** — provides infrastructure topology management and protocol management for the 7850 VSG and third-party GNEs. Standard infrastructure management features include 5650 CPAM IGP maps, path monitoring, protocol history, and associated alarms. The infrastructure layer also includes the DC Manager tool and support for V-Node discovery and management.
- **Dynamic Service Layer** — provides support for discovery, management, and assurance of virtualized services. Standard service management features include persistence of VM and service objects, service mapping to the IP underlay network, BGP VPN route analytics features, fault correlation, and event logging.
- **OSS Support** — provides support for the 5620 SAM-O interface with operational alarm and route analytic flows.

2.3 About this guide

This guide focuses on the Nuage Virtualization feature set. Where appropriate, existing 5620 SAM or 5650 CPAM features have been highlighted when they are integral to data center workflows.

This guide assumes you have followed the workflows for setup and deployment outlined in the other guides provided with this documentation suite. Some existing 5620 SAM and 5650 CPAM functionality available in the Nuage Virtualization feature set may be useful for data center network management without being highlighted in this guide. See the *5620 SAM User Guide* and the *5650 CPAM User Guide* for more information on 5620 SAM and 5650 CPAM.

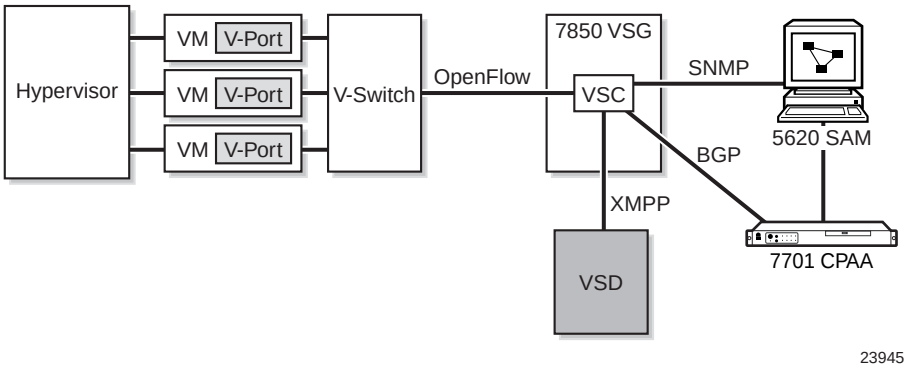
3 — Nuage data center service delivery solution

3.1 Data center service delivery solution overview

The Nuage data center service delivery solution provides end-to-end provisioning, management, and assurance for virtualized services.

Figure 3-1 shows a simplified view of the solution using a 7850 VSG setup. In a standalone VSC setup, a GNE or 7850 VSA is used as the L3 routing component.

Figure 3-1 Nuage data center service delivery solution



3.2 Virtualized Services Directory

The Nuage Virtualized Services Directory (VSD) is a policy-based system which can be used for creating virtualized services and provisioning them on the 7850 VSG. It has a web-based UI for administrator and tenant onboarding. The VSD is responsible for user management databases, policy creation, and cross-system interfaces. The VSD represents the user- or service-based outward functionality of the data center network.

The VSD does not communicate directly with the 5620 SAM. It communicates with the 7850 VSG or standalone VSC from which the 5620 SAM discovers virtualized network and service objects. The 5620 SAM integrates these objects into the IP underlay network view for event correlation and other functionality.

3.3 Distributed Virtual Routing and Switching

The Nuage distributed Virtual Routing and Switching (dVRS) service solution is implemented and monitored by the VSD. Service creation and first-level monitoring is provided by the VSD. The solution supports service objects specific to data centers, such as VxLAN encapsulation. The solution also supports dynamic data center service behavior, such as VM mobility. The solution supports interfacing with the WAN network through methods such as BGP option B and VLAN-VLAN interfaces. The service is a combined L2/L3 forwarding solution that consists of component services that are discovered and monitored by the 5620 SAM.

See Chapter 10 for more information on virtualized services.

3.4 7850 VSG

The Alcatel-Lucent 7850 Virtual Switch Gateway (7850 VSG) is the main hardware component of the data center solution. The 7850 VSG is a top-of-rack switch that provides connectivity to servers which store virtual machines (VMs). It is based on the SROS platform and includes standard Ethernet and L3 routing functionality.

The 7850 VSG includes the virtual services controller (VSC) component. The VSC is a software-defined controller for the V-Switches attached to the 7850 VSG. It includes a CLI interface and protocol capabilities to enable the 7850 VSG to function as an integrated switch. The VSC can also be managed as a standalone software VM component without a 7850 VSG. In a standalone VSC setup, a separate L3 router is deployed (either a GNE or a 7850 VSA) to function with the VSC as a two-part router.

The 7850 Virtual Switch Aggregator (7850 VSA or 7850 VSA-8) is a variant of the 7850 VSG. The 7850 VSA functions as an IP router as an end-of-rack switch. It includes the SROS feature set, like the 7850 VSG. It can be deployed with the standalone VSC in a two-part router setup.

The 5620 SAM can discover and manage the 7850 VSG, the 7850 VSA, and the standalone VSC. The VSD configures service elements on these network elements, such as virtual ports, ACL filters, and QoS policies. The 5620 SAM supports standard equipment management features for the 7850 VSG, 7850 VSA, standalone VSC, and all SROS-based NEs. See Chapter 7 for more information.

4 — 5620 SAM Nuage Virtualization platform and components

4.1 5620 SAM Nuage Virtualization component overview

The two main components of the Nuage Virtualization solution are the 5620 SAM and the 5650 CPAM. Functionality from these two components is extended with unique data centers feature sets to provide assurance-based management of a data centers network. The solution has the following components:

- 5620 SAM
- 5650 CPAM
  - 7701 CPAA

4.2 5620 SAM

The 5620 SAM provides integrated element, network, and service operations management for advanced network solutions. The main network management operations of the 5620 SAM are:

- element management with FCAPS functionality
- network infrastructure management, service provisioning, scripting, and customer management
- network and service assurance including topology views and OAM diagnostic testing
- OSS integration with external applications

In a data center context, 5620 SAM element management functionality is expanded by the 5620 SAM to discover and manage network elements specific to data centers. The 7850 VSG, 7850 VSA, and the standalone VSC can be discovered and managed by the 5620 SAM, similar to any other SROS-based network element. The virtual components, such as virtual switches and virtual ports, can be configured with statistics collection, similar to a traditional port in the 5620 SAM. Standard element management functionality in the 5620 SAM includes the following:

- network element backup and restore
- equipment configuration and status monitoring
- performance statistics collection
- threshold crossing alarms

Network infrastructure management features include support for service creation and management. In a data center context, network infrastructure management is extended to provide support for virtualized service management. Standard network infrastructure management functionality in the 5620 SAM includes the following:

- manual and scripted service provisioning
- service management
- policy-based subscriber management

Network and service assurance features include support for topology maps, alarm management, service testing and troubleshooting, and performance management. In a data center context, assurance features are extended to include topology maps for virtual network objects and virtualized services, as well as alarms unique to those objects. Standard network and service assurance functionality in the 5620 SAM includes the following:

- dynamic physical and service topology maps
- alarm filtering and correlation
- statistics collection and plotting

5620 SAM system architecture

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

See the *5620 SAM System Architecture Guide* for more information.

5620 SAM GUI

The 5620 SAM GUI allows an operator to perform device, network, policy, and service management functions. Multiple 5620 SAM GUI clients can connect to a 5620 SAM server at once.

You can customize the GUI as it is seen by the operator by creating a custom workspace. A custom workspace allows you to hide specific menu items or other GUI elements to display only what is relevant to management of your network. The 5620 SAM includes a custom workspace called DataCenter_Nuage-Operations-4LS, which hides the 5620 SAM menu items which are not relevant for data center network management. To apply the data center custom workspace, you must add the workspace to the workspace selector, and then change the workspace view.

See the *5620 SAM User Guide* for more information about the 5620 SAM GUI and workspace customization procedures.

4.3 5650 CPAM

The 5650 CPAM provides real-time IGP and BGP topology capture, inspection, visualization, and troubleshooting. It retrieves routing data from the 7701 CPAA and aggregates it for route analytics and assurance functionality.

In a data centers context, the 5650 CPAM provides the IGP topology functionality which provides visibility and mappings for virtualized services and related components. It extends its reachability event correlation functionality to virtual objects and enables historical impact and root cause analysis for associated faults. It offers BGP reachability analysis for virtualized services and stores a log of reachability information.

See the *5650 CPAM User Guide* for more information.

7701 CPAA

The 7701 CPAA is a mountable rack that provides an analysis and distributed computing platform. It is a necessary component for any 5650 CPAM deployment. The following are the main functions of the 5650 CPAM:

- listening to routing data from the routing protocols that are running on it
- providing route calculation for routes passing through the routing areas the 7701 CPAA is responsible for
- performing routing analysis and providing the results to the 5650 CPAM, so the 5650 CPAM can generate network-wide reports or alarms

5 — DC applications

5.1 5620 SAM DC application overview

The 5620 SAM provides network management functionality using web-based applications. The use of the 5620 SAM DC applications is intended mainly for inventory management, network fault monitoring, and troubleshooting purposes. The applications are external to the 5620 SAM client GUI and do not require a local client installation.

See the *5620 SAM User Guide* for more information about applications not specific to data centers, such as the Fault Management application.

Browser compatibility

The 5620 SAM DC applications are supported on the latest version of Mozilla Firefox and Google Chrome.

Note — You must configure the Browser Path parameter in your User Preferences to launch a browser from the 5620 SAM client. Choose Application→User Preferences from the 5620 SAM main menu.

User group access permissions

Access to the applications is controlled through 5620 SAM user groups. The default admin user group can access all 5620 SAM DC applications. See the *5620 SAM System Administrator Guide* for more information about how to grant access permissions for applications to a user group.

5.2 5620 SAM applications

You can use the following URL to access the launch panel, from which you can launch all supported applications.

http://*server*/login

where
***server* is the hostname or IP address of the 5620 SAM server (active or standby).**

When both the active and standby 5620 SAM servers are up, you can connect to either to launch the applications. If only one of the servers is up, you must connect to that server.

Table 5-1 describes the DC applications and lists the URLs from which you can access the individual applications.

Table 5-1 5620 SAM DC applications

Application	Direct URL
Inventory Management	http://*server*/dcinventory
Service Navigator	http://*server*/dcservicenavigator

GUI element buttons

Table 5-2 describes some of the buttons you see in the DC applications.

Table 5-2 DC application buttons

Description	Button
The Navigation button allows you to navigate to any other application.	
The Search button allows you to submit search queries on inventory lists with search fields. You can also click the Search button to refresh the contents of an inventory list.	
The Refresh button allows you to refresh all information on the screen.	

Integrated help

You can click the Help button (?) to view tours which describe GUI elements and explain workflows for each panel.

Equipment management

6 — Device commissioning and discovery

6.1 Device commissioning and discovery overview

The 5620 SAM supports the discovery and management of the 7850 VSG, 7850 VSA and standalone VSC. The discovery and provisioning of data center devices is streamlined and accelerated using discovery rules, auto-provisioning, and scripted post discovery actions.

The 5620 SAM also supports discovery of other Alcatel-Lucent devices and generic NEs. Discovery and management workflows for the 7850 VSG and its variants is similar to that of other SROS-based devices.

See the *5620 SAM User Guide* for more information on device commissioning and discovery.

See the *5650 CPAM User Guide* for more information on 7701 CPAA commissioning and discovery.

6.2 7850 VSG commissioning

The 5620 SAM supports both in-band and out-of-band management for the 7850 VSG and its variants. Before the 7850 VSG can be discovered, you must enable and configure SNMP, SSH and Telnet through the device CLI.

Commissioning a 7850 VSG or its variants for discovery by the 5620 SAM is the same as for other SROS-based devices, except for the notes below. See the *5620 SAM User Guide* for more information and workflows.

Note 1 — You must install the 5650 CPAM and configure the IGP/BGP administrative domains before discovering the 7850 VSG/VSA or standalone VSC in order to use the following functionality:

- historical event correlation
- upstream router functionality
- BGP map highlights
- Inventory Management application

Note 2 — The 7850 VSG and standalone VSC should be added to a Data Center in the 5620 SAM, otherwise the 5620 SAM raises VirtVPNBGP alarms on the associated V-Ports.

6.3 5620 SAM device discovery

The 5620 SAM discovers NEs using SNMP. During the discovery process, the 5620 SAM scans the network for devices according to user-specified IP addresses or address ranges. Device discovery and provisioning are simplified with discovery rules and post-discovery actions.

Discovery rules

You can create discovery rules by using the Discovery Manager to scan the network for multiple nodes using a specified set of discovery rules. Discovery rules use rule elements to specify which NEs or subnets are to be included in or excluded from the discovery process. You can use discovery rules to automatically apply various management policies to NEs as they are discovered. You can also assign post-discovery actions to a discovery rule to automatically execute scripts on discovered NEs.

6.4 5620 SAM automated device provisioning

You can use user-defined or system-defined control scripts to automatically provision devices after discovery. An auto-provisioning control script uses script cascading to execute a series of configuration scripts following a predefined workflow. You can assign an auto-provisioning control script as a post-discovery action assigned to a discovery rule.

Post-discovery actions

Post-discovery actions accelerate NE provisioning by automatically executing a control script upon the successful discovery of NEs in a discovery rule. Post-discovery actions are applied to a discovery rule during discovery rule creation. See the *5620 SAM User Guide* for more information about post-discovery actions.

End-to-End IP Auto-Provisioning Bundle

The End-to-End IP Auto-Provisioning Bundle is provided as one of the script bundle examples in the 5620 SAM Script Manager. You can assign the End-to-End IP Auto-Provisioning Bundle to be executed on a group of 7850 VSGs as a post-discovery action for a discovery rule.

The End-to-End IP Auto-Provisioning Bundle invokes the following component script bundles:

- Equipment Provisioning Bundle
- General IP Bundle
- OSPF Configuration Bundle
- ISIS Configuration Bundle
- MPLS Configuration Bundle
- BGP Configuration Bundle

If the auto-provisioning script bundle fails to execute upon successful discovery of the 7850 VSG, you can manually execute the control script any time after the device has been discovered. If the device has been partially configured, either due to manual configuration or a partially executed script, the script bundle will configure only what still needs to be configured.

See the *5620 SAM Scripts and Templates Developer Guide* for descriptions of component script bundles and for more information about script development and execution.

Bulk operations

You can use the 5620 SAM bulk operations function to modify a large amount of information at once. You can execute bulk changes on one or multiple target NEs in your network. See the *5620 SAM User Guide* for more information about bulk operations.

6.5 Device commissioning and discovery procedures

The following procedure describes device discovery and auto-configuration.

Procedure 6-1 To discover a network element and execute and auto-configuration script

Perform this procedure to discover a 7850 VSG or other SROS network element and execute an auto-configuration script.

Create script bundles

1. Choose Tools→Scripts from the main menu. The Scripts Manager opens.
2. Click Browse Examples. The Browse Examples of Scripts form opens.
3. In the script examples navigation tree, expand Examples→Miscellaneous→End-to-End IP Auto-Provisioning Bundle.
4. Select the script bundle example and click Create Bundle. The Script Bundle (Create from example) form opens.
5. Configure the required parameters and Click OK.
6. Repeat steps 3 to 5 to create the following script bundles:
   - Script Bundle Examples→Routing Related Bundles→General IP Configuration Bundle
   - Script Bundle Examples→Routing Related Bundles→OSPF Configuration Bundle
   - Script Bundle Examples→Routing Related Bundles→ISIS Configuration Bundle
   - Script Bundle Examples→Routing Related Bundles→BGP Configuration Bundle
   - Script Bundle Examples→Routing Related Bundles→MPLS Configuration Bundle
   - Script Bundle Examples→Miscellaneous→Equipment Provisioning Bundle
   - Script Bundle Examples→Miscellaneous→Cut-in Cut-out Bundle
7. Close the Browse Examples of Scripts form.

Create a script execution instance

8. On the Scripts Manager form, choose Script Bundle (Scripting).
9. Choose the End-to-End IP Auto-Provisioning Bundle and click Properties. The Script Bundle (Edit) form opens.
10. In the Members panel, choose Configure End-to-End IP CTL and click Properties. The Control Script (Edit) form opens.
11. Click on the Instances tab.

12 Click Create. The Instance Configuration form opens.

13 Click Add and configure the Input File information, as required.

14 Save your changes and close the forms.

Create a post-discovery action

15 Choose Administration→Discovery Manager from the main menu. The Discovery Manager form opens.

16 Click on the Post Discovery Actions tab.

17 Click Create. The Post Discovery Action (Create) form opens.

18 Configure the required parameter.

19 Click Select for the Control Script Name and choose the Configure End-to-End IP CTL script.

20 Click Select for the Control Script Instance Name and choose the Configure End-to-End IP CTL script instance you created in step 12.

21 Click OK.

Create a discovery rule

22 On the Discovery Manager form, click on the Discovery Rules tab.

23 Click Create. The Create Discovery Rule step form opens.

24 Configure the parameters in Step 1, as required, and click Next.

25 Click Create to create a rule element. The Topology Discovery Rule Element form opens.

26 Configure the parameters and click OK to add a rule element to the discovery rule. Repeat this step to add multiple rule elements, as required.

27 Configure the options in the other steps of the step form, as required. See the *5620 SAM User Guide* for more information on these steps.

28 On the Add Post Discovery Action step, select the post-discovery action you created in step 16.

29 Click Finish to create the discovery rule.

30 Click Apply on the Discovery Manager form to save changes.

Execute the discovery rule

31 On the Discovery Rules tab, select the discovery rule you created and click Rescan. The 5620 SAM scans the IP addresses specified in the discovery rule elements and discovers them into the network. The network elements are automatically configured with the specified script bundles.

7 — Equipment management

7.1 Equipment management overview

The 5620 SAM provides standard FCAPS support for the 7850 VSG, 7850 VSA, standalone VSC, and other managed network elements. Equipment management functionality such as alarms and inventory is expanded to include virtual network components.

Standard FCAPS support provided for data center network elements includes the following:

- network element backup and restore
- equipment configuration and status monitoring
- fault management
- SNMP performance statistics collection
- threshold crossing alarms
- user security

Workflows for equipment management for the 7850 VSG and its variants is the same as for any other SROS-based network element. See the *5620 SAM User Guide* for more information on equipment management.

7.2 High availability virtual chassis

The 5620 SAM supports HA virtual chassis management. A virtual chassis consists of two Release 2.1 7850 VSG or 7850 VSA NEs operating as a logical entity. Virtual chassis are useful for providing twice as much switching capacity. They also provide redundancy with an HA CPM process and two distinct switching devices. The two NEs in the virtual chassis are managed with a single IP address. The 5620 SAM displays a virtual chassis as a single network element with each 7850 VSG represented as a card slot.

Note — The 7850 VSG NEs in virtual chassis are linked using VFL ports. The VFL ports should not be shut down with the 5620 SAM. Tagging VFL ports and blocking VFL port shutdown is targeted for a future release. If you attempt to shut down a VFL port, the 5620 SAM raises an exception to prevent it.

Network infrastructure management

8 — Network management

9 — Network monitoring and troubleshooting

8 — Network management

8.1 Network management overview

The 5620 SAM provides management and assurance for the data centers network infrastructure. Support for routing protocols, physical and IP maps, and other related features serve to help you visualize and troubleshoot the network underlay.

In addition to preexisting 5620 SAM functionality, the Nuage Virtualization solution includes new infrastructure management features unique to data centers management to improve visibility and correlation for virtual network components. These features include the following:

- Data Center Manager
- Cloud Network navigation tree
- Virtual Node (V-Node) management

The purpose of Nuage Virtualization infrastructure management features is to improve operator visibility of the virtual components. Each new data center management feature is equipped with search functionality and lists associations with related virtual and physical network components.

8.2 Data Center Manager

The Data Center Manager is a central display for all virtual objects in the data center network. The Data Center Manager provides a view of associations between the VSC, V-Node, V-Switch, and V-Port. The filter table allows you to search for specific VMs based on their VM UUID or associations to a specific V-Node. You can navigate from the Data Center Manager to detailed properties forms of any managed virtual object.

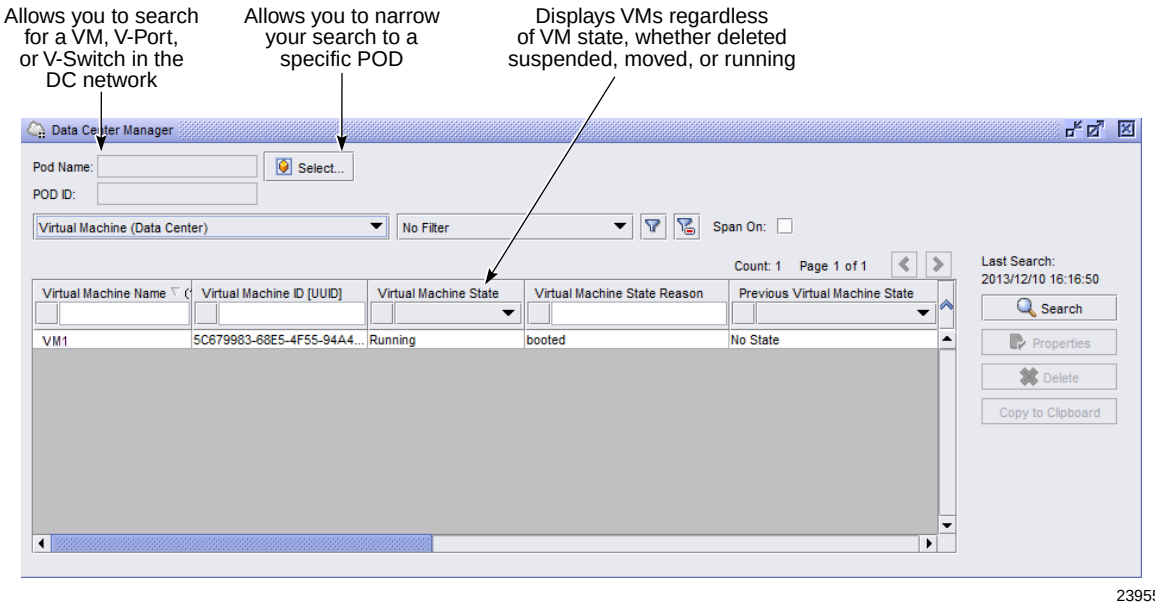
The Data Center Manager allows you to search for VMs network-wide. The filter table allows you to specify VMs based on their Site ID, VM UUID, or VSD enterprise information.

The Data Center Manager displays virtual objects in the network regardless of state. For example, a VM which has been deleted or moved would still display in the Data Center Manager with the current and previous state listed.

You can access the Data Center Manager by choosing Application→Data Center Manager.

Figure 8-1 shows the Data Center Manager form.

Figure 8-1 Data Center Manager



23955

8.3 Virtual object persistence

The 5620 SAM supports persistence for VMs, V-Ports, V-Switches, and virtualized service objects. Persistence allows the 5620 SAM to retain knowledge that a component, such as a VM, was attached to the underlay at a particular time and place regardless of its current state within the compute. Operations can easily understand transients or history as demonstrated by how the 5620 SAM has tracked the current and last known state for the service object along with complete logging of events in the event log. See Chapter 11 for more information about the event log.

The period of time that a persisted object is retained in the 5620 SAM database is defined by ageout constraint policies. When the age of an object reaches the ageout value, the 5620 SAM deletes the object from the database. See Procedure 8-5 for information on configuring ageout constraint policies for virtual network objects.

Table 8-1 lists the ageout times defined by the default ageout constraint policies.

Table 8-1 Default ageout times

Persisted object	Default ageout time (hours)
VM	168
V-Port	168
GW V-Port	168
V-Switch	720
VRSG V-Switch	720
VSG V-Switch	720

(1 of 2)

Persisted object	Default ageout time (hours)
VPLS V-Site	168
VPRN V-Site	168

(2 of 2)

8.4 Virtual object properties forms

Virtual object properties forms display information which helps to identify associated objects. These relationships provide simplified navigation to downstream routers and associated service objects. You can access properties forms for associated virtual objects is from the V-Node properties form. You can also query the entire data center network for a specific virtual component using the Data Center Manager or the Cloud Network navigation tree.

Virtual machine properties

The VM properties form can be accessed by querying the Data Center Manager or the Cloud Network navigation tree.

The form displays the following information:

- VM UUID — unique identifier string that remains constant through VM moves
- Current and previous VM state — current administrative state and last known persisted state
- User name and enterprise — associated customer information
- V-Switch — ID and site address of the associated V-Switch
- V-Port — navigation to the associated V-Port

Virtual port properties

The V-Port properties form can be accessed from the properties form of the associated VM. It is also available from the switch view of the V-Site on an associated virtualized service. V-Port properties are read-only, but you can assign ACL filters and TCAs to a V-Port like any other physical port. The V-Port properties form provides navigation to the virtual sites of associated virtualized services.

The form displays the following information:

- Site ID — IP address and administrative state of the associated 7850 VSG or standalone VSC
- Port Type — shows whether them V-Port is a VM, host, or bridge V-Port.
- MAC address
- Floating IP address — distributed NAT IP address for the V-Port, if applicable
- VM UUID — identifier for the associated VM
- VPLS service — associated EVPN service
- VPRN service — associated dVRS service
- Network domain — domain, zone, and network name for the associated customer on VSD

- QoS panel — displays information on QoS forwarding classes and DSCP, and of traffic rates
- Virtual Port Multicast Channel Map tab — associated VM multicast groups
- Egress ACL and Ingress ACL tabs — associated ACLs
- Virtual port redirect target tab — redirect target policy information
- Ingress Advance Forward tab— advance forward properties form ingress ACLs
- Virtual Port DSCP To FC Mapping tab — associated DSCP mapping table

Multicast channel maps

Multicast channel maps define a range of addresses of multicast groups available to the VM. These maps generate a list of multicast groups which are available to be joined. A multicast channel map can define multiple ranges of multicast groups, but the ranges will never overlap. A multicast channel map is distributed to each VM in an enterprise.

Multicast channel maps are defined in VSP and discovered as read-only objects by the 5620 SAM.

Egress and ingress ACL

The Egress ACL and Ingress ACL tabs list the ACLs for the V-Port. DSCP bits can be included as part of the matching criteria. Some entries can be reflexive, meaning that flow rules are created in both directions.

If the V-port is associated with a policy group, the Policy Group Tag displays the group.

Virtual port redirect target

The Virtual port redirect target tab displays redirect target policy information for the Vport or gateway port (excluding VSGs). If redirection is enabled on the port, the redirection trigger shows the condition that results in redirection.

DSCP mapping tables

DSCP mapping tables define mappings between DSCP remarkings and QoS forwarding classes. These tables are used by QoS policies to assign forwarding classes to customer traffic.

DSCP mapping tables are defined in VSP and discovered as read-only objects by the 5620 SAM.

Virtual switch properties

The V-Switch properties form can be accessed from the V-Site form of an associated virtual service. It is also available from the properties form of the associated virtual services controller.

You can also view V-Switch properties for VTEP nodes by selecting VTEP Virtual Switch (Data Center) from the DC Manager drop-down menu.

The form displays the following information:

- Personality — Indicates whether the VM is operating as a software gateway for a standalone VSC or 7850 Virtual Switch Gateway. It also indicates if it is a VTEP NE.
- OpenFlow information
- Underlay routers

You can click the Discover Underlay Routers button to refresh the list of underlay routers.

Virtual services controller properties

The VSC properties form can be accessed from the virtual site of an associated virtualized service properties form. The same tabs are also available from the NE properties form of the 7850 VSG or standalone VSC.

The form displays the following information:

- VSD and XMPP server information — address of the associated VSD client and XMPP communication
- OpenFlow — read/write access for OpenFlow communication, as well as peer access filters
- V-Switches — filterable list of associated V-Switches

8.5 Data center management

The 5620 SAM provides support for management of multiple data centers. You can create a data center object from the Data Center Manager or the Cloud Network navigation tree. You can create up to 16 data centers. You cannot delete a data center if it currently has any network elements.

Before you can discover network elements in the new data center, you must perform the following:

- discover and manage the 7701 CPAA
- create and configure the administrative domain

If you discover a network element from the new data center before performing the above tasks, you will need to unmanage and remanage the network element.

IP addresses across separate data centers can overlap, but duplicate IP addresses within a single data center should not occur. If the 5620 SAM detects a duplicate V-Switch IP address due to a misconfiguration, it raises a critical alarm.

You can move network elements from one data center to another. When the last network element in a data center is moved to another data center, the administrative domain association is cleared from the previous data center.

The 5620 SAM creates the first data center object automatically. Procedure 8-1 explains how to create additional data centers.

8.6 Virtualization control management

The 5620 SAM provides support for visibility and management the virtual node (V-Node). The V-Node is a virtual network component that is unique to the 7850 VSG and standalone VSC. It is created by the 7850 VSG to expose the virtual switch and related components to the VSC as a virtual line card. The V-Node is a management entity that encapsulates the virtual routing components from the associated VSC and maps them hierarchically to related virtual machines and virtual services. The purpose of the V-Node is to expose a simplified view of associations from the perspective of the VSC, resulting in easier mapping and correlation.

The 5620 SAM supports the following for V-Node management:

- read-write access for OpenFlow and XMPP interfaces
- automatic discovery of VSC associations into the V-Node, such as virtual switches, virtual ports, and virtual machines
- filterable and searchable display of all virtual associations through the Data Center Manager
- correlation of VSC faults to related virtual objects, including persisted objects

The V-Node is useful to 5620 SAM for service discovery and event correlation. The V-Node discovers virtual services through an OpenFlow interface between the VSC and the V-Switch. Then the 5620 SAM discovers the service from the V-Node using SNMP. The V-Node is not the only mechanism through which the 5620 SAM discovers virtual services. See Chapter 10 for more information of virtual service discovery.

The V-Node exposes service relationships to the 5620 SAM, allowing a partial view of the data plane when combined with 5650 CPAM route analytics and NMS deduction. The V-Node displays the related V-Switch and VMs. 5620 SAM deduction also helps the V-Node deduce upstream IP transport, mapping to the routers used to transport traffic for the V-Switch.

Virtual Node in the 5620 SAM

The 5620 SAM displays the V-Node if virtual switch information is configured on the discovered 7850 VSG or standalone VSC. The V-Node properties form provides a filterable and searchable interface for virtual associations for the VSC, including software gateways. You can access the form from the General tab on the properties form of the associated 7850 VSG. You can also access the form from the Data Center Manager form. The Data Center Manager allows you to view all V-Nodes in the network, and filter or search for them based on IP address or other properties.

The V-Node properties form displays a general which includes information on operational state and the associated VSC. The Virtual Node IP is the same as the IP address for the associated VSC. The Virtual Services Controller, Virtual Switches, Virtual Machines, and Virtual Ports tabs list associated virtual components in a filterable and searchable interface.

8.7 Software gateways

The 5620 SAM supports software gateways as a standard attachment for virtualized L2 services. A software gateway is represented as a VM operating as a service gateway for a virtualized service. The DC Manager exposes the VM mode as a V-Switch personality.

You can view software gateways in your network by choosing VRSG Virtual Switch or VSG Virtual Switch from the DC Manager drop-down list. Software gateways are also viewable from the DC applications. A V-Switch with VRSG personality is a operating a software gateway from a standalone VSC. A V-Switch with a VSG personality is operating as a software gateway from a 7850 VSG.

Port profiles

Basic configuration of a software gateway is done using port profiles. Port profiles define the following:

- VLAN ranges that can be used locally for manually configured services
- provisioning modes that define how VLANs within the range are processed

Note — In Nuage 2.1, the only provisioning mode supported is push.

You can assign port profiles to ports or LAGs configured on a 7850 VSG or 7850 VSA. The port or LAG must be configured with Dot1q encapsulation. You can view and create port profiles by choosing Policies→Data Center from the 5620 SAM main menu. You can assign port profiles to ports or LAGs from their respective properties forms.

See Procedure 8-6 for more information or creating and distributing port profiles.

8.8 NSG management

The 5620 SAM supports discovery of the Network Services Gateway () virtual switch from the VSP. The NSG is the network-forwarding plane for network services at central and remote locations. With an NSG at every enterprise site, the VNS solution can create overlay VPNs to interconnect customer sites.

You can use the Data Center Manager to see NSG V-Switches in the DC network. Select NSG Virtual Switch (Data Center) from the DC Manager drop-down menu. The DC Manager lists the same information that it does for all V-Switches, except it also includes the Data Path ID and gateway QoS queue information.

The Data Path ID is used as the main ID for the NSG instead of the V-Switch IP. The reason for this is that a rebooted NSG V-Switch would have a new V-Switch IP, whereas the Data Path ID would remain unchanged.

The Gateway QoS Queue tab displays forwarding class information for the gateway. You can view this information from the Data Center Manager, but configuration is performed from the VSP.

8.9 VRS redundancy

The standalone VSC supports a VRS redundancy configuration for control of a V-Switch. The 5620 SAM represents the redundancy configuration by creating a virtual switch session for each VSC/V-Switch association and mapping primary and secondary associations to a virtual switch session group.

The virtual switch session group allows you to view the status and associations of VSCs and V-Switches in the network, as well as any aggregated or related alarms. The 5620 SAM automatically creates a virtual switch session group when it discovers two virtual switch sessions which belong to the same 5650 CPAM administrative domain and which target the same V-Switch instance. Each group can have only one primary virtual switch session.

You can view a list of all virtual switch session groups from the data center object properties form, which is accessible from the Data Center Manager. You can view the virtual switch session groups for a specific VSC from the V-Node properties form. Each of these forms has a Virtual Switch Session Group tab which allows you to navigate to the session group properties form.

A VSC can act in the primary or secondary role in a redundancy setup, and can be associated to more than one virtual switch session group. If you are managing more than one data center with the 5620 SAM, you should ensure that the primary and secondary VSC are in the same data center.

8.10 Workflow for VSC redundancy setup

This workflow explains the high-level steps required to configure VSC redundancy.

1. Discover the 7701 CPAA to be associated with the redundancy setup.
2. Create an IGP and BGP administrative domain. See the *5650 CPAM User Guide* for more information on administrative domains.
3. Associate the 7701 CPAA with the administrative domains.
4. Discover all other NEs to be associated with the redundancy setup.
5. Add the discovered standalone VSCs to a data center.

   The 5620 SAM automatically creates the virtual switch session group when it discovers the two VSCs targeting the same V-Switch instance.

8.11 Network management procedures

This section explains data center network management workflows.

Procedure 8-1 To configure a data center

This procedure explains how to create a data center from the Data Center Manager or the Cloud Network navigation tree.

Open the data center creation form

1 Perform one of the following:

   a Use the Cloud Network navigation tree.

      i Choose Cloud Network from the navigation tree view selector. The Cloud Network navigation tree is displayed.

      ii Right-click on the Cloud Network in the navigation tree and choose Create Data Center. The Data Center (Create) form opens.

   b Use the Data Center Manager.

      i Open the Data Center Manager form and select Data Center (Data Center).

      ii Click Create. The Data Center (Create) form opens.

Configure general parameters and contact information

2 Configure the parameters on the General tab, as required.

   The General tab displays general identification information for the data center, such as name, description, and location.

3 Assign a contact information profile.

   The Contact Information tab lists the contact information profiles assigned to the data center. Contact information profiles list the name, phone number, email, and other information related to the associated contact. You can assign an existing contact information profile to the data center, or create a new one.

4 Click Apply to save your changes.

Assign sites to the data center

5 Click on the Network Elements tab.

6 Click on Assign Sites. The Assign filter form opens.

   The Assign Filter form allows you to filter all available network elements based on designated criteria. You can filter on more than one parameter at once. If you assign no filter criteria, all available network elements are listed.

7 Click OK to view the filtered list of network elements.

8 Select network elements from the Unassigned Sites or Assigned Sites panel and use the arrows buttons to move them.

9 Save your changes and close the forms.

Procedure 8-2 To search the data center network using the Cloud Network navigation tree

This procedure explains how to search for data center network objects using the Cloud Network navigation tree search functionality. Similar functionality exists for other navigation tree views, such as the Equipment view. See the *5620 SAM User Guide* for more information on searching those navigation tree views.

Navigate to the Cloud Network navigation tree and open the search panel

1 Choose Cloud Network from the navigation tree view selector. The Cloud Network navigation tree is displayed.

2 Enter Ctrl+F or click Find to expand the search panel.

Search for a data center network object

3 Configure search criteria for the object:

- Search for a VM using the VM UUID.
- Search for a V-Port using the IP or MAC address.
- Search for a network element using the site ID, site name, or management IP address.
- Search for a physical component using the shelf, card slot, daughter card slot, or port number.

4 Click Find to execute the search.

The first object matching the search criteria is highlighted and expanded in the navigation tree.

5 Use the Next and Previous arrow buttons to find additional matching objects.

Procedure 8-3 To configure OpenFlow on a VSC

Perform this procedure to configure OpenFlow parameters on a VSC, if required. You can configure hold times and configure the default network QoS policy. You can also assign peer access filters.

Navigate to the VSC properties form

1 To open the VSC properties form, perform one of the following:

a Click on the Data Centers Components tab on the NE properties form of the associated 7850 VSG or standalone VSC.

b Click Properties for the Virtual Services Controller on an associated Virtual Site properties form.

See Procedure 8-4 for information on navigating from a VM or V-Port to an associated virtual site.

Configure OpenFlow properties

2 Configure authentication, hold time, and QoS policy parameters on the General tab.

3 Assign one or more peer access filters for OpenFlow peers on the Peer Access Filter tab.

4 Save your changes and close the form.

Procedure 8-4 To navigate from a VM or V-Port to associated virtualized services or advertising routers

This procedure demonstrates how to use the Data Center Manager to search for a VM or V-Port and navigate to the associated virtualized services and view underlay routers.

1 Open the Data Center Manager form and select Virtual Machine (Data Center).

2 Search for the VM by using the filter criteria specify a VM UUID or Site ID.

3 Select the VM and click Properties. The Virtual Machine properties form opens.

4 Navigate to the associated V-Port properties form by selecting the V-Port and clicking Properties. The Virtual Port properties form opens.

5 To navigate to an associated virtual site, perform one of the following steps.

   a To navigate to an associated EVPN virtual site, click Properties in the VPLS Service panel. The Virtual Site VPLS properties form opens.

   b To navigate to an associated dVRS virtual site, click Properties in the VPRN Service panel. The Virtual Site VPRN properties form opens.

6 From the Virtual Site properties form, you can navigate to the associated service, network element, or V-Switch by clicking the appropriate Properties button.

   The Upstream panel provides tabs which list advertising routers and the controller view of the service site.

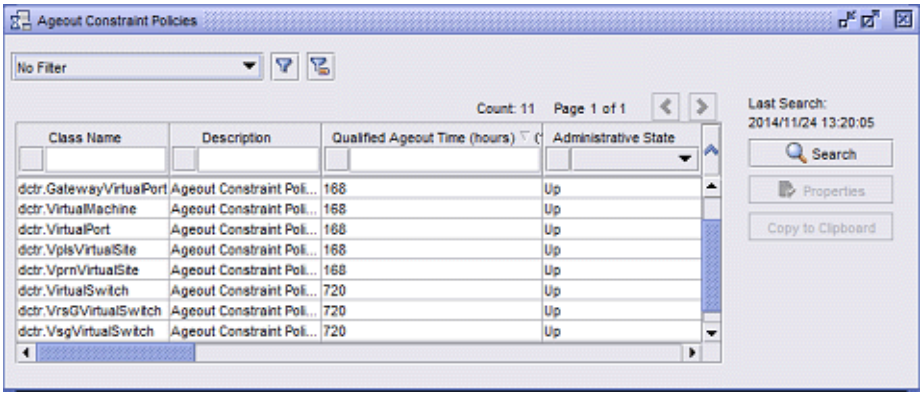
Procedure 8-5 To configure an ageout constraint policy

This procedure demonstrates how to configure an ageout constraint policy to set the period of time that the 5620 SAM retains a persisted object in the database. Default ageout constraint policies are already defined in the 5620 SAM and you cannot create new policies.

1 Choose Administration→Constraint Policies→Ageout Constraint Policies from the 5620 SAM main menu. The Ageout Constraint Policies form opens.

The Ageout Constraint Policies form lists the default policies for all persisted network objects. You can configure a default policy, but you cannot create a new one. Figure 8-2 shows the Ageout Constraint Policies form.

Figure 8-2 Ageout Constraint Policies form

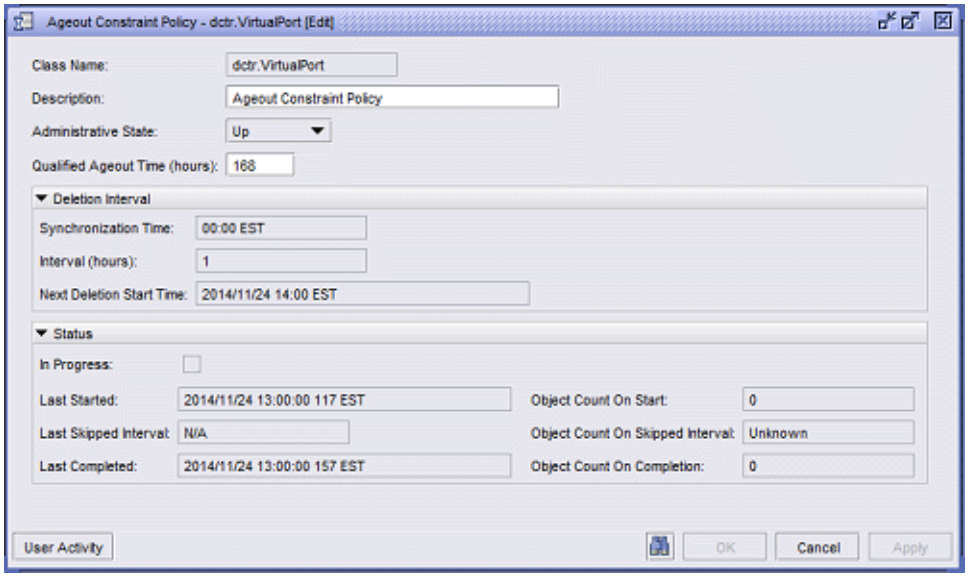


2 Select a policy and click Properties. The Ageout Constraint Policy form opens.

3 Configure the Qualified Ageout Time (hours) parameter.

The Status panel shows information on the latest ageout event. Figure 8-3 shows the Ageout Constraint Policy properties form.

Figure 8-3 Ageout Constraint Policy properties form



4 Save your changes and close the forms.

Procedure 8-6 To configure a port policy

Perform this procedure to define a VLAN range in a port policy and assign it to a 7850 VSG port or LAG.

Create the port policy

1 Choose Policies→Data Center→ from the 5620 SAM main menu. The Data Center Port Profile Policies form opens.

2 Click Create. The Port Profile (Create) form opens.

3 Configure the required parameters and click Apply. The form updates.

4 Click on the VLAN Range tab and click Create. The VLAN Range (Create) form opens.

5 Configure the required parameters and click OK.

Distribute the port policy

6 Perform one of the following to distribute the port policy:

a Distribute the policy to 7850 VSG ports, as required:

i Click OK to save the policy and close the form.

ii On the equipment tree, expand Network→NE→Shelf→Card Slot→Daughter Card Slot.

iii Right-click on a port and choose Properties. The Physical Port (Edit) form opens.

iv Select a profile in the Port Profile panel.

v Save your changes and close the form.

b Distribute the policy to 7850 VSG LAGs, as required:

i Click OK to save the policy and close the form.

ii On the equipment tree, expand Network→NE→Logical Groups→LAGs.

iii Right-click on a LAG and choose Properties. The LAG (Edit) form opens.

iv Select a profile in the Port Profile panel.

v Save your changes and close the form.

9 — Network monitoring and troubleshooting

9.1 Network monitoring and troubleshooting overview

The infrastructure layer of the 5620 SAM includes network monitoring and troubleshooting features to provide advanced visibility and fault management for the DC network. Using the DC manager, you can quickly find the path to the associated VSC for any VM or V-Switch in the network. You can then use 5650 CPAM topology functionality to graphically highlight the path and assign IP path monitors. Retention of historical faults and alarms allows you monitor historical changes on a path between a router and a virtual component.

9.2 5650 CPAM IGP topology maps

You can use 5650 CPAM IGP topology features to map and monitor data center network infrastructure. Topology maps display real-time network topology information for a designated IGP administrative domain. They provide a color-coded interface from which you can see a visual representation of routers, paths, and virtual objects within the specified IGP administrative domain. The topology view provides quick navigation to properties forms, telnet sessions, and feature configuration from within the IGP administrative domain.

The Nuage Virtualization solution supports all functionality of 5650 CPAM IGP topology maps excluding MPLS features. See the *5650 CPAM User Guide* for more information about topology management. The rest of this section will elaborate on the topology features which are most relevant to data centers network management.

Map highlighting

5650 CPAM map highlighting can be used to highlight L2/L3 services, composite services, service tunnels, SPF and CSPF routes, and OAM diagnostics results on IGP maps.

In a data centers network, map highlighting is most useful for mapping paths from a VM or V-Switch to either an associated controller or a PE router. By performing a SPF highlight from a virtual object to a PE router, you can create a highlighted mapping between the virtual object to the network underlay.

IP path monitors

5650 CPAM IP path monitors can be used to monitor the route between any two routers seen by the 5620 SAM. When a network topology changes, such as a link metric or state change, the system evaluates whether the routes of any registered path are affected. If this is the case, new routes are recorded and the 5650 CPAM is informed. If there is no route for a monitored path as a result of a topology change, a record is logged. If there is a change in the SPF calculation based on a topology change, the change is recorded. You can use map highlighting to highlight current versus historical paths, including their respective costs.

IP path monitors help with data center network management by maintaining a historical log of changes to the control path between a VSC and an associated VM or V-Switch. The monitors can also find historical faults or alarms raised on the path, which can be correlated to affected objects. IP path monitors can also monitor paths from virtual objects to routers in the network underlay.

Topology checkpoints

Applying a checkpoint to an object creates a snapshot of a real topology object at a specific time. When you apply a checkpoint to a real network object, all of the properties of the real object at checkpoint time—for example, metric and bandwidth on IGP links—are copied to the checkpointed object. A checkpointed object is displayed in the same manner as the real topology object, and shares the same OSS class name.

After you have set up the network and the network is operational, you can apply a checkpoint to the network to create a snapshot of the current state—which can include routers, links, metric configuration, or bandwidth usage—and compare it with checkpoints collected at different times. In addition, you can compare the results on an IGP history map.

9.3 Operational groups

The 5620 SAM supports operational groups to associate multiple service endpoints (such as SAPs and SDPs) on the same or different service instances. The operational group can be used to monitor the status of its member components and perform actions based on operational state changes. The status of the operational group is derived from user-defined thresholds of the number of operational member components.

The Nuage Virtualization feature set extends the operational group functionality to include physical ports and LAGs on the 7850 VSG and 7850 VSA. A physical port can be assigned as a member or a monitor of an operational group.

You can create an operational group from an NE properties form and assign it to a 7850 VSG physical port or LAG from the object properties form.

9.4 Network monitoring and troubleshooting procedures

The procedures in this section explain how to use 5620 SAM assurance features to monitor and troubleshoot network infrastructure in the data center network.

Procedure 9-1 To map the control path from a VSC to an associated VM

This procedure demonstrates how to use an 5650 CPAM IGP topology map to highlight a control path between a VSC and an associated VM. Perform this procedure to assess reachability between a VSC and associated V-Switches.

1. Choose Tools→Route Analysis→IGP Topology from the main menu. The IGP topology map opens.
2. Right-click on the map and choose Highlight→Paths→IP→SPF. The Find Object form opens.
3. Enter the VSC site address as the First IP.

4 Enter the V-Switch site address as the Second IP.

5 Click OK. The control path between the VSC and the V-Switch is highlighted on the IGP topology map.

Procedure 9-2 To map the path from an NE to an associated virtual component

This procedure demonstrates how to use a 5650 CPAM IGP topology map to highlight a path between an NE and an associated virtual component, such as a VM, V-Switch, or VSC.

1 Choose Tools→Route Analysis→IGP Topology from the main menu. The IGP topology map opens.

2 Right-click on the map and choose Highlight→Paths→IP→SPF. The Find Object form opens.

3 Enter the NE site address as the First IP.

4 Enter the V-Switch or VSC site address as the Second IP.

5 Click OK. The path between the NE and the virtual network component is highlighted on the IGP topology map.

Procedure 9-3 To configure an operational group

Perform this procedure to configure an operational group and assign physical ports or LAGs.

Configure an operational group

1 On the equipment tree, right click on a 7850 VSG/VSA and choose Properties. The Network Element (Edit) form opens.

2 Click on the Globals tab, then on the Service tab, and then on the Operational Groups tab.

3 Click Create. The Operational Groups (Create) form opens.

4 Configure the required parameters to define operational group behavior.

The Hold Time parameters specify how long to wait before notifying group monitors that operational status has transitioned from to up or down. The Threshold parameter specifies the minimum number of active members for the group to be considered operationally up.

5 Save your changes and close the form.

Add ports or LAGs to the operational group

6 Add ports to the operational group, as required.

i On the equipment tree, expand NE→Shelf→Card Slot→Daughter Card Slot→Port.

ii Right-click on a port and choose Properties. The Physical Port (Edit) form opens.

iii Select an operational group in the OperGroup and ServiceProfile panel.

You can assign the port to be a member or a monitor of an operational group.

iv Save your changes and close the forms.

7 Add LAGs to the operational group, as required.

i On the equipment tree, expand NE→Logical Groups→LAGs.

ii Right-click on a LAG and choose Properties. The LAG (Edit) form opens.

iii Select an operational group in the OperGroup and ServiceProfile panel.

iv Save your changes and close the forms.

Service management

10 — Virtualized services

10.1 Virtualized services overview

The 5620 SAM provides support for virtualized services. Management and assurance functionality for services are extended to accommodate the unique requirements for virtualized services. As the dVRS service solution is designed to allow for complete VM mobility, 5620 SAM service management is suited to manage a dynamic service. In addition to the core service management and assurance functionality available from the 5620 SAM and 5650 CPAM, the following functionality is added to the 5620 SAM for virtualized services:

- Automatic discovery of dVRS, EVPN, and VPRN services from the 7850 VSG or standalone VSC and creation of services elements.
- Comprehensive connectivity log for virtual components to provide a historical record of state changes in VMs and V-Ports.
- Historical event correlation to isolate the root cause of a problem and the impacts to service.

See the *5620 SAM User Guide* for more information on service management. See the *5650 CPAM User Guide* for more information on service troubleshooting.

See Chapter 11 for more information and workflows on service management and troubleshooting specific to data centers.

10.2 Distributed virtual routing and switching overview

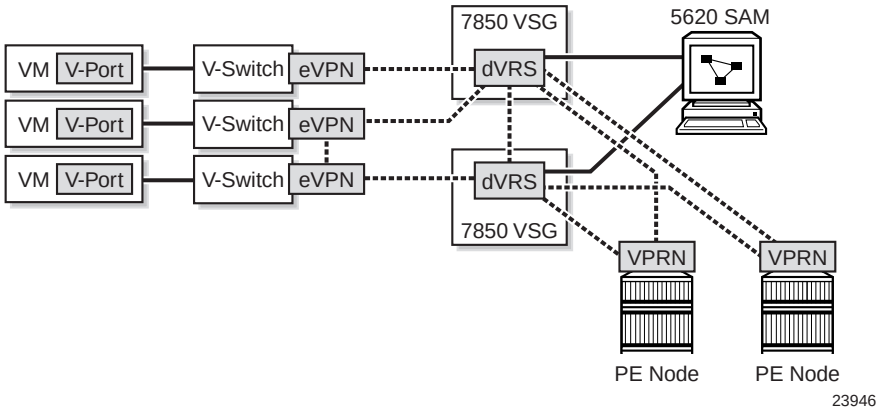
The Alcatel-Lucent distributed Virtual Routing and Switching (dVRS) service solution is implemented and monitored by the VSD. It is unique to data centers networking because it functions with the assumption that the majority of network traffic is between VMs. The service is a combined L2/L3 forwarding solution that consists of two component services which are discovered and monitored by the 5620 SAM:

- dVRS service
- EVPN service

The two components are associated using auto-bind tunnels. Underlying transport towards the VMs is encapsulated with VxLAN over UDP tunnels. Tunnels can be encapsulated with VxLAN at the V-Switch or at the 7850 VSG. Transport on the auto-bind tunnels is encapsulated using VPN over GRE tunnels. All VxLAN and GRE tunnels originate and terminate on the V-Switch. Therefore, the 5620 SAM can deduce underlay routers and ports on the V-Switch. These associations can be used for correlation and service mapping for associated virtual components, such as the VSC.

Figure 10-1 shows the main service and virtual network components in the distributed virtual routing and switching solution.

Figure 10-1 Distributed virtual routing and switching



The 5620 SAM also supports the discovery of a standalone EVPN service. The standalone EVPN serves as a virtualized VxLAN-based L2-only service. The standalone EVPN service operates for the following use cases:

- SWGW-to-VM — remote site to DC connectivity
- SWGW-to-SWGW — intra-DC connectivity
- VM-to-VM — intra-DC connectivity

10.3 Virtualized service discovery

Virtualized services are configured in the VSD and discovered for management automatically by the 5620 SAM based on VM UUID. The 5620 SAM discovers the virtualized service from the 7850 VSG or standalone VSC using a combination of the following:

- SNMP from V-Node management
- IGP and BGP from 5650 CPAM route analytics

Upon discovery of the virtualized service, the 5620 SAM creates an associated lightweight service and links it to its associated dVRS/EVPN service as a transported service (unless it is a standalone dVRS or EVPN service.)

10.4 Lightweight services

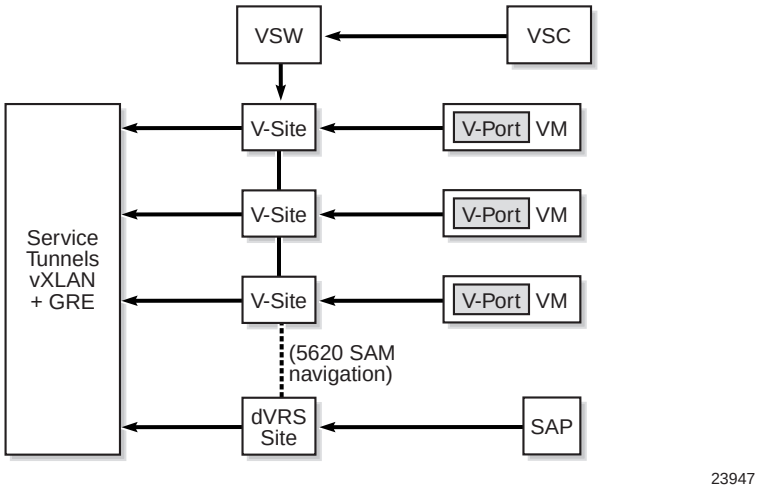
When the 5620 SAM discovers a dVRS or EVPN service from the 7850 VSG or standalone VSC, a corresponding lightweight service is automatically created. A virtual site (V-Site) is created for each corresponding dVRS or EVPN site. The V-Site includes the Nuage customer identifiers from the service. Enterprise, domain, zone and SROS customer are all associated with the V-Site and are viewable from the data plane and control views of the service. For L2 EVPN sites which contain a spoke SDP binding, the 5620 SAM creates a virtual spoke SDP on the virtual site from the V-Switch to the underlay router.

Lightweight services are unique to virtualized services and serve to alleviate the difficulties of managing and monitoring a service which is dynamic in nature. VMs are inherently mobile and service objects may be created and deleted frequently as VMs move. The lightweight service is able to track the VM in the network with the VM UUID while maintaining alarm correlations, statistics, and other data related to that VM. As VMs move and service objects are automatically deleted, the 5620 SAM maintains a log of persisted service objects so that historical routing information is not lost. Deleted V-Switch Sites are retained by the service with the operational state and state cause exposed to the user. The 5620 SAM differentiates between virtual sites which are down due to a network failure or due to an expected event. Virtual service objects are persisted for a user-defined length of time.

A lightweight service reflects the characteristics of a VM-based service by acting as a simplified proxy of the service information and assigning it as a V-Site to the V-Switch. The V-Site parent object is associated to the V-Switch rather than the NE. This lightweight service serves to provide a data plane view of the service from the perspective of the VSC. Each V-Site then links to the VSC view of the service through a control instance. In the case of a master/slave setup, a V-Site links to two control instances. The control view of the service provides more information on statistics, TCAs, and faults. It also allows you to perform event retrieval, which is not available on the V-Switch view of the service.

Figure 10-2 shows a high-level model of a dVRS lightweight service.

Figure 10-2 Control view and data plane view from a lightweight service



10.5 Services Manager

The Services Manager allows you to search for service objects based on specific criteria. You can search for lightweight service views of a virtualized service by searching for V-Sites. VPLS and VPRN service search criteria include the service domain, zone, and customer name, which allow you to search for a dVRS or EVPN service based on the VSD domain.

You can access the Services Manager by choosing Manage→Service→Services.

10.6 Virtualized service object properties forms

Virtualized service properties forms display information which helps to identify associated objects in the data center network. These relationships provide simplified navigation to associated service and virtual network objects. You can access properties forms for virtualized services is from the Services Manager. You can also navigate to a service from its associated V-Port. See Chapter 8 for more information.

Virtualized service properties form

The 5620 SAM represents a dVRS service as a VPRN with routed VPLS associations. The service properties form and child forms display the following information specific to a virtualized service.

- The General tab displays the VSD domain.
- The Virtual Machines tab lists all VMs associated with the dVRS service.
- The Transported Services tab lists all EVPN services associated with the dVRS service.
- The Sites tab displays sub-tabs which show VPLS sites, dVRS V-Sites, and EVPN V-Sites of the associated EVPN service.

The 5620 SAM represents an EVPN service as a VPLS. The service properties forms display the following information specific to a virtualized service.

- The General tab displays the VSD domain.
- The Virtual Machines tab lists all VMs associated with the EVPN service.
- The Service Tunnels tab lists all dVRS services associated with the EVPN service.
- The SDP Binding tab includes the Virtual Spoke SDP Bindings tab which lists all virtual spoke SDPs associated with the EVPN service.

These tabs offer visibility of associated services and virtual objects for each virtual service, and provide navigation to the properties forms for those objects. Because it is possible for a standalone dVRS or EVPN service to be managed by the 5620 SAM, the Service Tunnels and Transported Services tabs are useful for showing whether the service is attached.

V-Site properties form

The V-Site properties form can be accessed from the navigation tree or Sites tab on the virtualized service properties form. It provides the lightweight view of the service from the V-Switch. The form is read-only, but provides navigation to associated service and network objects.

The Upstream panel lists all advertising routers for the V-Site. It also provides navigation to the VSC view of the service on the Control Instances sub-tab. The Control Instances sub-tab lists two control instances in a master/slave scenario.

Site properties form

The VPRN dVRS Site and VPLS EVPN Site properties forms provide the VSC view of the virtualized service. It lists the same customer, VM, and transported service information as the service form. It includes statistics, TCAs, and faults information which is otherwise not available from the V-Switch view of the service.

11 — Services assurance and troubleshooting

11.1 Service assurance and troubleshooting overview

The primary purpose of the 5620 SAM in virtualized service management is improved awareness and assurance. Lightweight services offer opportunities for service object persistence to accommodate for the constant deletion and creation of service objects as VMs move within the network. As a result, event retrieval and correlation features in the 5650 CPAM are extended to persisted service objects and DC-specific events. 5650 CPAM BGP VPN route analytics are extended to virtualized services to provide assurance and troubleshooting for dVRS and EVPN service objects.

11.2 5650 CPAM for visibility and assurance

The 5650 CPAM BGP functionality provides a full view of the DC network and associated WAN routing. It supports multivendor topology views through dynamic discovery of IGP and BGP routing contexts. These views are combined with the V-Switch and VM mappings derived from V-Node discovery to create a complete mapping of the network underlay to the network overlay. The 5650 CPAM automatically monitors virtual services as they relate to the VM and V-Port state.

You can use BGP reachability analysis to monitor the BGP state for VMs and NEs in the DC network. Other BGP VPN features, such as map highlighting, can be used to associate and map virtual objects to the network underlay.

The remainder of this chapter will focus on 5650 CPAM features which have been extended with DC-specific enhancements. For more information on 5650 CPAM BGP and IGP assurance features, see the *5650 CPAM User Guide*.

11.3 Network object persistence

Due to the dynamic nature of virtualized services, it is necessary for the 5620 SAM to provide historical persistence for VMs and service objects that have been moved or deleted entirely. Lightweight services also provide persistence for service objects such as V-Sites. Network object persistence allows you to see where a VM existed in the network during a specific timeframe. You can then correlate historical faults to a persisted object to see how a current fault relates to a persisted event. The 5620 SAM differentiates between virtual sites which are down due to a network failure or due to an expected event.

11.4 Event retrieval log and correlation

Network events are stored in a history log which can be used for fault correlation. You can open the event log from the Service Navigator application. When you use the event log, you can specify a period of time from which you want to query the log for events. You can specify an interval or rewind from the current time.

The event log stores BGP events and DC events. BGP events include reachability alarms and flapping occurrences for the BGP prefix. When you perform event retrieval on a dVRS service, you can troubleshoot historical events by correlating DC events to BGP events. For example, if there is an Prefix Down BGP event, this means the virtual object was likely deleted and there will be a VM Down event for the related virtual object. In this case, an alarm would not be raised as long as the relation between events is evident. Flapping events on the VM can occur for legitimate reasons, which can be distinguished by the 5620 SAM. Alarms regarding VM state changes should only be generated when needed.

The event log provides access to two correlation features for BGP and DC events:

- root cause analysis
- impact analysis

See the *5650 CPAM User Guide* for more information on root cause analysis and impact analysis.

DC network events monitored in the 5620 SAM include the following:

- BGP: Next Hop Change
- BGP: Prefix Up
- BGP: Prefix Down
- BGP: Prefix Flapped
- DC: Vport Up
- DC: Vport Down
- DC: Vport Move
- DC: VM Up
- DC: VM Down
- DC: VM Move
- DC: Virtual Switch Up
- DC: Virtual Switch Down
- DC: VSwitch Controller Up
- DC: VSwitch Controller Down
- IGP: Upstream Connection Up
- IGP: Upstream Connection Down
- IGP: Upstream Redundancy Change

Learning correlation algorithm

The 5620 SAM uses an algorithm to determine the window in which to find a correlated event, called a learning correlation algorithm. The algorithm dynamically learns the correlation interval and calculates the average and standard deviations. The algorithm takes into account variables such as time delays and 5620 SAM release load. The learning correlation algorithm improves event and alarm correlation reliability over that of a basic correlation algorithm.

The algorithm can be set to use preset values as opposed to dynamically learned values.

Historical Event Correlation Manager

You can access the Historical Event Correlation Manager from the Inventory Management application. It allows you to configure the window of time in which events can be correlated. You can also use the Correlation Partition Manager to perform the following:

- configure historical retention behavior
- configure the maximum database size and length of a historical interval
- manually clear the historical events database

BGP event correlation

The 5620 SAM correlates DC events for impact and root cause analysis.For the purposes of event correlation, the IGP: Upstream Connection Up and Down events are similar to the VSwitch Controller Up and Down events. The IGP monitor is used to discover and log the underlay router events. An IGP: Upstream Redundancy Change event is logged when a second path to a reachable underlay router is discovered.

11.5 5620 SAM fault correlation engine

The 5620 SAM supports a fault management framework unique to data centers support. In addition to the fault management rules provided as part of the 5650 CPAM, the 5620 SAM supports a new set of correlation rules which help to monitor and troubleshoot virtual network and service objects. The 5620 SAM correlation framework is extended to persisted virtual network and service objects to allow you to view impact analysis for moved or deleted VMs, for example. This new framework allows for more flexible correlation rules and allows correlation between specific alarms. Alarms are still modeled in the 5620 SAM, but are correlated with the engine.

The 5620 SAM fault management framework includes rules for correlating data center alarms across the following:

- service status from virtualized service sites to virtual network components (V-Switch, V-Port, and VM, for example)
- threshold crossing alarms from virtualized service sites to the V-Port
- BGP prefix reachability alarms from IGP monitor to virtual network components
- BGP prefix reachability alarms from virtual network components to virtualized service sites

BGP prefix fault correlation

In addition to the existing 5650 CPAM correlation framework, the 5620 SAMsupports framework for correlating data center-specific alarms based on DC network events in the event log.

The 5620 SAM supports correlation for absent V-Port or BGP Prefix events. In cases where a V-Port or BGP Prefix event is expected, but not present, the 5620 SAM raises an alarm.

11.6 BGP troubleshooting

The 5650 CPAM includes BGP functionality for monitoring and troubleshooting a data center network. The 5650 CPAM discovers and monitors BGP routing information by consolidating the data from the 7701 CPAAs and providing an overview of a carrier network. You can use the information to, for example, monitor whether the change in the number of BGP routes may compromise the stability of the network, or if key BGP routes are disappearing. For VPRN routes, a high rate of change for a set of VRFs is flagged by the 5650 CPAM.

This section will briefly describe some of the BGP VPN troubleshooting features which are relevant for data center network management. For more information and workflows on BGP and the 5650 CPAM, see the *5650 CPAM User Guide*.

Administrative domains

An administrative domain is a user-configured grouping that represents a logical routed network. The 5650 CPAM supports IGP administrative domains and BGP AS administrative domains.

An IGP administrative domain is a routed network with OSPF, ISIS, or both protocols running. There can be only one backbone domain for each protocol. For OSPF, multiple areas with the same area ID cannot exist.

A BGP AS administrative domain is an administrative domain which represents the standard BGP AS, confederation AS, or sub-AS. A BGP confederation AS administrative domain contains other BGP sub-AS.

BGP route profiles

The 5650 CPAM supports the creation of BGP route profiles. BGP route profiles are used to monitor BGP prefix updates according to user-defined rules. The profiles tag incoming BGP events that match defined profiles. Other applications can then register with the 5620 SAM JMS server to receive a notification each time a BGP event matches a defined BGP route profile. BGP route profiles can also be used to retrieve matching BGP events.

BGP event retrieval and impact analysis

The 5650 CPAM supports BGP event retrieval, which must be configured to perform BGP impact analysis or route cause analysis. You can perform a VPRN BGP impact analysis to discover all route distinguishers and route targets within the VPN.

IGP prefix monitors

The 5620 SAM automatically discovers IGP prefixes for specific administrative domains, It discovers OSPF or IS-IS prefixes as well as protocol unspecified prefixes. The discovery includes the resolving route for the prefix, advertising routers, protocol information, and area ID. With this information, the 5620 SAM automatically creates an IGP monitor for the IGP routes in the area for that protocol. The IGP monitor allows you to accurately discover the relationship between V-Switches and VMs and the routing layer. For example, V-Switch22 routers through IPR22 and IPR23. Therefore, any in-routing or edge aggregation routers may be related to the affected V-Switch and VM.

The IGP prefix monitor logs events if there is a change in the advertising routers of the IGP route. These events include connection up, connection down, and redundancy change. These events are logged in the event retrieval log on the dVRS service. See Section 11.4 for more information about the event retrieval log.

IGP reachability is also used for fault correlation. IGP failures result in correlated alarms on the associated virtual components and virtualized services. The withdrawal of an IGP prefix is correlated to the affect V-Switches and all related virtualized services. The 5620 SAM monitors and presence or absence of an IGP prefix and displays the IGP Prefix state for the V-Switch.

11.7 Services assurance and troubleshooting procedures

Procedure 11-1 To troubleshoot a virtual service using CPAM maps

Perform this procedure to highlight a path in a virtual service.

Navigate to a virtual site

1 Open the Services Manager by choosing Manage→Service→Services from the 5620 SAM main menu.

2 Search for a virtualized service and click Properties.

3 Select a virtual site from the service navigation tree and click Properties.

Define a source and target for the map highlight

4 Click Navigate and select IGP View: Highlight to Target. The Find Target form opens.

By default, the V-Switch for the V-Site is listed as a target for the highlight source.

5 To add more source sites, if required, perform the following steps.

- **i** Click Add. The Select Source Site for Target form opens.
- **ii** Select a Site and click OK.

6 Click Select. The Select Target form opens.

7 To select a highlight target, perform one of the following steps.

- **a** Select a service site as a highlight target.
  - **i** Select Site (Service Management).
  - **ii** Select a site and click OK.
- **b** Select a V-Port as a highlight target.
  - **i** Select Virtual Port (Data Center).
  - **ii** Select a V-Port and click OK.

Display the route highlight on the topology map

8 Click OK in the Find Target form. The IGP Topology Map is displayed with the specified route highlighted.

See the *5650 CPAM User Guide* for more information on the features available from the IGP Topology Map.

Statistics management

12 — Statistics collection and plotting

12 — Statistics collection and plotting

12.1 Statistics collection and plotting overview

The 5620 SAM performs on-demand or scheduled statistics collection for managed NEs, services, or virtual network objects. These statistics can be used to monitor or troubleshoot a data centers network, or to perform SLA or billing functions. Statistics collection can be configured with policies that are distributed to specified network objects. Statistics are displayed in tabular or graphical form using the statistics plotter.

12.2 Statistics collection

The 5620 SAM collects network performance statistics by polling network element MIB tables using SNMP. Performance statistics provide information about physical equipment, routing, and other NE properties. MIB statistics collection policies define performance statistics collection at the NE level or the network object level. The 5620 SAM supports the collection of some statistics counters from standard system, interface, and routing MIBs on generic NEs.

The 5620 SAM collects accounting statistics to gather throughput information for queues that are associated with SAPs, network ports, and subscriber profiles. Accounting statistics policies can be defined for V-Ports to monitor service, network, or subscriber accounting statistics. The 5620 SAM uses FTP or SFTP to collect MIB-based accounting statistics from NEs. Queue filters can specify which queues are processed by the statistics collector and which are ignored.

The 5620 SAM collects server performance statistics to monitor 5620 SAM system functions and processes. Server performance statistics are collected from internal 5620 SAM data, such as memory usage and alarm counters.

BGP statistics can be collected and monitored using functionality from the 5650 CPAM. Network BGP statistics are collected by the 7701 CPAA and retrieved by the 5650 CPAM. MIB statistics policies can be applied to the 7701 CPAA to define the collection of specified statistics counters. BGP statistics can be plotted and stored using the statistics plotter. The 5650 CPAM has BGP-specific threshold crossing alarms which are raised by the 7701 CPAA when specified thresholds are reached.

Collected statistics are stored in the 5620 SAM database and are retained for a specified duration. Statistics data can be backed up and recalled from the database.

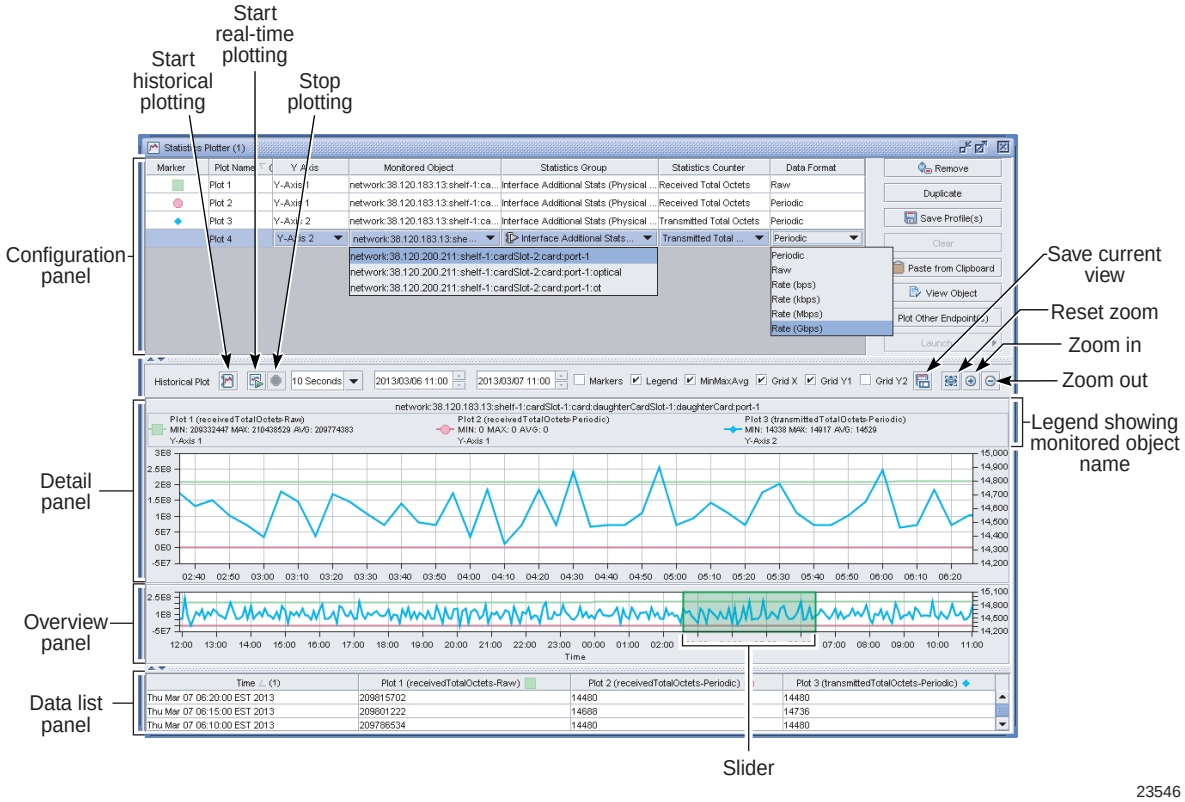
See the *5620 SAM Statistics Management Guide* for more information on statistics collection.

12.3 Statistics plotting

All supported statistics types can be viewed in tabular or graphical format using either historical or real-time data. Tables list specific values of historical data, and table data can be sorted, filtered, and exported to files in different formats. Graphs can be used to identify trends and display multiple statistics counters simultaneously using the 5620 SAM Statistics Plotter. The statistics plotter graphs collect statistics from a specified time period, including real-time plotting. The statistics plotter can plot ingress and egress utilization statistics using calculated values. Plotted utilization statistics provide an accessible view of the bandwidth usage on a specified port in both tabular and graphical form.

Figure 12-1 shows the 5620 SAM Statistics Plotter and outlines some of the features.

Figure 12-1 5620 SAM Statistics Plotter



See the *5620 SAM Statistics Management Guide* for more information on statistics plotting and graphing.

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

www.alcatel-lucent.com