# Avaya Configuration and Orchestration Manager Administration — Utilities

2.3
NN47226-600
05.03
June 2011

**Notice**

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

**Documentation disclaimer**

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

**Link disclaimer**

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

**Warranty**

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

**Copyright**

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

**Third-party components**

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

**Trademarks**

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

**Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

**Contact Avaya Support**

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

## Contents

# Chapter 1: New in this release

The following sections detail what's new in *Avaya Configuration and Orchestration Manager Administration — Utilities* (NN47226-600) for Release COM 2.3.



## Features

See the following sections for information about feature changes:



### VSN Manager

The Virtual Services Network (VSN) Manager permits you to configure and view Layer 2, and Layer 3 Shortest Path Bridging MAC (SPBm) throughout the discovered network. You can add, delete and edit L2 SPBm and L3 SPBm across multiple devices. For more information about the VSN Manager, see Using the Virtual Services Network Manager on page 305.

### VSN Wizard

The Virtual Services Network (VSN) Wizard permits you to configure VSN service on multiple devices. For more information about the VSN Wizard, see VSN wizard on page 359.

All Configuration and Orchestration Manager (COM) wizards support working offline. For more information about offline mode, see Offline Mode on page 370.

## VSN template

You can create a Virtual Services Network (VSN) template using the VSN Wizard or the Templates tool. For more information about the VSN template, see Template support on page 371, and Adding a VSN template on page 380

## Virtualized Services Manager Shortest Path Bridging MAC

With The Virtualized Services Manager, you can map and highlight Shortest Path Bridging MAC (SPBM) meshes and trees. For more information, see Virtual Services Network Manager on page 306.

## SPBM-BVLAN

The VLAN Manager supports SPBM BVLAN VLANs. You can create, read or update the SPBM BVLANS on ERS 8600/8800 v 7.1 devices. For more information about the SPBM-BVLAN, see VLAN Manager features on page 28, and Creating an spbm—based VLAN on page 50.

## Trap Viewer

The Trap viewer tool is added to the Managers panel. For more information about the Trap Viewer, see Using the Trap Viewer on page 333.

## Syslog Viewer

The Syslog viewer is moved from the Trap/Log Manager to the Managers panel. For more information about the Syslog Viewer, see Using the Syslog Viewer on page 335.

## Bulk Configuration Manager

In Configuration and Orchestration Manager (COM) 2.3, the Bulk Configuration Manager (BCM) supports the Virtual Services Platform (VSP) 9012, Wireless LAN 8180, and ERS 8800 devices. For more information about the BCM, see Using the Bulk Configuration Manager on

page 301. For more information about the configuration of the BCM, see *Avaya Bulk Configuration Manager Fundamentals* (NN48021-100).

# Other changes

See the following sections for information about changes that are not feature-related.

Figures on page 9

## Figures

Figures in this document are updated. New figures show installer changes.

# Chapter 2: Introduction

This document provides the information you require to configure various managers in the Configuration and Orchestration Manager (COM) 2.3.

# Chapter 3: Using the topology view

This chapter describes the topology view and the tasks that you can use it to perform.

**Navigation**



## About the topology view

The topology feature in COM performs a discovery of the devices in your network, and creates a topology map showing the discovered devices and the connections between them. You can use the topology view to:

- display a logical topology map of your network.
- view link data and device connections.
- view device properties data.
- view real-time information from devices for the following:
  - dump topology
  - learned MAC addresses
  - port status
- launch element managers for the devices.
- debug or troubleshoot network problems.
- pan through the topology map to focus on a specific area of network.
- manually add the devices using the add button. These devices are visible on the topology as standalone devices and permit you to launch the element manager and other right click menu functions from the topology view. However, these devices are not available in the multi-element manager functionality.
- save the current topology and export it to an XML file which you can load into COM again. This provides a way for you to save multiple topologies without having to do a rediscovery.

If you saved the layout of a topology and rediscovered the network, the previously discovered devices maintain their layout position and eliminate the need to relayout the topology after each discovery.

- view the unreachable status. The devices in the topology view show an orange color to indicate the unreachable status. Unreachable status means that the device did not respond to SNMP queries from COM because the device was down, or because the SNMP credentials provided to COM are not correct for the device in unreachable state.

For more information about using the topology map features, see *Avaya Configuration and Orchestration Manager—Using the Product Interfaces* (NN47226–100).

Using the topology view to perform a discovery is the first step in managing your network using COM. A discovery is a snapshot taken of part or all of a network. When you perform a discovery, the information collected by COM to create the topology map is also used to populate the device inventory.

The topology feature can discover devices that support the following protocols:

- 802.1ab (Link Layer Data Protocol, or LLDP)
- Avaya Discovery Protocol (NDP), formerly known as Bay Networks Autotopology Discovery Protocol, or SynOptics Network Manager Protocol (SONMP)

One of these protocols must be enabled on the device in order for COM to discover it.

In order for COM to discover the devices in a topology, you must first configure the device credentials. COM uses the SNMPv1/v2/v3 credentials of the device to properly perform a discovery. If the device credentials are not configured, COM will use the default community strings (public and private) to attempt to discover the device. If the credentials are not configured, the audit log displays errors for these devices.

You can configure device credentials using the Device and Server Credentials editor in the Avaya Unified Communications Management (UCM platform). For more information about configuring device credentials, see *Avaya Unified Communications Management Fundamentals* (NN48014-100).

# Understanding the topology map

You can use the topology map to gain a high-level view of your network, or to view detailed information about devices and links in the topology.

For information about navigating the topology and displaying information on the topology map, see Viewing discovery results on page 17. For information about the tools and utilities that you can use to work with devices on the topology map, see Working with devices on the topology map on page 19.

# Configuring and performing a discovery

This section provides information about the following topics:



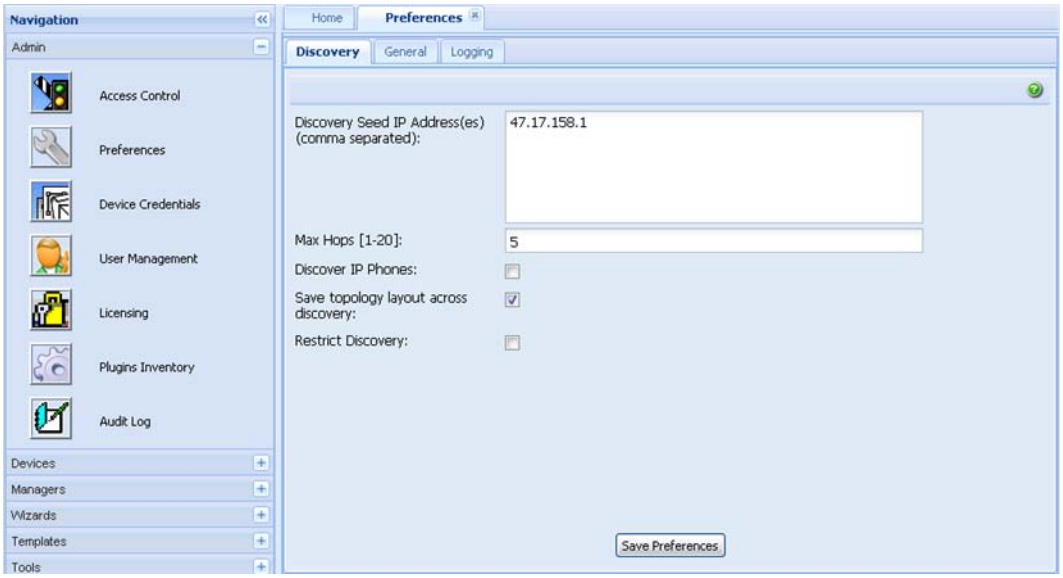
## Configuring a network discovery

Perform the following procedure to configure a network discovery. COM uses the information you configure to discover devices and create a topology map.

### Procedure steps

1. From the Navigation pane, open **Admin** and then select **Preferences**.

   The Preferences dialog box appears in the Contents pane.



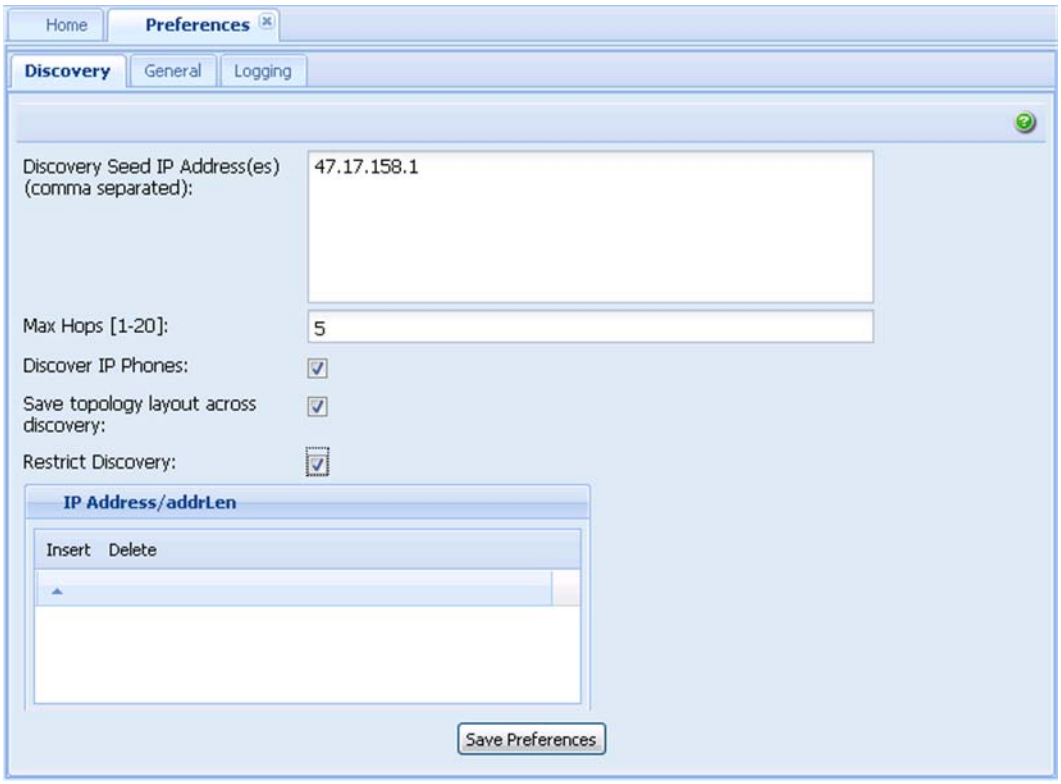

   Or

   Navigate to the **Home** tab tool bar, and click on the **Set Discovery Preferences** button (represented by a wrench).

2. In the **Discovery Seeds** field, enter the IP address of one or more devices in the network. Separate multiple IP addresses with a comma.
3. In the **Max Hops** field, enter the maximum number of hops.

4. Check the **Discover IP Phones** check box to discover the IP phones and to appear in the topology map.
5. Check the **Save topology layout across discovery** check box to save the topology map.
6. In the **Restrict Discovery** check box, check the check box to restrict device discovery to only the devices entered in the subnets.

   If Restrict Discovery check box is selected, then the IP Address/addrLen dialog box appears.




7. Click **Insert** to enter the IP addresses.
8. To delete an IP address, select the required row and click **Delete**.
9. Click **Save Preferences**.

## Performing a network discovery

Before you begin, ensure that you have configured the discovery settings and entered the credentials for the devices in your network. You must enter the SNMPv1/v2 credentials for each device in order for COM to properly discover the device. If you do not configure these device credentials, COM will discover devices, but the functionality available through COM will be limited.

For information about setting device credentials, see *Avaya Unified Communications Management Fundamentals* (NN48014-100). For information about setting discovery preferences, see Configuring a network discovery on page 15.

### Procedure steps

1. On the **Home** tab, click the **Discover Network Topology** button.

   A dialog box displays, showing the progress of the discovery.

   **Note:**
   If you wish to cancel the discovery process, click **Stop** on the dialog box.
2. An Info dialog box displays to confirm that the discovery is complete. Click **OK**.

## Updating discovery information

Use the following procedure to refresh the topology view and update it to include new devices.

### Procedure steps

On the **Home** tab, click the **Refresh Device Topology** button.

An updated topology map displays.

# Viewing discovery results

This section provides information about the following topics:



## Navigating the discovery results

This procedure describes how to use the topology map to perform the following tasks:

- zoom in and out
- search by device IP or by SysName
- clear the highlights

### Procedure steps

1. Select the **Home** tab.
2. Use the buttons on the toolbar to navigate the topology map. The following table lists the options available.

**Table 1: Navigation tools**

| Task/button | Description |
|---|---|
| Zoom-in and Zoom-out | Allows you to zoom in or out of the topology view. |
| Search IP Address/SysName | Allows you to search and highlight an IP address you are looking for. You can search based on:<br>• a partial or full IP address<br>• IPv4 format<br>• IPv6 format<br>Enter an IP address or a partial IP address, and then click Search. The given device with the specified IP address on the map is selected. If you enter a partial IP address, the topology selects the first occurrence of a device that matches the partial IP address, and if you continue to enter, the next one is selected. If the IP address is not found, the search button stops selecting an address. |
| Panning tool | Allows you to move the map to view specific sections. Right-click on any blank area of the map and drag it in the desired direction. |
| Navigation tool | Allows you to navigate the map by moving the blue square provided at the bottom right corner of the map. |

## Displaying information on the topology map

This procedure describes how to use the topology map to perform the following tasks:

- display port names
- toggle between names and addresses
- display link data

### Procedure steps

1. Select the **Home** tab.
2. Click the **View Device Information** button on the toolbar.

The following table lists the options available.

**Table 2: Displaying topology information**

| Task | Description |
|---|---|
| Display port names | Select the check box to display port names on the topology map. |
| Toggle Addr / Name | Select the check box to toggle the name and address of the device. |
| Link data | Select the link details to view:<br>• link speeds<br>• link duplex<br>• link types<br>• link mismatch<br>• clear highlights<br>COM displays the real-time settings for the interface attributes, and highlights the topology map based on the discovered data. |

# Working with devices on the topology map

This section describes how to use the topology map to perform the following tasks:

- ping devices
- view connections
- view device properties
- launch an element manager
- view a topology dump
- view learned MAC addresses
- view port status

### Procedure steps

1. Select a device on the topology map and right-click on the device.
2. Select an option from the right-click menu. The following table lists the options available.

**Table 3: Right-click options**

| Menu option | Description |
|---|---|
| Ping | Allows you to ping the selected device from the server. |
| Show connections | Displays the neighbors of a device on the topology map. It does not display live connections, only what is on the topology map. |
| Properties | Displays the following properties of the device:<br>• Name<br>• IP address<br>• Device type<br>• Location<br>• Contact<br>• Version<br>• Uptime<br>• Description |
| Launch Element Manager | Launches the element manager for the selected device. |
| Dump Topology | Displays the topology based on the real-time queries of devices. |
| Learned Mac Addresses | Displays the learned Mac addresses on the selected device. |
| Port Status | Displays the status of the port:<br>• green—the port is in-service<br>• red—the port is out-of-service<br>• blue—the port is being tested |
| Close | Closes the topology map. |

# Working with multiple topologies

The Home tab on the COM interface displays one active topology at a time, but you can work with multiple topologies if needed. You can export a saved topology from the topology view or from the Device Inventory manager, and then discovery a new topology. To work with the saved topology, you can import it using the topology view or the Device Inventory Manager. When you import a saved topology, the existing topology is overwritten by the data in the imported file.

### Navigation


- Saving a topology on page 21
- Exporting and importing a topology from the Device Inventory Manager on page 21
- Exporting and importing a topology from the topology map on page 22


## Saving a topology

You can change the topology layout to meet your needs and save it. The topology is saved for the server and is not saved on a per-user basis.

### Procedure steps

1. Select the **Home** tab.
2. Click the **Save Topology** button on the toolbar, located to the right of the Search for device IP window.

   The button is

   A confirmation window displays.
3. Click **OK**.

## Exporting and importing a topology from the Device Inventory Manager

To work with multiple topologies, you must export the active topology to an XML file, and then discover a new topology. You can repeat this process as often as you need to, and can revert to a saved topology by importing it back into COM.

Use the following procedure to export and import a topology using the Device Inventory Manager.

### Procedure steps

1. To save an existing topology, select **Devices** from the Configuration and Orchestration Manager Navigation pane.

   The Devices panel appears.
2. From the **Devices** panel, click **Device Inventory** icon.

   The Device Inventory Manager dialog box appears.
3. From the Device Inventory Manager toolbar, click the **Import/Export Inventory** button.

   The Import/Export Inventory dialog box appears.

4. Select **Export inventory to an XML file** and click **Export**.
5. Click **Save**.
6. Set the discovery preferences and discover a new topology. The new topology becomes active on the Home tab.
7. To save the currently active topology, repeat steps 1 through 5.
8. To reload the original topology, select **Devices** from the navigation pane.
9. From the **Devices** panel, click **Device Inventory** icon.
10. From the Device Inventory Manager toolbar, click the **Import/Export Inventory** button.
11. Select **Import inventory from an XML file** and click **Browse** to navigate to the location of the file.
12. Select the file and click **Open**.
13. Click **Import**.

    The Device Inventory table and the topology view are updated.

## Exporting and importing a topology from the topology map

To work with multiple topologies, you must export the active topology to an XML file, and then discover a new topology. You can repeat this process as often as you need to, and can revert to a saved topology by importing it back into COM.

Use the following procedure to export and import a topology using the Device Inventory Manager.

### Procedure steps

1. To save an existing topology, select the **Home** tab.
2. Click the **Import/Export Topology** icon, located on the right side of the toolbar.

   The Import/Export Inventory dialog box appears.
3. Select **Export inventory to an XML file** and click **Export**.
4. If you are using IE7, click **Save**.

   If you are using Firefox 3.x, click **save file**.
5. Set the discovery preferences and discover a new topology. The new topology becomes active on the Home tab.
6. To save the currently active topology, repeat steps 1 through 5.
7. To reload the original topology, click the **Import/Export Topology** button from the navigation pane.

   The Import/Export Inventory dialog box appears.

8. Select **Import inventory from an XML file** and click **Browse** to navigate to the location of the file.
9. Select the file and click **Open**.
10. Click **Import**.

    The Device Inventory table and the topology view are updated.

# Chapter 4: Using VLAN Manager

VLAN Manager allows you to create VLANs and configure routing and domain synchronization for them. You can also use VLAN Manager to create and manage Avaya Spanning Tree Groups (Avaya STG), as well as Multiple Spanning Tree Protocol (MSTP) and Rapid Spanning Tree Protocol (RSTP) instances.

COM organizes VLAN management according to four primary taskflows:

- **Configuration of Spanning Tree Groups**

  Creating STGs is the first step in the process of configuring VLANs. You must create an STG before you create a VLAN on Avaya devices. If you do not create anSTG, the device will use the default STG that is included in the factory configuration. There are three types of STG:

  - Avaya STG
  - RSTP
  - MSTP

  **Note:**
  Avaya STGs are filtered out for VSP because they are not supported.

  **Note:**
  In the VLAN manager, Wireless Controller (WC) devices do not support the MSTP mode.

- **Basic configuration of VLANs**

  Basic configuration of VLANs includes the creation and deletion of VLANs, synchronizing the VLAN name, adding members to a VLAN group, and deleting VLANs.

- **Routing**

  You can use COM to configure OSPF and VRRP routing interfaces on a VLAN.

- **Domain synchronization**

  Domain synchronization allows you to distribute the VLAN configuration of one device to other devices in your network.

**Note:**
WC devices work in a similar way to the mERS5600 devices. The workflow of VLAN manager for the WC is similar to the mERS5600 version 6.2 and above.

This section describes using VLAN Manager to manage and view VLANs on Avaya Ethernet Switches and Avaya Ethernet Routing Switches.

### Navigation



# About VLAN Manager

VLAN Manager supports the VLAN and STG MIBs, and lets you manage VLAN and STG configurations across a single device or multiple devices. This section describes VLAN Manager conventions and features.

### Navigation



## VLAN

VLAN is a collection of ports on one or more switches that defines a broadcast domain. You can assign ports to a VLAN or you can create a policy VLAN, which determines the port membership in the VLAN based on the traffic entering that port. For example, in an IP subnet-based VLAN, the port belongs to the VLAN only if the traffic passing through the port is on the specified IP subnet.

You control path redundancy for VLANs by implementing the Spanning Tree Protocol (STP).

## Spanning Tree Protocol

The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. When multiple paths exist, the spanning tree algorithm configures the network so that

a bridge or switch uses only the most efficient path. If that path fails, the protocol automatically reconfigures the network to activate another path, thus sustaining network operations. The collection of ports in one spanning tree is called a Spanning Tree Group (STG) and a network can include multiple instances of STGs.

All the devices supported by COM support at least one STG. The Passport 1000 Series switch and the Ethernet Routing Switch 8600 modules support multiple spanning trees, thus multiple Spanning Tree Groups.

**Note:**
VSP 9000 supports RSTP and MSTP, but does not support Avaya STG protocol.

**Note:**
In the VLAN manager, WC devices do not support the MSTP mode.

Table 4: Maximum STGs and VLANs supported by switches on page 27 lists the details for different switches.

**Table 4: Maximum STGs and VLANs supported by switches**

| Switch | Maximum number of STGs | Maximum number of VLANs |
|---|---|---|
| Passport 1000 Series switch | 25 | 101 |
| Ethernet Routing Switch 1424/1612/1624/1648 switches | 1 | 2048 |
| Ethernet Routing Switch 8100 modules | 1 | 2000 |
| Ethernet Routing Switch 8300 modules | 64 | 4000 |
| Ethernet Routing Switch 8600 and 8800 modules | 64 | 4096 |
| BayStack 380 3.0 | 1 | 512 |
| BayStack 420 | 1 | 32 |
| Ethernet Switch 410/450 | 1 | 64 |
| Ethernet Switch 325/425 | 1 | 255 |
| Ethernet Switch 460/470 | 8 | 256 |
| Ethernet Routing Switch 5510, 5520, 5530, 3510 and 5600 | 8 | 256 |
| Ethernet Routing Switch 45xx | 8 | 256 |
| Ethernet Routing Switch 25xx | 1 | 256 |
| Business Policy Switch 2000 | 8 | 256 |

| Switch | Maximum number of STGs | Maximum number of VLANs |
|---|---|---|
| Virtual Services Platform | 64 | 4096 |
| Wireless Controller | 8 | 256 |

## VLAN Manager features

The VLAN Manager supports six types of VLANs and three types of STGs:

- VLANs:
  - port-based
  - protocol-based
  - subnet-based
  - source MAC address-based
  - sVLAN-based
  - ID-based
  - spbm-bvlan-based
- STGs:
  - Avaya STGs
  - RSTP
  - MSTP

The VLAN Manager allows you to do the following:

- Configure and monitor VLANs and STGs across one or multiple devices.
- View and edit port membership information for the following:
  - ports not belonging to an STG
  - ports belonging to multiple STGs
  - individual routing ports and brouter ports

**Note:**
The VLAN Manager does not support the configuration of port members through the Edit screen for spbm-bvlan-based VLANs.

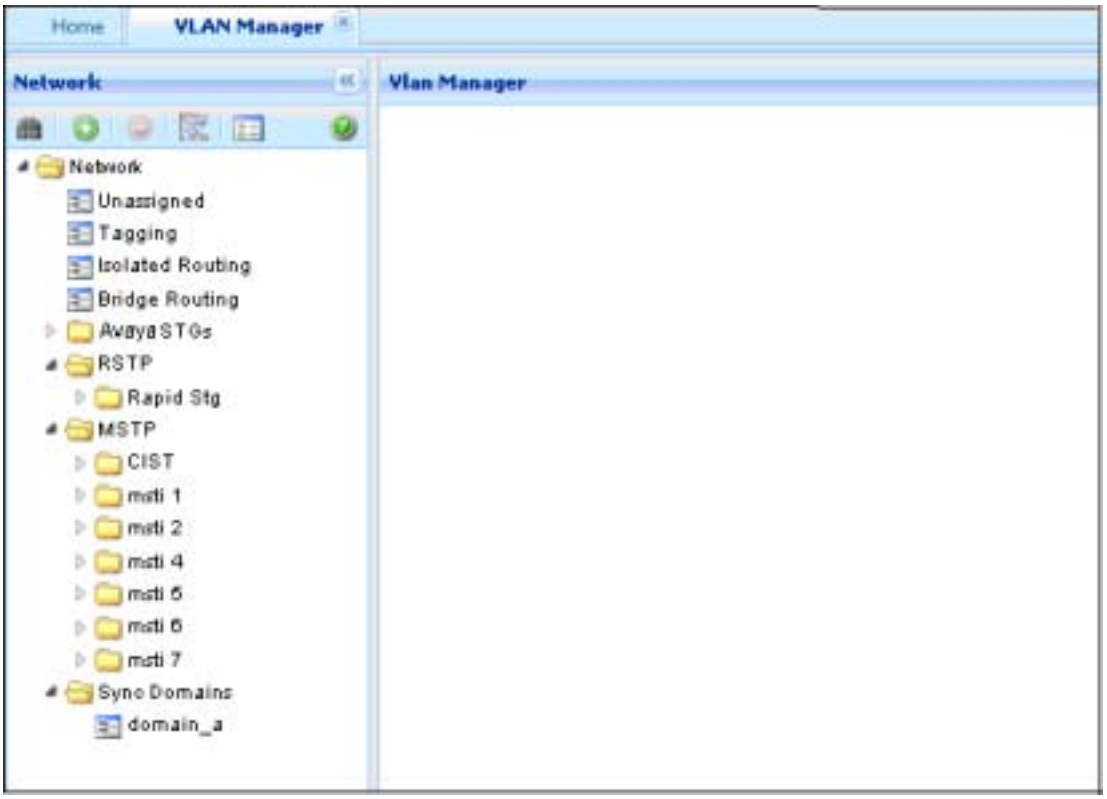
- View Spanning Tree configuration information in the COM topology map, such as the ports that are blocking or forwarding. You can also see which device is the root of the Spanning Tree configuration. For more information, see Viewing STG and VLAN information on page 73.

# Starting VLAN Manager

Perform the following procedure to start the VLAN Manager.

### Procedure steps

In the COM Navigation pane, expand the managers and click on the **VLAN manager**. The VLAN manager is launch and appears in the content pane.




# Using the VLAN Manager window

This section details the VLAN Manager interface as seen in the following figure.

Table 5: VLAN Manager window on page 30 describes the parts of the VLAN Manager window.

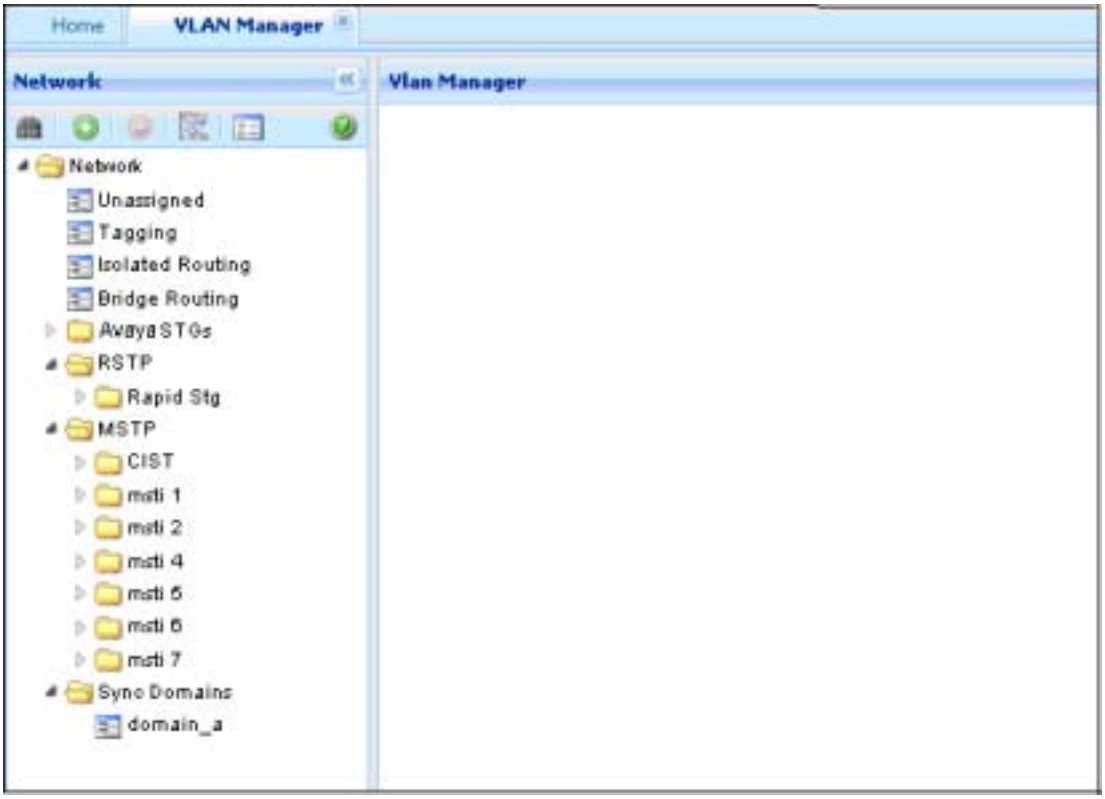



**Figure 1: VLAN Manager**

### Table 5: VLAN Manager window

| Area | Description |
|---|---|
| Navigation pane | Provides a navigation tree showing VLAN Manager network folder resources and a toolbar for working with items in the pane. For more information, see Navigation pane on page 31. |
| Contents pane | Displays information selected in the contents pane and a toolbar for working with items in the pane. For more information, see Contents pane on page 33. |
| Status bar | Displays status information, it includes discovery information, type of node highlighted, and command status. For more information, see Status bar on page 34. |

## Navigation

- Navigation pane on page 31
- Contents pane on page 33
- Status bar on page 34

## Navigation pane

The VLAN Manager Navigation pane, provides access to all VLAN Manager resources as shown in the Figure 2: Navigation Pane on page 31 figure.

To open the folder, double-click a folder, or click the pointer (>) sign to the left of the folder name. Click an item to examine detailed information in the Contents pane.

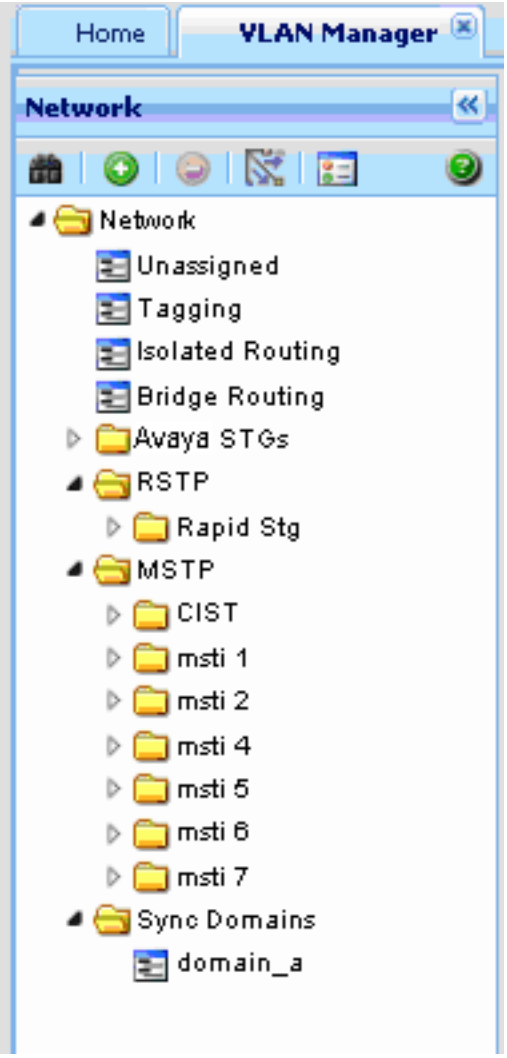



**Figure 2: Navigation Pane**

The following table details the VLAN Manager Navigation pane.

**Table 6: VLAN Manager Navigation pane**

| Area | Description |
|---|---|
| Network folder | Contains all of the icons and folders in the Navigation pane. |
| Port membership icons | Shows the types of port membership, including Unassigned, Tagging, Isolated Routing and Bridge Routing. For more information, see Port membership types on page 58. |
| Avaya STG folders | Shows Spanning Tree Groups (STG) on the discovered devices. Click the pointer (>) to the left of the folder or double-click an STG folder to open and close the folder. For more information, see Viewing Spanning Tree Groups on page 73. |
| VLAN icons | Show you information about VLANs. Click one of the icons to view information about that VLAN in the contents pane. |
| MSTP folder | Represents Multiple Spanning Tree Protocol. Double-click the folder to view aspects of MSTP. Click one of the icons to view information about that aspect of the MSTP in the contents pane. |
| CIST folder | Shows you information about the MSTP Common and Internal Spanning Tree (CIST). Click one of the icons to view information about that aspect of the CIST in the contents pane. |
| MSTI folder | Shows you information about Multiple Spanning Tree instances (MSTI). Click one of the icons to view information about that aspect of the MSTI in the contents pane. |
| RSTP folder | Shows you information about the Rapid Spanning Tree Protocol (RSTP). Click one of the icons to view information about that aspect of the RSTP in the contents panel. |
| Sync Domains folder | Allows you to define new synchronization domains and, when opened, provides a list of the sync domains defined previously. For more information, see Domain synchronization on page 62. |

## Navigation pane toolbar

The navigation toolbar allows you to add, or delete VLANs and STGs. You can also highlight MLT constructs on the Topology Map using the Highlight on Topology button as shown in the following figure.

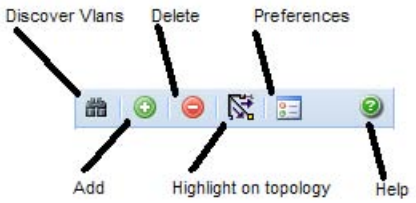



**Figure 3: Navigation pane toolbar**

**Table 7: Navigation pane toolbar fields**

| Button | Description |
|---|---|
| Discover Vlans | Allows you to manually start the Vlan discovery process. |
| Add | Allows you to add Vlans and STGs to the network. |
| Delete | Allows you to remove Vlans and STGs from the network. |
| Highlight on topology | Highlights devices in the content pane for the selected Vlan ot STG. |
| Preferences | Opens the Preferences dialog box. |
| Help | Launches help relative to the VLAN Manager. |

## Contents pane

Use the contents pane to view information on resources you select in the Navigation pane.

Click an icon In the Navigation pane to display corresponding information tables in the Contents pane.


**Figure 4: VLAN Manager Content pane**

The content pane tabs appear for STGs. The content pane fields vary in accordance with the resource you select in the Navigation pane, and the content pane tab, if applicable.

**Table 8: VLAN Manager Content pane toolbar**

| Button | Description |
|---|---|
| Add | Add a row. |
| Delete | Delete the selected row. |
| Apply changes | All the changes are applied and saves. |
| Revert changes | Revert back the changes. |
| Add VRRP | Insert |

## Status bar

The VLAN Manager status bar is located at the bottom of the VLAN Manager tab and contains two fields. The following table describes the VLAN Manager status bar fields.

**Table 9: VLAN Manager status bar fields**

| Field | Description |
|---|---|
| Message | Located on the left, the message field displays information about VLAN Manager operations. |
| Icon | Located on the right, the icon field provides a legend for different types of VLANs found in the network. For more information about VLAN icons, see VLAN icons on page 77. |

# Creating and configuring Avaya Spanning Tree Groups

The following sections topics describe how to create and modify Avaya STGs, and provide information about Avaya STG membership:

### Navigation

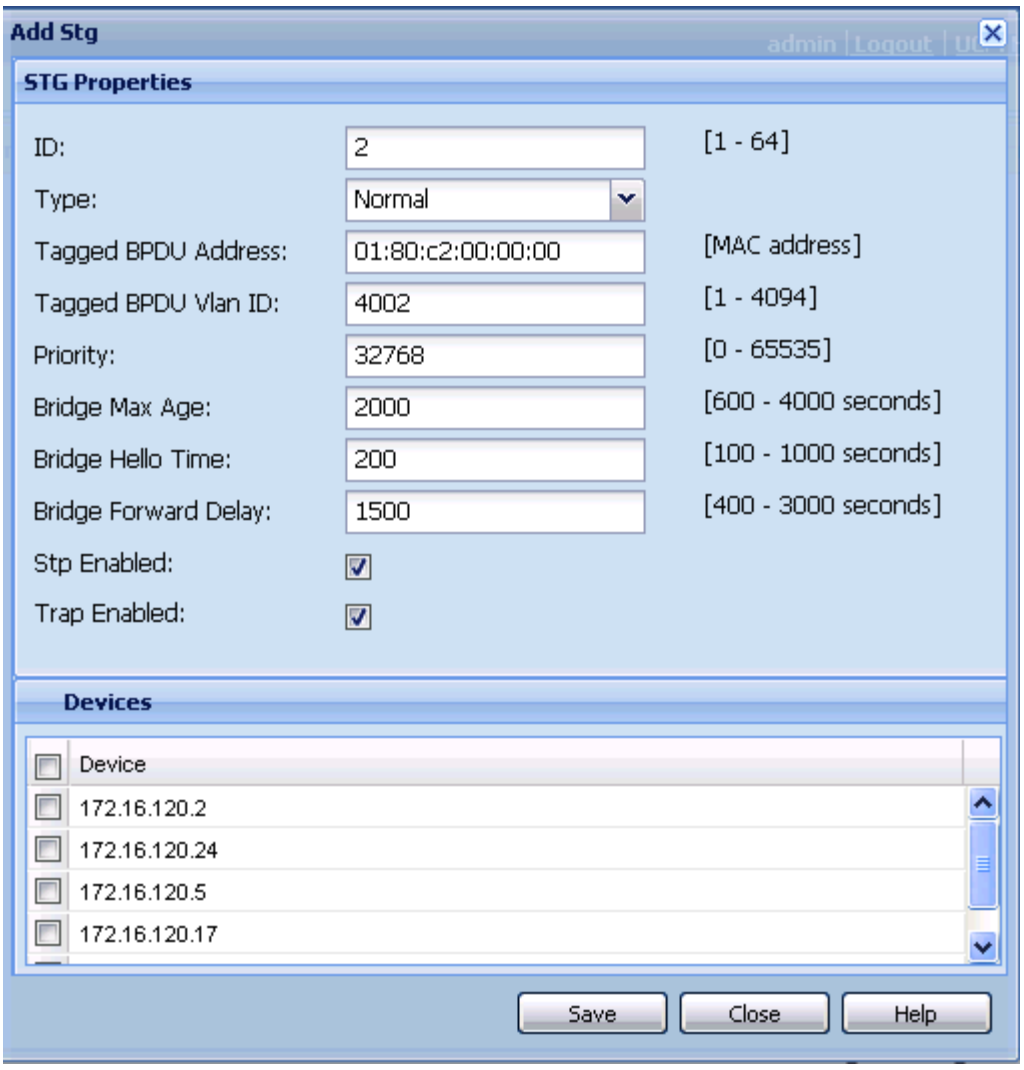
# Creating an Avaya Spanning Tree Group

Perform the following procedure to create a new Avaya Spanning Tree Group.

### Procedure steps

1. From the navigation tree, select the Avaya STGs folder.
2. Click **Add**.

   The Add STG dialog box appears.




3. Insert values or select options in the option boxes appropriately.
4. Click **Save**.

## Add STG dialog box fields

The following table describes the items in the Add STG dialog box.

**Table 10: Add STG dialog box items**

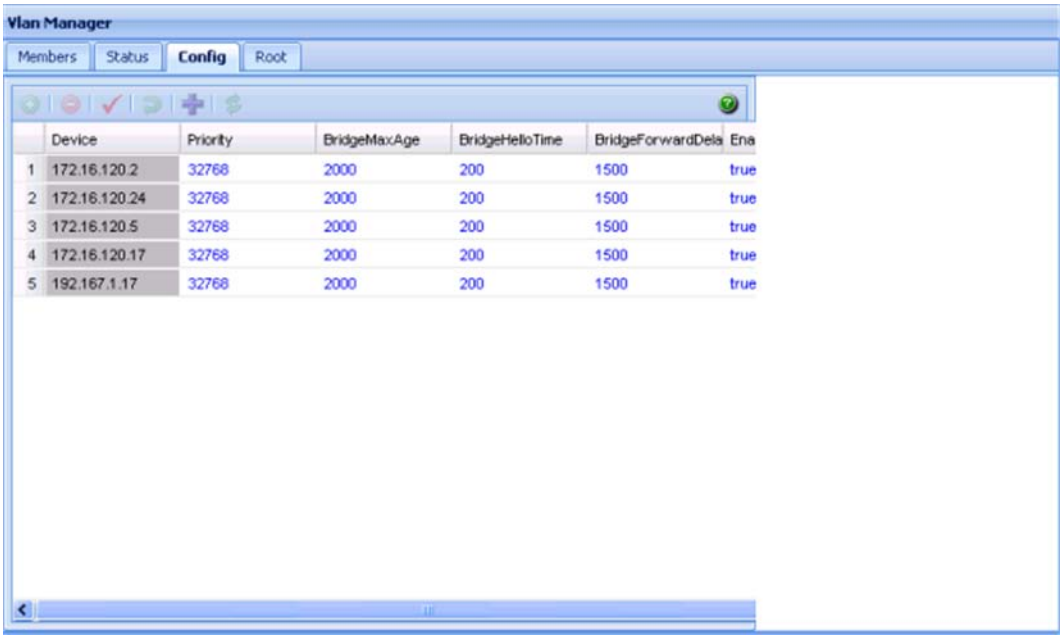
| Field | Description |
|---|---|
| ID | A number between 1 and 64 that identifies the new Spanning Tree Group (STG) configured on the network. |
| Type | Select the type of STG, either normal or svlan. |
| TaggedBpdu Address | A MAC address, specifically for tagged BPDUs. |
| TaggedBpdu Vlan ID | The VLAN tag associated with the STG. This ID is used to tag BPDUs through a non-IEEE tagging bridge to another Avaya Ethernet Switch or Ethernet Routing Switch. |
| Priority | STP bridge priority, in decimal. The range is 0 (highest priority) to 65535 (lowest priority). The default is 32768. |
| Bridge Max Age | Value in hundredths of a second that all bridges use for MaxAge when this bridge is acting as the root.<br>**Important:**<br>The 802.1D-1990 standard specifies that the range for this parameter is related to the value of dot1dStpBridgeHelloTime. The default is 2000 (20 seconds). |
| Bridge Hello Time | Value in hundredths of a second that all bridges use for Hello Time when this bridge is acting as the root. The granularity of this timer is specified by the IEEE 802.1D-1990 standard to be in increments of 1/100 of a second. The default is 200 seconds. |
| Bridge Forward Delay | Value in hundredths of a second that all bridges use for Forward Delay when this bridge is acting as the root. The default is 1500 (15 seconds). |
| Stp Enabled | Enables or disables the spanning tree algorithm for the Spanning Tree Group. |
| Trap Enabled | Enables SNMP traps to be sent to trace receiver every time an STP topology change occurs. |
| Device | Selects all the devices on the device list. |
| Save | Applies your settings and closes the dialog box. |
| Close | Discards your settings and closes the dialog box. |
| Help | Opens COM Online Help in a Web browser. |

# Configuring Avaya STG parameters

Use the Config table to view and configure Avaya STG parameters. Perform the following procedure to open the Config table.

### Procedure steps

In the Navigation pane, open an Avaya STG and select **Config**.




## Job aid

The following table describes the fields in the Configuration table.

| Field | Description |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Priority | The Spanning Tree Protocol (STP) bridge priority, in decimal. The range is 0 (highest priority) to 65535 (lowest priority). The default is 32768. |
| BridgeMax Age | The value in hundredths of a second that all bridges use for MaxAge when this bridge is acting as the root. |
| BridgeHello Time | The value in hundredths of a second that all bridges use for Hello Time when this bridge is acting as the root. The granularity of this timer is specified by the IEEE 802.1D-1990 standard to be in increments of 1/100 of a second. The default is 200 (2 seconds). |

| Field | Description |
|---|---|
| BridgeForward Delay | The value in hundredths of a second that all bridges use for Forward Delay when this bridge is acting as the root. The default is 1500 (15 seconds). |
| EnableStp | Enables or disables the spanning tree algorithm for the Spanning Tree Group. |
| StpTrap Enable | Enables or disables SNMP traps to be sent to trace receiver every time an STP topology change occurs. |
| TaggedBpdu Address | A MAC address; specifically for tagged BPDUs. |
| TaggedBpdu VlanId | The VLAN tag associated with the Spanning Tree Group. This ID is used to tag BPDUs through a non-IEEE tagging bridge to another Ethernet Routing Switch. |

## Editing an Avaya Spanning Tree Group

Perform the following procedure to edit a Spanning Tree Group.

### Procedure steps

1. Select an Avaya STG folder.
2. Click **Config**.

   The **Config** tab appears displaying the Avaya STG details.
3. In the Avaya STG table in the contents pane, click the item that you want to edit.

   The field is highlighted, and you can edit directly in the table.
4. Type information in the text boxes, or select from a list.

   The changes appear in bold.
5. On the VLAN Manager toolbar, click **Apply Changes**.

## Deleting an Avaya Spanning Tree Group

Perform the following procedure to delete an Avaya Spanning Tree Group.

### Procedure steps

1. In the navigation pane, select an Avaya STG folder (except STG 1).
2. On the VLAN Manager toolbar, click **Delete**.

3. Click **+** to open the Avaya STG dialog to add members you want to delete.
4. Click **Yes** to confirm the deletion, or **No** to cancel the deletion, and return to the table view.

## Adding members to an Avaya Spanning Tree Group

Perform the following procedure to add members to an existing Avaya Spanning Tree Group.

### Procedure steps

1. In the Navigation pane, under an existing Avaya STG, click the Members folder.
2. Click **+** to open the Avaya STG dialog dialog to add members you want to add.
3. Select the desired additional members from the device list.
4. Insert values or select options in the option boxes, as required.
5. Click **Save**.

   The new members are added to the Avaya STG.

## Deleting members from an Avaya Spanning Tree Group

Perform the following procedure to delete members from an existing Avaya Spanning Tree Group.

### Procedure steps

1. In the Navigation pane, under an existing Avaya STG, click the **Members** folder.
2. In the contents pane, select the device to remove.
3. On the VLAN Manager toolbar, click **Delete**.
4. Click **Yes** to confirm the deletion, or **No** to cancel the deletion, and return to the table view.

## Editing Avaya Spanning Tree Group port membership

Perform the following procedure to edit port membership in an Avaya Spanning Tree Group.

**Note:**
The VLAN Manager does not support the configuration of port members through the Edit screen for spbm-bvlan-based VLANs.

### Procedure steps

1. From the navigation tree, select the Avaya STG folder.
2. Click **Members**.
3. In the contents pane, the port members for each device in the Avaya STG appear.
4. To change the port membership for a device, click the associated **PortMembers** entry, and choose the ports to include.
5. On the Contents pane toolbar, click **Apply Changes**.

# Creating and configuring VLANs for an Avaya STG

When you create VLANs for an Avaya STG using the VLAN Manager, follow these rules:

- VLANs must have unique VLAN IDs and names.
- Trunk (tagged) ports can belong to multiple VLANs and multiple Spanning Tree Groups.
- VLANs cannot belong to multiple Spanning Tree Groups.
- An access (untagged) port can belong to one and only one port-based VLAN or it can belong to one and only one policy-based VLAN for the given protocol.
- If you enable tagging on a port that is in a VLAN, the Spanning Tree Group configuration for that port is lost.
- A frame VLAN membership is determined by the following order of precedence:
  - VLAN ID
  - Source MAC-based VLAN
  - IP subnet-based VLAN
  - Protocol-based VLAN
  - Port-based VLAN
  - ID-based VLAN
  - spbm-bvlan-based VLAN

The following sections describe how to create and configure each of the different types of VLAN supported by COM.


- Creating a port based VLAN on page 41
- Creating a subnet based VLAN on page 43
- Creating a protocol based VLAN on page 45

## Creating a port based VLAN

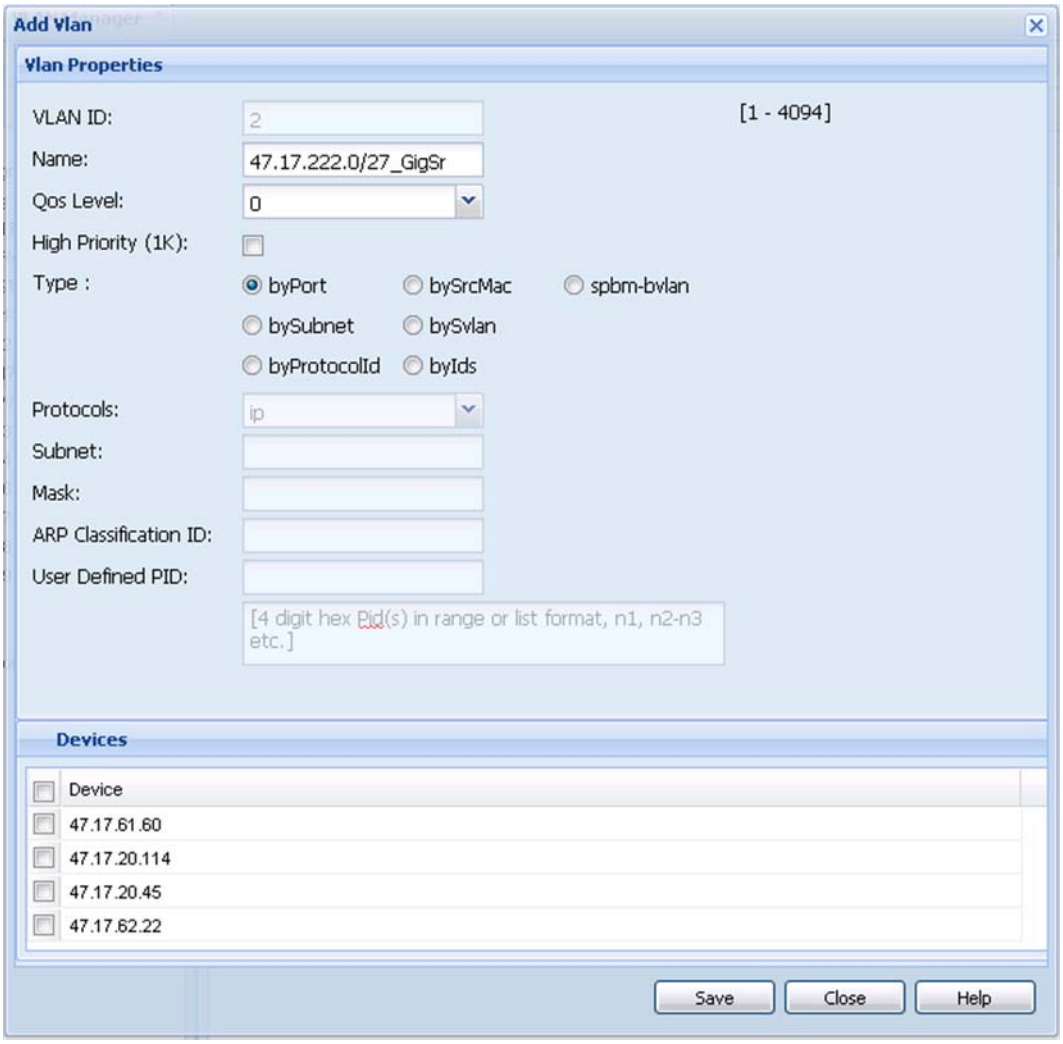
Perform the following procedure to create a port based VLAN.

### Procedure steps

1. From the Navigation tree, expand **Network** folder, and then select **Avaya STGs** folder.
2. Select **STG**.

   The General tab appears in the contents pane and displays the VLAN table.
3. Select a device in the Content pane.
4. Click **Add** to insert a port based VLAN.

   The Add Vlan dialog box appears.




5. In the **VLAN ID** field, type the VLAN ID. The value can be from 1 to 4094, as long as it is not already in use.
6. In the **Name** field, type the VLAN name (optional). If no name is entered, a default is created.
7. For an Ethernet Routing Switch 8600, select the **QoS Level** .
8. For Passport 1000 Series switch, specify whether the VLAN traffic will be tagged as **High Priority (1K)**.
9. From the **Type** field, select the **byPort** type option.

   Other items in the dialog box that apply to a port-based VLAN are activated.
10. Select the devices to be configured from the Device pane.

**Important:**

Not all VLAN types are available on all devices that COM supports. Devices that do not support port-based VLANs will be absent from the device list.

11. Click **Save** to save all the changes.

## Creating a subnet based VLAN

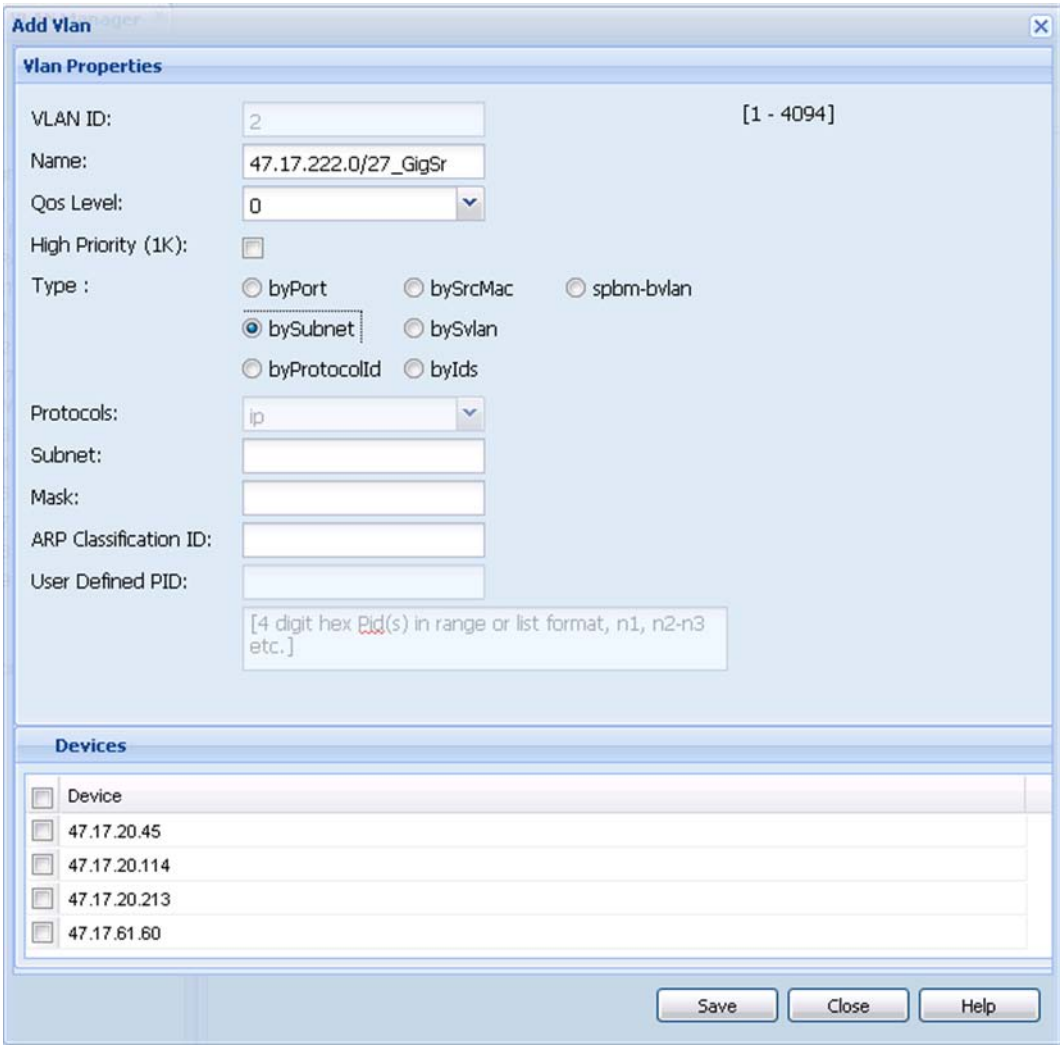
Perform the following procedure to create a subnet based VLAN.

### Procedure steps

1. From the Navigation tree, expand **Network** folder, and then select **Avaya STGs** folder.
2. Select **STG**.

   The General tab appears in the contents pane and displays the VLAN table.
3. Select a device in the Content pane.
4. Click **Add** to insert a subnet based VLAN.

   The Add Vlan dialog box appears.




5. In the **VLAN ID** field, type the VLAN ID. The value can be from 1 to 4094, as long as it is not already in use.
6. In the **Name** field, type the VLAN name (optional). If no name is entered, a default is created.
7. For an Ethernet Routing Switch 8600 or VSP 9xxx, select the **QoS Level** .
8. For Passport 1000 Series switch, specify whether the VLAN traffic will be tagged as **High Priority (1K)**.
9. From the **Type** field, select the **bySubnet** type option.

   Other items in the dialog box that apply to a subnet-based VLAN are activated.
10. In the **Subnet** field, type the source IP subnet address.
11. In the **Mask** field, type the IP subnet mask.
12. In the **ARP-Classification-Id** field, type the ARP classification ID.

**Important:**

The value is 0, if swL2StaticVlanType is not byIpSubnet(2). The range of the object is between 1 and 4094, if swL2StaticVlanType is byIpSubnet(2). This object is useful when the first IpSubnet entry is created and it does not allow to modify.

13. Select the devices to be configured from the Device pane.

**Important:**

Not all VLAN types are available on all devices that COM supports. Devices that do not support subnet-based VLANs will be absent from the device list.

14. Click **Save** to save all the changes.

## Creating a protocol based VLAN

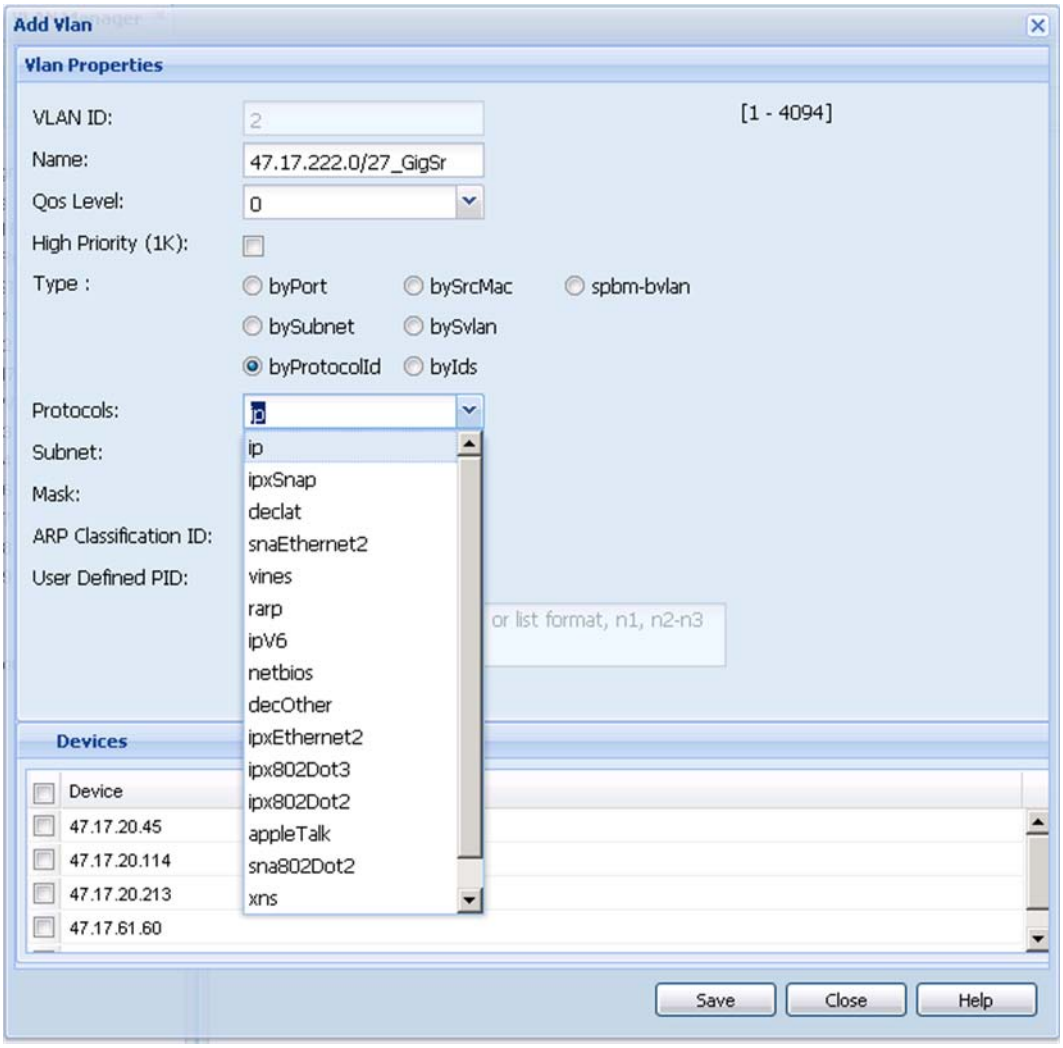
Perform the following procedure to create a protocol based VLAN.

### Procedure steps

1. From the Navigation tree, expand **Network** folder, and then select **Avaya STGs** folder.
2. Select **STG**.

   The General tab appears in the contents pane and displays the VLAN table.
3. Select a device in the Content pane.
4. Click **Add** to insert a protocol based VLAN.

   The Add Vlan dialog box appears.




5. In the **VLAN ID** field, type the VLAN ID. The value can be from 1 to 4094, as long as it is not already in use.
6. In the **Name** field, type the VLAN name (optional). If no name is entered, a default is created.
7. For an Ethernet Routing Switch 8600 or VSP 9xxx, select the **QoS Level** .
8. For Passport 1000 Series switch, specify whether the VLAN traffic will be tagged as **High Priority (1K)**.
9. From the **Type** field, select the **byProtocolId** type option.

   Other items in the dialog box that apply to a protocol Id based VLAN are activated.
10. In the **Protocol** field, select the required protocol from the drop-down list.
11. Select the devices to be configured from the Device pane.

**Important:**

Not all VLAN types are available on all devices that COM supports. Devices that do not support protocol Id based VLANs will be absent from the device list.

12. Click **Save** to save all the changes.

## Creating a source MAC address based VLAN

Perform the following procedure to create a source MAC address based VLAN.

### Procedure steps

1. From the Navigation tree, expand **Network** folder, and then select **Avaya STGs** folder.
2. Select **STG**.

   The General tab appears in the contents pane and displays the VLAN table.
3. Select a device in the Content pane.
4. Click **Add** to insert a source MAC address based VLAN.

   The Add Vlan dialog box appears.
5. In the **VLAN ID** field, type the VLAN ID. The value can be from 1 to 4094, as long as it is not already in use.
6. In the **Name** field, type the VLAN name (optional). If no name is entered, a default is created.
7. For an Ethernet Routing Switch 8600 or VSP 9xxx, select the **QoS Level** .
8. For Passport 1000 Series switch, specify whether the VLAN traffic will be tagged as **High Priority (1K)**.
9. From the **Type** field, select the bySrcMac type option.

   Other items in the dialog box that apply to a source MAC address based VLAN are activated.
10. Select the devices to be configured from the Device pane.

    **Important:**

    Not all VLAN types are available on all devices that COM supports. Devices that do not support source MAC address based VLANs will be absent from the device list.
11. Click **Save** to save all the changes.

## Creating a sVLAN based VLAN

Perform the following procedure to create a sVLAN based VLAN.

### Procedure steps

1. From the Navigation tree, expand **Network** folder, and then select **Avaya STGs** folder.
2. Select **STG**.

   The General tab appears in the contents pane and displays the VLAN table.
3. Select a device in the Content pane.
4. Click **Add** to insert a sVLAN based VLAN.

   The Add Vlan dialog box appears.
5. In the **VLAN ID** field, type the VLAN ID. The value can be from 1 to 4094, as long as it is not already in use.
6. In the **Name** field, type the VLAN name (optional). If no name is entered, a default is created.
7. For an Ethernet Routing Switch 8600, select the **QoS Level** .
8. For Passport 1000 Series switch, specify whether the VLAN traffic will be tagged as **High Priority (1K)**.
9. From the **Type** field, select the **bySvlan** type option.

   Other items in the dialog box that apply to a Svlan-based VLAN are activated.
10. Select the devices to be configured from the Device pane.

    **Important:**
    Not all VLAN types are available on all devices that COM supports. Devices that do not support Svlan-based VLANs will be absent from the device list.
11. Click **Save** to save all the changes.

## Creating an ID based VLAN

Perform the following procedure to create an ID based VLAN.

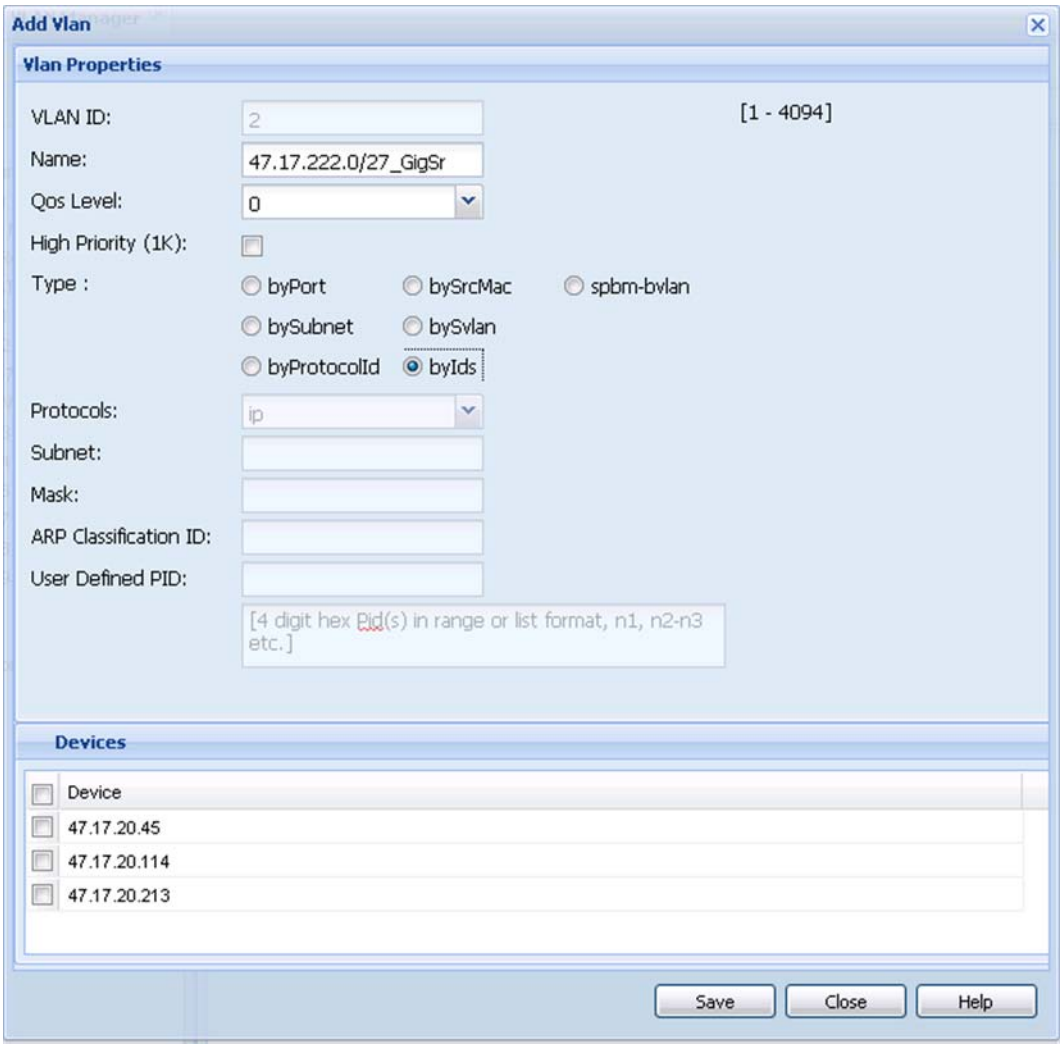
### Procedure steps

1. From the Navigation tree, expand **Network** folder, and then select **Avaya STGs** folder.
2. Select **STG**.

The General tab appears in the contents pane and displays the VLAN table.

3. Select a device in the Content pane.
4. Click **Add** to insert an ID based VLAN.

   The Add Vlan dialog box appears.




5. In the **VLAN ID** field, type the VLAN ID. The value can be from 1 to 4094, as long as it is not already in use.
6. In the **Name** field, type the VLAN name (optional). If no name is entered, a default is created.
7. For an Ethernet Routing Switch 8600, select the **QoS Level** .
8. For Passport 1000 Series switch, specify whether the VLAN traffic will be tagged as **High Priority (1K)**.
9. From the **Type** field, select the **byIds** type option.

   Other items in the dialog box that apply to a ID based VLAN are activated.

10. Select the devices to be configured from the Device pane.

**Important:**
Not all VLAN types are available on all devices that COM supports. Devices that do not support ID based VLANs will be absent from the device list.

11. Click **Save** to save all the changes.

## Creating an spbm—based VLAN

Perform the following procedure to create an spbm—based VLAN.

### Prerequisites

- ERS 8600/8800 v 7.1 switch
- mib attribute rcPlsbGlobalEnable set to true.

### Procedure steps

1. From the Navigation tree, expand **Network** folder, and then select **Avaya STGs** folder.
2. Select the required STG.

   The General tab appears in the contents pane and displays the VLAN table.
3. Select a device in the Content pane.
4. To insert an spbm— based VLAN, click **Add**.

   The Add Vlan dialog box appears.
5. In the **VLAN ID** field, type the VLAN ID. The value can be from 1 to 4094, as long as it is not already in use.
6. In the **Name** field, type the VLAN name (optional). If no name is entered, a default is created.
7. For an Ethernet Routing Switch 8600, select the **QoS Level**.
8. For Passport 1000 Series switch, specify whether the VLAN traffic will be tagged as **High Priority (1K)**.
9. From the **Type** field, select the **spbm** type option.

   Other items in the dialog box that apply to a port-based VLAN are activated.
10. Select the devices to be configured from the Device pane.

**Note:**
Not all VLAN types are available on all devices that COM supports. Devices that do not support port-based VLANs will be absent from the device list.

11. Click **Save** to save all the changes.

## Job aid

The following table describes the fields in the Add Vlan dialog box.

| Field | Description |
|---|---|
| VLAN ID | The VLAN ID. |
| Name | VLAN name |
| QosLevel | In an Ethernet Routing Switch 8000 Series you can set the Quality of Service (QoS) level for traffic in the VLAN to a level between 0 and 7. |
| HighPriority | In a Passport 1000 Series switch, you can select HighPriority mode for all traffic in the VLAN. |
| Type | Type by which you want to add the device. Options:<br>• by port<br>• by subnet<br>• by protocol<br>• by source MAC Address<br>• by SVLANs<br>• by ID<br>• by spbm |
| Protocols | Type of protocol. |
| Subnet | The source IP subnet address. |
| Mask | The IP subnet mask. |
| ARP Classification ID | The ARP classification ID. |
| User Defined PID | The user defined PID. |
| Devices | List of devices. |

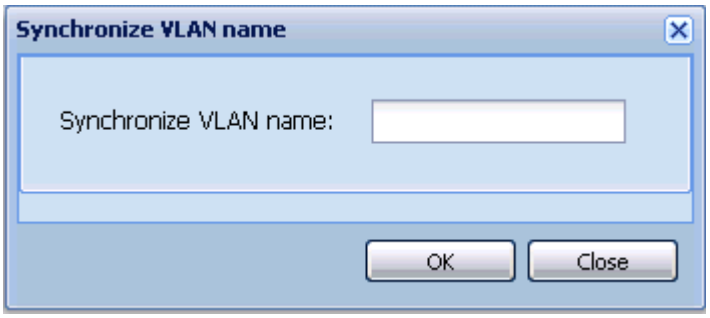
## Synchronizing VLAN name

Perform the following procedure to synchronize the VLAN name.

### Procedure steps

1. From the Navigation tree, select **Default (1)**.
2. Click **Synchronize VLAN Name** button on the content pane toolbar.

The Synchronize VLAN name dialog box appears.




3. In the **Synchronize VLAN name** field, type the VLAN name.
4. Click **OK**.

# Managing Rapid Spanning Tree Protocol

The following sections describe how to edit Rapid Spanning Tree Protocol (RSTP) instances and provide information about RSTP membership.

Configuring RSTP properties on page 52

**Note:**
Rapid Spanning Tree Protocol does not support spbm-bvlan VLAN type.

## Configuring RSTP properties

Perform the following procedure to configure RSTP properties.

### Procedure steps

1. From the navigation tree, select the **RSTP** folder.
2. Select the **Rapid STG** folder and select the **Config** item.
3. In the contents pane, click the item that you want to edit.

   The field is highlighted, and you can edit directly in the table.
4. Type information in the text boxes, or select from a list.

   The changes appear in bold.
5. On the VLAN Manager toolbar, click **Apply Changes**.

# Creating and configuring VLANs for Rapid Spanning Tree Protocol

The following sections topics describe how to create and configure VLANs for Rapid Spanning Tree Protocol (RSTP) instances:



**Note:**
Rapid Spanning Tree Protocol does not support spbm-bvlan VLAN type.

## Adding a VLAN to the Rapid Spanning Tree

Perform the following procedure to add a VLAN for RSTP.

### Procedure steps

1. From the navigation tree, select the **RSTP** folder.
2. Select the **Rapid STG** folder and do one of the following:
    a. From the VLAN Manager menu bar, choose **Edit > Insert**.
    b. On the VLAN Manager toolbar, click **Insert**.

    The New VLAN dialog box appears.
3. Insert values or select options in the option boxes.
4. Click **Ok**.

## Deleting a VLAN from the Rapid Spanning Tree

Perform the following procedure to delete a VLAN from RSTP.

### Procedure steps

1. In the navigation pane, select a VLAN from the **Rapid STG** folder and do one of the following:
    a. From the VLAN Manager menu bar, choose **Edit > Delete**.
    b. On the VLAN Manager toolbar, click **Delete**.

The Delete dialog box appears.

2. Click **Yes** to confirm the deletion of the VLAN.

## Adding members to a VLAN group in Rapid Spanning Tree

Perform the following procedure to add members to a VLAN group in RSTP.

### Procedure steps

1. From the navigation pane, under a Rapid STG group, select the VLAN to which you want to add a member.
2. Do one of the following:
    a. From the VLAN Manager menu bar, choose **Edit > Insert**.
    b. On the VLAN Manager toolbar, click **Insert**.

    The Add VLAN dialog box appears.
3. Select the additional members from the device list.
4. Insert the values or select the options as required.
5. Click **OK**.

# Managing Multiple Spanning Tree Protocol instances

The following sections topics describe how to add and delete Multiple Spanning Tree Protocol (MSTP) instances and provide information about MSTP membership:

### Navigation


- Adding an MSTI in Multiple Spanning Tree on page 54
- Deleting an MSTI on page 55
- Adding port members on page 55
- Editing MSTP properties on page 55


## Adding an MSTI in Multiple Spanning Tree

Perform the following procedure to add an MSTI instance.

### Procedure steps

1. From the navigation tree, select the **MSTP** folder.
2. On the VLAN Manager toolbar, click **Add**.

The **Add MSTP** dialog box appears.

3. In the **Id** field, enter the desired MSTI identifier.
4. Select the **Devices** required for the MSTP.
5. Click **Save**.

## Deleting an MSTI

Perform the following procedure to delete an MSTI instance.

### Procedure steps

1. In the Navigation pane, under the **MSTP** folder, select the MSTI instance to delete
2. On the VLAN Manager toolbar, click **Delete**.
3. Click **Yes** to confirm the deletion, or **No** to cancel the deletion, and return to the table view.

## Adding port members

Perform the following procedure to add ports to an MSTI or CIST.

### Procedure steps

1. In the **Port Members** table, select a device in the list.
2. Click in the **PortMembers** cell for the device to which you want to add port membership.

   The PortMembers dialog box appears .


3. Select the port number(s).
4. Click **Save**.

## Editing MSTP properties

Perform the following procedure to edit the MSTP properties.

### Procedure steps

1. In the Navigation pane, select the **CIST** folder.
2. To edit the MSTP properties, choose the **MSTP** tab.
3. To edit the CIST properties, choose the **CIST** tab.
4. To edit the MSTI Region properties, choose the `MSTI Region` tab.
5. In the contents pane, click the item that you want to edit.

   The field is highlighted, and you can edit directly in the table.
6. Type information in the text boxes, or select from a list.

   The changes appear in bold.
7. On the VLAN Manager toolbar, click **Apply Changes**.

# Managing VLANs for MSTP

The following sections topics describe how to create and delete VLANs for Multiple Spanning Tree Protocol (MSTP) instances, as well as hpw to add memberts to a VLAN group.


- Adding a VLAN in Multiple Spanning Tree on page 56
- Deleting a VLAN in Multiple Spanning Tree on page 57
- Adding members to a VLAN in Multiple Spanning Tree on page 58

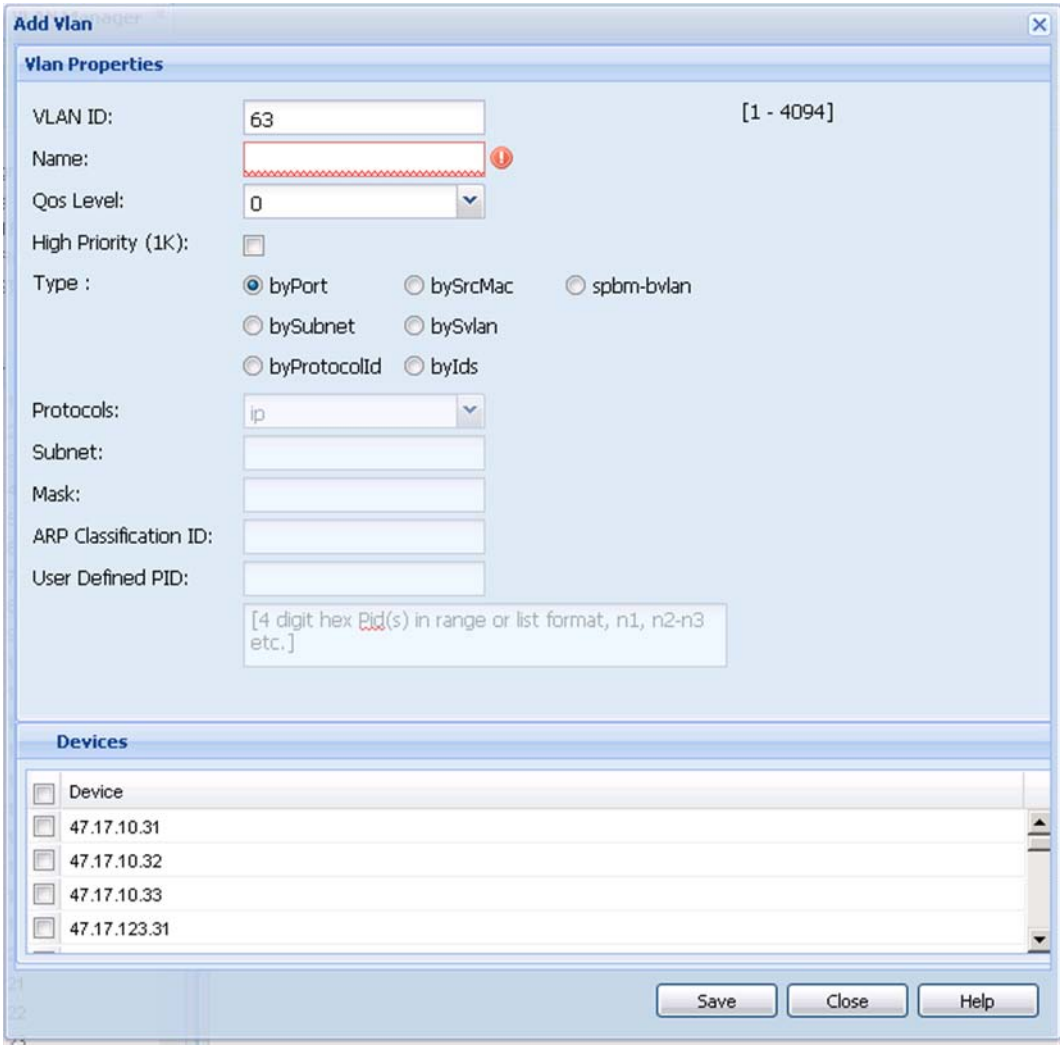

## Adding a VLAN in Multiple Spanning Tree

Perform the following procedure to add a VLAN to the CIST or MSTI.

### Procedure steps

1. From the navigation tree, select the **MSTP** folder.
2. Select the **CIST** folder or an **MSTI** folder.
3. On the VLAN Manager toolbar, click **Add**.

   The **Add VLAN** dialog box appears.




4. Insert values or select options in the option boxes.
5. Click **Save**.

## Deleting a VLAN in Multiple Spanning Tree

Perform the following procedure to delete a VLAN in Multiple Spanning Tree.

### Procedure steps

1. In the Navigation pane, under the **CIST** or **MSTI** folder, select the VLAN to delete.
2. On the VLAN Manager toolbar, click **Delete**.
3. Click **Yes** to confirm the deletion, or **No** to cancel the deletion, and return to the table view.

## Adding members to a VLAN in Multiple Spanning Tree

Perform the following procedure to add members to a VLAN in Multiple Spanning Tree.

### Procedure steps

1. From the Navigation pane, under an STG group, select the VLAN to which you want to add a member.
2. On the VLAN Manager toolbar, click **Add**.

   The Add VLAN dialog box appears.
3. Select the additional members from the device list.
4. Insert the values or select the options as required.
5. Click **Save**.

# Configuring port members

This section provides information about the port membership types supported in COM, and how to use VLAN Manager to configure them. For information about how to view port membership, including viewing unassigned ports, see Viewing port membership information on page 82

This section contains the following topics:



## Port membership types

In the Navigation pane, the four tables represent the various port memberships described in the following table.

**Table 11: Port membership types and STGs**

| Port type | Description |
|---|---|
| Unassigned | A port that does not belong to any STG. If no devices in the network contain unassigned ports, a table does not appear in the contents pane. For more information, see Viewing the unassigned ports on page 82. |

| Port type | Description |
|---|---|
| Tagging | A port that has tagging enabled and can belong to multiple STGs. If a tagged frame is received on a tagged port, with a VLAN ID specified in the tag, the switch directs it to that VLAN, if it is present. For more information, see Viewing tagged ports on page 83. |
| Isolated Routing Port (IRP) | A port that can only route IP packets and does not belong to any STG or VLAN. For more information, see Viewing isolated router ports on page 84. |
| Bridge Routing (brouter ports) | A port that can route IP packets as well as bridge all non routable traffic. The routing interface is not subjected to the Spanning Tree Protocol. For more information, see Viewing bridge routing ports on page 85. |

## Adding port members

Perform the following procedure to add port members.

### Procedure steps

1. In the **Port Members** table, select a device in the list.
2. Click in the **PortMembers** cell for the device to which you want to add port membership.
3. Select the port number(s).
4. Click **Save**.

## Adding tagged ports

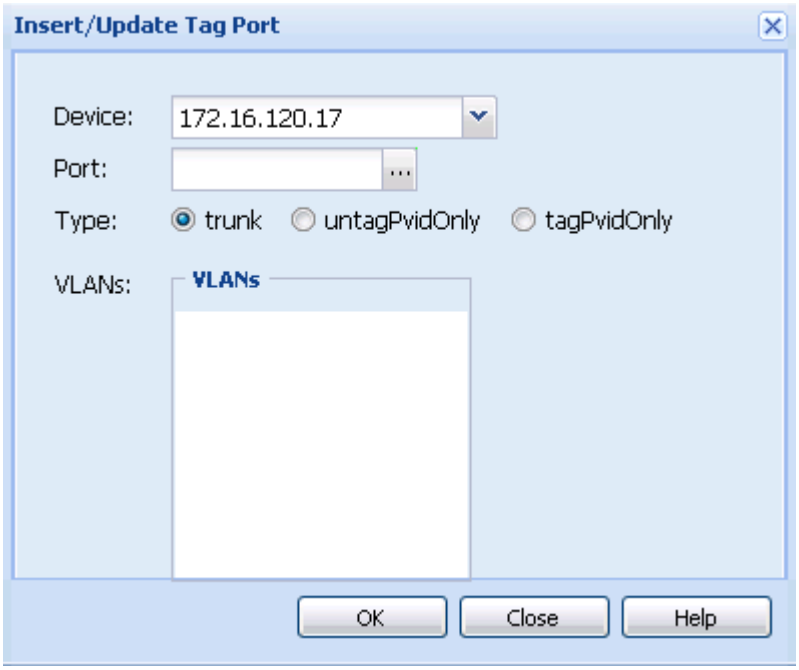
Perform the following procedure to add tagged ports.

### Procedure steps

1. In the Navigation pane, select **Tagging**.

   The Tagging Ports table appears in the contents pane.
2. Click **Add**.

   The Insert/Update Tag Port dialog box appears.




3. Select the **Device** address you want to add.
4. Click the **Port** ellipsis button. The ports for the selected device appears.
5. Select the port you want to use.
6. Click **Save**. The ports dialog box closes.
7. Select the VLAN available on the selected device.
8. Click **OK**. An Operation Result dialog box appears when the addition is complete.
9. Click **OK**. The Operation Result dialog box closes and the added port is visible in the Content pane.

## Job aid

The following table describes the fields in the Tagging Ports table.

| Field | Description |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Port | Port on which tagging is enabled. |
| Type | Type of port: trunk or untagPvidOnly or tagPvidOnly. |
| VlanIds | VLAN IDs of which the port is a member. |

# Configuring routing on a VLAN interface

VLAN Manager allows you to configure certain routing interfaces. For more information, see the following topics:.



## Enabling OSPF on a VLAN interface

You can use VLAN Manager to enable and disable OSPF routing on a VLAN interface.

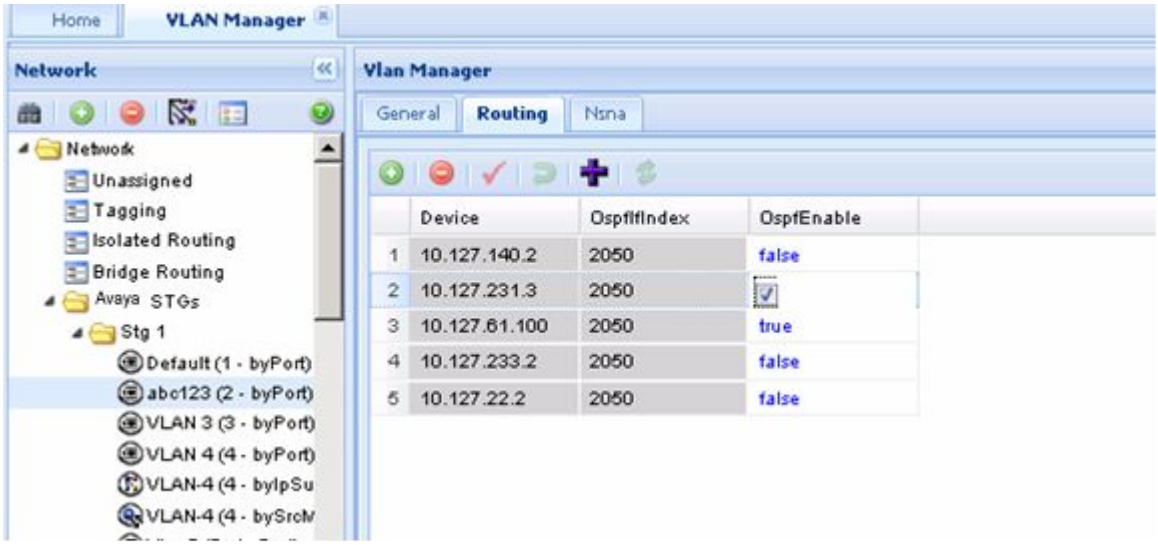
Perform the following procedure to enable OSPF routing on a VLAN interface.

### Procedure steps

1. In the Navigation pane, select a VLAN.

   The General tab appears in the contents pane and displays the VLAN table.
2. Click the **Routing** tab.

   The Routing tab appears in the contents pane.




3. In the **OspfEnable** field, choose **true** to enable OSPF on this VLAN.
4. Click **Apply Changes**.

## Inserting a VRRP interface on a VLAN

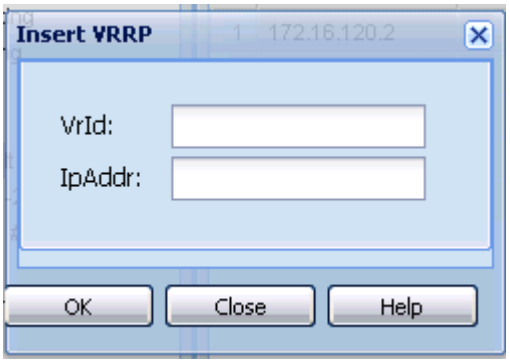
You can use VLAN Manager to insert a VRRP routing interface for a VLAN. Before inserting the VRRP interface, ensure the VLAN has an assigned IP address for routing. Perform the following procedure to insert a VRRP interface on a VLAN.

### Procedure steps

1. In the Navigation pane, select a VLAN.

   The General tab appears in the contents pane and displays the VLAN table.
2. Select a device that supports VRRP.
3. Click **Add Vrrp** button (+ sign).

   The Insert VRRP dialog box appears.




4. In the **VrId** and **IpAddr** field, enter the Virtual Router ID and IP address for the VRRP interface.
5. Click **Ok**.

   The new VRRP interface appears in Routing Manager under the VRRP Interfaces folder.

# Domain synchronization

Domain synchronization allows you to distribute the VLAN configuration from one device, called the server node, to other devices in your network. Domain synchronization synchronizes the VLANs between the same spanning tree mode devices.

With domain synchronization you can:

- select any subset of devices to be part of the synchronization domain (sync domain)
- synchronize to any subset of the VLANs of the server node

- add new server node VLANs
- delete or modify existing server node VLANs

To apply domain synchronization to your network, first gain familiarity with the domain synchronization interfaces and then perform the appropriate procedures. The following list provides links to the information you require:



# Domain synchronization interfaces

There are three domain synchronization interfaces to become familiar with before performing the related procedures:

- Sync Domain interface on page 63

  Use the Sync Domain interface to define a new sync domain or to modify an existing sync domain.

- New server node VLAN interface on page 65

  Use the New VLAN interface to add a new VLAN to the server node.

- IP Address and Net Mask interfaces on page 67

  Use the IP Address and Net Mask interfaces to review and change the IP addresses and network masks of domain members.

## Sync Domain interface

The figure below shows the Sync Domain interface which you use to define a new sync domain or modify an existing sync domain. The table that follows the figure describes the elements of the interface. Relevant procedures follow the table.

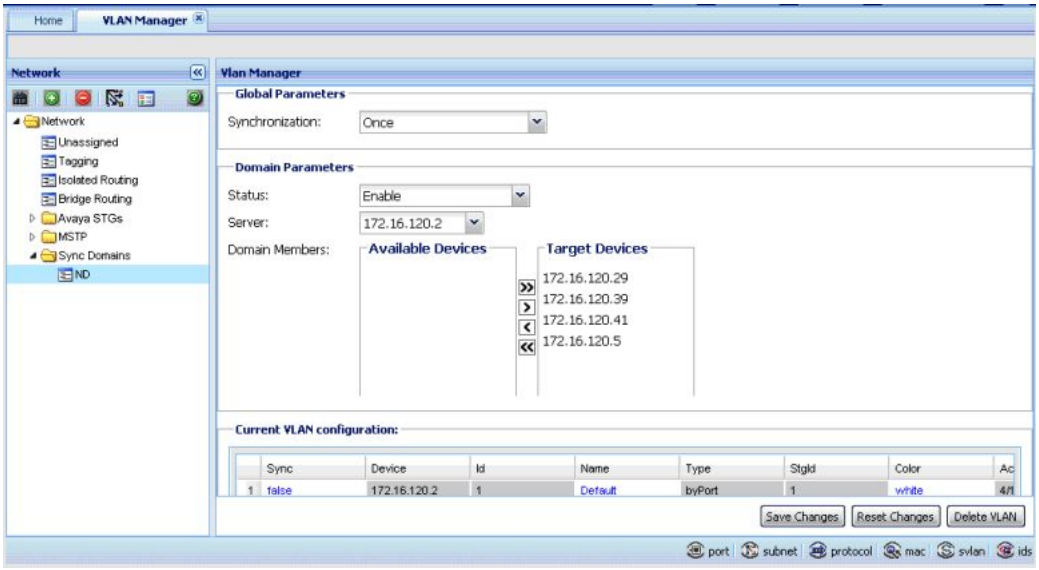



**Figure 5: Sync Domain interface**

## Table 12: Sync Domain interface elements

| Field | Description |
|---|---|
| Sync Domain name | The name of a sync domain can include any printable character to a maximum of 32 characters. |
| Global Parameters | Global parameters apply to all sync domains. |
| Synchronization | Synchronization is a global parameter. There are two synchronization options:<br>• Once<br>Synchronization occurs when you save the domain by clicking **Save Changes**.<br>• Configuration change in VM<br>Synchronization occurs if any server node configurations are changed in VLAN Manager. |
| Domain Parameters | Domain parameters only apply to the specific sync domain whose Sync Domain interface is open. |
| Status | **Enable** activates the sync domain. Synchronization does not occur when the status is **Disable**, regardless of the global parameters. |
| Server Node | The VLAN configurations of the server node provide the synchronization source. You select the server node from a list of all devices in your network that are discovered by VLAN Manager. |
| Domain Members | Domain members are the devices whose VLANs are synchronized to the server node. You select these target |

| Field | Description |
|---|---|
| | devices from a list of available devices. The list is generated by filtering the devices discovered by VLAN Manager using the server node's spanning tree mode. |
| Current VLAN Configuration | A table where each row is dedicated to one server node VLAN. The columns of the table display VLAN attributes. |
| Current VLAN Configuration table, Sync | The Sync attribute is unique to domain synchronization. The VLAN configuration is distributed to domain members only when Sync is **True**, regardless of any other synchronization settings.<br>Sync is **False** for all VLANs when the sync domain is created. |
| Current VLAN Configuration table, IP Address | The IP address of the server node is displayed. For information on the IP addresses used for domain members, see IP Address and Net Mask interfaces on page 67. |
| Current VLAN Configuration table, Net Mask | The network mask of the server node VLAN is displayed. For information on the network masks for domain members, see IP Address and Net Mask interfaces on page 67. |
| Current VLAN Configuration table, Other columns | These are standard VLAN attributes. |
| Save Changes | Pressing **Save Changes** saves any changes you have made to the sync domain definition or to server node VLAN configurations. If **Once** is selected as a synchronization option, then domain members are synchronized now. Domain members are also synchronized if you changed any server node VLAN configurations. |
| Reset Changes | Pressing **Reset Changes** removes all changes made since the last **Save Changes**. |
| View Log | Click View Log to view the sync domain log file, syncDomains.log. |
| Help | Pressing **Help** invokes on-line help for the Sync Domain interface. |

## New server node VLAN interface

The figure below shows the New VLAN interface which you use to add a new VLAN to the server node. The table that follows the figure describes the elements of the interface. Relevant procedures follow the table.

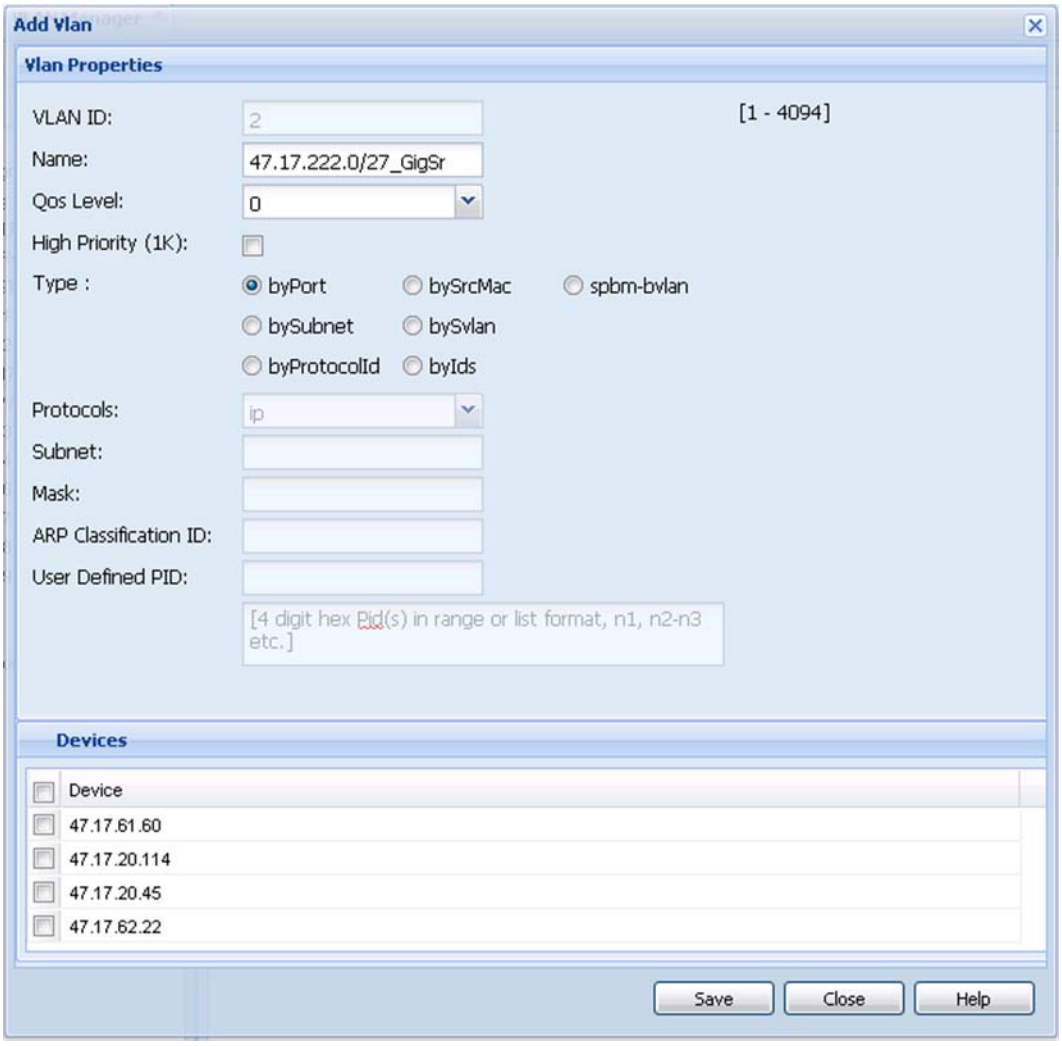



**Table 13: New server node VLAN interface elements**

| Element | Description |
|---|---|
| VLAN Id | This is the identity of the VLAN. VLAN Manager fills this with the next available number but you can change it. The VLAN Id ranges from 1 to 4094. |
| Name | You enter a name for the VLAN. |
| QOS Level | You can select from levels 0 through 7. |
| High Priority (1K) | You can choose to activate this, or leave unselected. |
| Type | You can choose byPort or byProtocolId. If byProtocolId is chosen, then you can change the default ProtocolId from ip to one of 15 other options. |

| Element | Description |
|---|---|
| Subnet, Mask, ARP-Classi-fication-Id, UsrDefined PId | One or more of these fields may be enabled, depending on the ProtocolId. |
| IP Address | You enter the IP address of the VLAN. |
| Net Mask | You enter the network mask of the VLAN. |
| Save | Press this button to create the new VLAN. The New VLAN interface closes and the VLAN appears in the Current VLAN Configuration table on the Sync Domain interface. |
| Close | Press Close to cancel any changes you have made and close the interface. |
| Help | This button invokes online help for the New VLAN interface. |

## IP Address and Net Mask interfaces

When a sync domain is created, all VLANs of the server node are listed in the Sync Domain interface. The IP address and network mask of each of these VLANs is provided in the Current VLAN Configuration table (see Table 12: Sync Domain interface elements on page 64 for details).

VLAN Manager generates IP addresses and network masks for domain member VLANs from the IP address and network mask of the server node VLAN. You access these generated values by double-clicking the IP address or network mask cell of the Current VLAN Configuration table. You can use these interfaces to review and change the IP addresses and network masks of domain members.

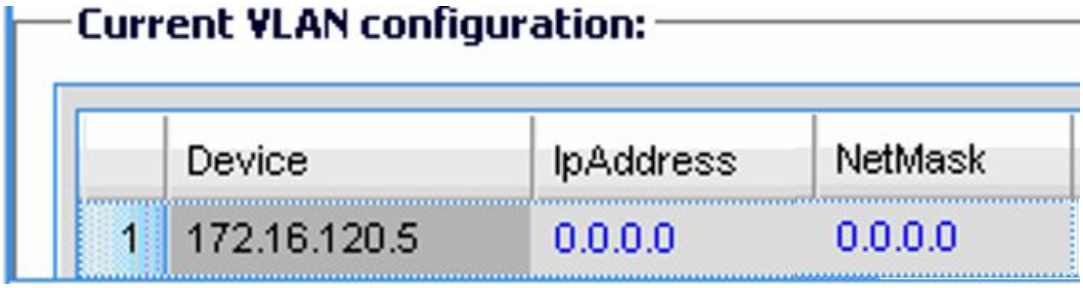



**Figure 6: IPAdress and NetMask interfaces**

### IP Address interface

VLAN Manager generates IP addresses for domain member VLANs by incrementing the IP address of the server node VLAN, as shown in the figure of the IP Address interface, above.

If the IP address is black, the IP address is available at the device. If the IP address is red, the IP address is not available. You can enter IP addresses manually; VLAN Manager looks for available IP addresses at the devices and assigns those IP addresses. If an IP address is not available, the entry defaults to 0.0.0.0.

**Save changes**: When you press **Save changes**, any changes you have made are saved and the interface closes.

**Reset changes**: When you press **Reset changes**, any changes you have made are discarded and the interface closes.

### Net Mask interface

VLAN Manager generates network masks for domain member VLANs by duplicating the network mask of the server node VLAN, as shown in the figure of the **Net Mask** interface, above.

If the network mask is black, the mask is available at the device. If the network mask is red, the network mask is not available. You can enter network masks manually. If a network mask is not available, the entry defaults to 0.0.0.0.

**Save changes** and **Reset changes** for the Net Mask interface are the same as described for the IP Address interface.

**Important:**
If the IP address and a network mask are not available at the device, the VLAN is synchronized except for the IP address and network mask.

## Domain synchronization procedures

You can create any number of sync domains. In addition to creating sync domains, you can add a new VLAN to the server node, modify the settings for an existing sync domain, change the attributes of an existing VLAN, and delete a sync domain or a server node VLAN. The domain synchronization procedures are:


- Creating a sync domain on page 68
- Adding a VLAN to a sync domain server node on page 69
- Modifying a sync domain on page 70
- Modifying a sync domain server node VLAN on page 71
- Deleting a sync domain on page 72
- Deleting a server node VLAN on page 72


## Creating a sync domain

Perform this procedure to create a new sync domain. This procedure does not provide instructions for adding a new VLAN to the server node; those instructions are provided by Adding a VLAN to a sync domain server node on page 69.

### Prerequisites

Familiarity with the Sync Domain interface is required for this procedure. See Sync Domain interface on page 63 for more details.

### Procedure steps

1. Start VLAN Manager.
2. Select (single click) **Sync Domains**.
3. From the toolbar, click the plus (+) sign.

   The New Sync Domain dialog box appears.
4. In the Domain Name field, type a name for the new sync domain.
5. Click **Save**.

   The Sync Domain interface appears.
6. In the **Global Parameters** region, select the required synchronization option.
7. In the **Domain Parameters** region, select **Enable**.
8. From the **Server** list, click the down arrow to expand the list and select the node you want as the server node.
9. To add devices to the domain, do one of the following:
   - To add one device, select it from the **Available devices** list and click **>>** to move it to the **Target devices** list.
   - To add several devices, hold down the Ctrl key, click on each device in the **Available devices** list, release the Ctrl key, and click **>>** to move the devices to the **Target devices** list.
   - To add a contiguous block of devices, hold down the Shift key, click on the first device in the **Available devices** list, click on the last device, release the Shift key, and click **>>** to move the devices to the **Target devices** list.
10. In the **Current VLAN Configuration** table, click the **Sync** entry to change it to **True** for each VLAN that you want to act as a synchronization source.
11. Click **Save Changes**.

## Adding a VLAN to a sync domain server node

Perform the following procedure to add a VLAN to the server node of a sync domain.

### Prerequisites

Familiarity with the New VLAN interface is required for this procedure. See New server node VLAN interface on page 65 for more details.

### Procedure steps

1. Start VLAN Manager.
2. Expand **Sync Domains**.
3. Select the sync domain to which you want to add a VLAN.
4. From the toolbar, click the plus (+) sign.

   The New VLAN interface appears.
5. For **STG Id**, click the down arrow to the right of the **STG Id** field and select the required STG Id from the list.
6. Edit the **Id** field if the assigned number does not meet your requirements.
7. In the **Name** field, type a name for the VLAN.
8. Select the **QOS Level**.
9. For **Type**, if you require byProtocolId, then:
   - In the **Type** area, select **byProtocolId**.
   - In the **ProtocolId** area, select the required **ProtocolId** .
   - If Subnet, Mask, ARP-Classification-Id, or UsrDefinedPId are enabled, change as required.
10. In the **IP Address** field, type the IP address of the VLAN.
11. In the **Net Mask** field, type the net mask of the VLAN.
12. Click **Save**.

    The New VLAN interface closes and the new VLAN appears in the Current VLAN Configuration table.
13. From the Sync Domain interface, click **Save Changes**.

    The SyncDomain Operation Description interface appears.

## Modifying a sync domain

Perform the following procedure to modify an existing sync domain. This procedure does not provide instructions for modifying a server node VLAN; those instructions are provided by Modifying a sync domain server node VLAN on page 71.

### Prerequisites

Familiarity with Creating a sync domain on page 68 is required for this procedure.

### Procedure steps

1. Start VLAN Manager.
2. Expand **Sync Domains**.
3. Select the required sync domain.
4. Modify the **Global Parameters** as required.

   Global parameters apply to all sync domains.
5. Change the **Status** and **Server** as required.
6. For **Domain Members**, use **>** and **>>** to add members to the domain and use **<** and **<<** to remove members from the domain.
7. In the **Current VLAN Configuration** table, change the **Sync** entry as required: **True** to synchronize domain members to the VLAN, **False** to remove the VLAN from the sync domain.
8. Click **Save Changes**.

## Modifying a sync domain server node VLAN

Perform the following procedure to modify a VLAN of a device that is acting as a server node for a sync domain.

### Prerequisites

Familiarity with the IP Address and Net Mask interfaces is required for this procedure. See IP Address and Net Mask interfaces on page 67 for details.

### Procedure steps

1. Start VLAN Manager.
2. Expand **Sync Domains**.
3. Select the required sync domain.

   Refer to the **Current VLAN Configuration** table for the remainder of this procedure.
4. To add (**True**) or remove (**False**) the VLAN from the sync domain, toggle the **Sync** field as required.
5. To change the name of the VLAN, edit the **Name** cell.
6. To change the port members, double-click the **PortMembers** cell and click a port number to select or deselect the port.

   A port is selected when the port number is depressed.

7. To change IP addresses, double-click the **IP Address** cell to open the IP Address interface.
8. Modify the IP addresses as required.
9. Click **OK** to save your changes and close the IP Address interface.
10. To change network masks, double-click the **Net Mask** cell to open the Net Mask interface.
11. Modify the network masks as required.
12. Click **OK** to save your changes and close the Net Mask interface.
13. Click **Save Changes**.

    The SyncDomain Operation Description interface appears.

## Deleting a sync domain

Perform the following procedure to delete a sync domain.

### Procedure steps

1. Start VLAN Manager.
2. Expand **Sync Domains**.
3. Select the required sync domain.
4. From the toolbar, click the (**X**) sign or click **Delete VLAN**.
5. Click **Save changes** when asked to confirm the action.

## Deleting a server node VLAN

Perform the following procedure to delete a server node VLAN.

### Procedure steps

1. Start VLAN Manager.
2. Expand **Sync Domains**.
3. Select the required sync domain.
4. In the **Current VLAN Configuration** table, select any cell of the VLAN you want to delete.
5. From the toolbar, click the ex (X) sign or click **Delete VLAN**.
6. Click **Save changes** when asked to confirm the action.

   The VLAN is deleted from the server node. If the sync domain is enabled, the VLAN is also deleted from all domain member devices.

# Viewing STG and VLAN information

You can use VLAN Manager to monitor the status of STGs and VLANs in the network, as well as view information about ports. This section provides information about the following topics:



# Viewing STG information

This section provides information about the following topics:



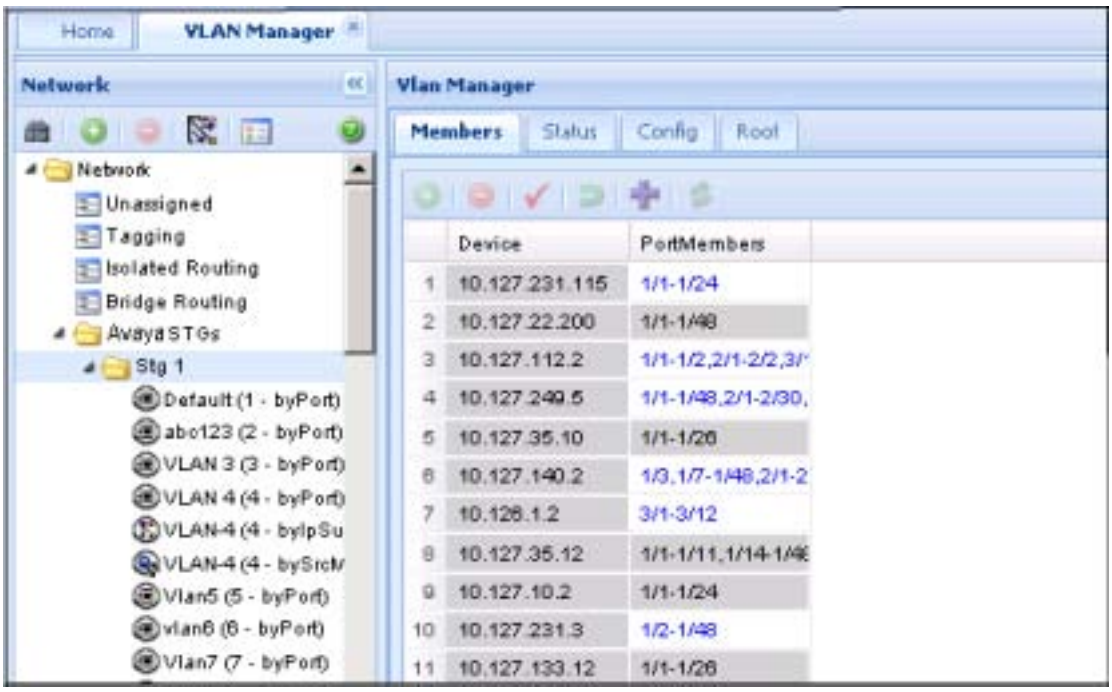
## Viewing Spanning Tree Groups

All devices supported by COM support the IEEE 802.1D Spanning Tree Protocol and at least one instance of a Spanning Tree Group.

Perform the following procedure to view an STG.

### Procedure steps

Open the folder for the STG you want to view.



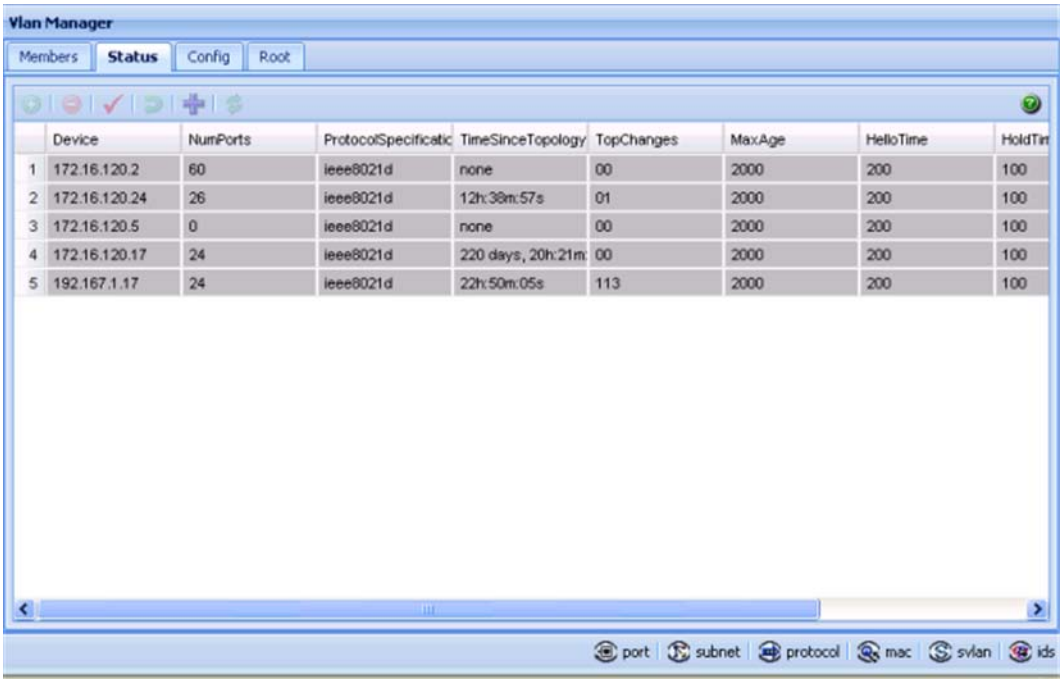

## Viewing STG status

Use the read-only Status table to view the status of the Spanning Tree Protocol for the selected STG that is associated with the network. Perform the following procedure to open the Status table.

### Procedure steps

In the Navigation pane, open an STG and select **Status**.

The Status table appears in contents pane.




## Job aid

The following table describes the fields in the Status table.

| Field | Description |
|---|---|
| Device | IP address of the bridge. |
| NumPorts | Number of ports controlled by this bridging entity. |
| Protocol Specification | An indication of which version of the Spanning Tree Protocol (STP) is operating. The IEEE 802.1d implementations display ieee8021d. |
| TimeSince Topology Change | Time in hundredths of a second since the last time a topology change was detected by the bridge entity or STG. |
| TopChanges | The number of topology changes detected by this bridge since the management entity was last reset or initialized. |
| MaxAge | Maximum age of STP information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that the bridge is currently using. The default value is 2000 (20 seconds). |
| HelloTime | Amount of time in hundredths of a second between transmission of configuration bridge protocol data units (BPDUs) by this device on any port when it is the root of the spanning tree. The default value is 200 (2 seconds). |
| HoldTime | Time interval in hundredths of a second during which no more than two configuration BPDUs are transmitted by this device. The default value is 100 (1 second). |

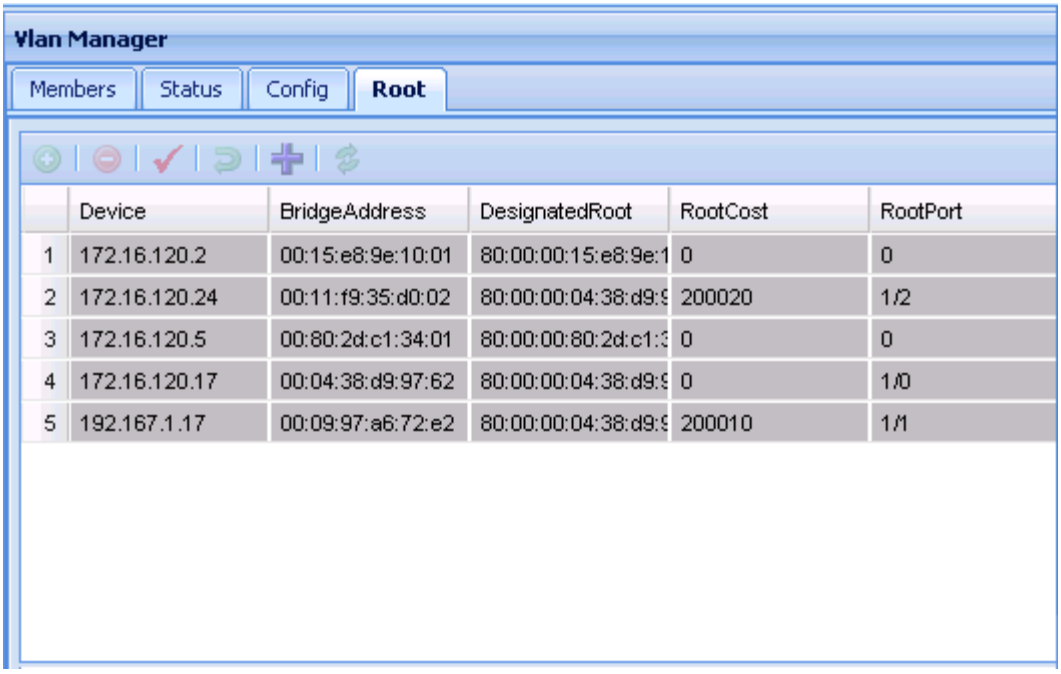
| Field | Description |
|---|---|
| ForwardDelay | Time interval in hundredths of a second that controls how fast a port changes its spanning state when moving toward the Forwarding state. This value determines how long the port stays in each of the Listening and Learning states, which precede the Forwarding state. This value is also used when a topology change is detected and is under way, to age all dynamic entries in the Forwarding Database. The default value is 1500 (15 seconds). |

## Viewing STG root status

Use the read-only Root table to view information about the device acting as root within a selected STG. Perform the following procedure to view the root table.

### Procedure steps

In the Navigation pane, open an STG and select **Root**.




### Job aid

The following table describes the fields in the Root table.

| Field | Description |
|---|---|
| Device | IP address of a device in the STG. |
| Bridge Address | MAC address used by this bridge when it must be identified in a unique fashion. |

| Field | Description |
|---|---|
| Designated Root | Bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol (as executed by this device). This value is used as the Root Identifier parameter in all configuration BPDUs originated by this device. |
| RootCost | Cost of the path to the root as seen from this bridge. |
| RootPort | Port number of the port that offers the lowest cost path from this bridge to the root bridge. |

# Viewing VLAN information

This section provides information about the following topics:

- VLAN icons on page 77
- Parts of VLAN icon on page 77
- Viewing the Default VLAN on page 78
- Updating VLAN discovery information on page 80

## VLAN icons

The VLAN icons in the Navigation pane, represent the VLANs that are part of an STG. The following figure Figure 7: VLAN Icon elements on page 77 shows elements of VLAN icons.


**Figure 7: VLAN Icon elements**

## Parts of VLAN icon

The following table Table 14: Parts of a VLAN icon on page 78 describes the elements of a VLAN icon.

**Table 14: Parts of a VLAN icon**

<table>
<tr><th>Part</th><th colspan="2">Description</th></tr>
<tr><td rowspan="8">Icon symbol</td><td colspan="2">Shows the type of VLAN.</td></tr>
<tr><td>Symbol</td><td>Description</td></tr>
<tr><td>  </td><td>Port based-a VLAN in which the ports are explicitly assigned to the VLAN.</td></tr>
<tr><td>  </td><td>Subnet based-a VLAN in which ports are dynamically added to the VLAN based on source IP subnet.</td></tr>
<tr><td>  </td><td>Protocol based–a VLAN in which ports are dynamically added to the VLAN based on a network protocol.</td></tr>
<tr><td>  </td><td>MAC SA based–a VLAN in which ports are dynamically added to the VLAN based on the source MAC address.</td></tr>
<tr><td>  </td><td>Stacked VLAN— a VLAN in which packets are transparently tunneled through the sVLAN domain by adding a 4-byte header to each packet.</td></tr>
<tr><td>  </td><td>ID-based VLAN—a VLAN in which ports are dynamically added to the VLAN based on the VLAN ID.</td></tr>
<tr><td rowspan="5">Icon label</td><td colspan="2">Shows information about the VLAN.</td></tr>
<tr><td>Label part</td><td>Description</td></tr>
<tr><td>VLAN name</td><td>The name of the VLAN.</td></tr>
<tr><td>VLAN ID</td><td>The ID number of the VLAN.</td></tr>
<tr><td>STG ID</td><td>The ID of the STG to which the VLAN belongs.</td></tr>
<tr><td></td><td>Typeface (italic or normal)</td><td>An italic icon label indicates that an IP address has been defined for the VLAN, and that the VLAN is routable.</td></tr>
</table>

## Viewing the Default VLAN

The following devices are factory configured with all ports contained in a port-based VLAN called the default VLAN:

- Ethernet Routing Switch 8000 Series
- Passport (legacy) 1050/1100/1150/1200/1250 switches
- Ethernet Routing Switches 1424/1648/1612/1624
- BayStack 380/420
- Ethernet Switches 350/410/450/460/470

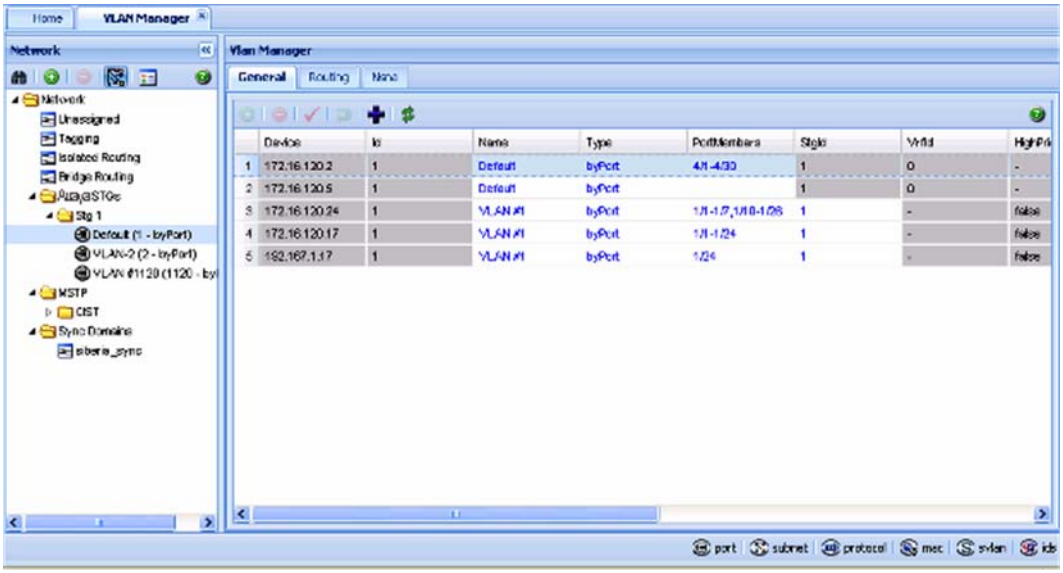
- Business Policy Switch 2000
- Ethernet Routing Switches 55xx/45xx/25xx/35xx
- Virtual Services Platform 9xxx
- Wireless Controller 8xxx

The VLAN ID of the default VLAN is always 1/1, and it is always a port-based VLAN. You cannot delete the default VLAN, although you can remove ports from it.

Perform the following procedure to view the Default Ports table.

## Procedure steps

From the navigation tree, select **Default(1)**. The General tab appears in the contents pane and displays the Default VLAN table.




## Job aid

The following table describes the fields in the Default VLAN table.

| Field | Description |
|---|---|
| Device | IP address, system name, or host name of the device. |
| ID | The VLAN ID. |
| Name | VLAN name |
| Type | Type by which you want to add the device. Options: by port, by subnet, by protocol, by source MAC Address, by SVLANs, and by ID. |
| Port Members | Ports that are assigned to the VLAN. |
| StgId | The STG ID. With Ethernet Switches 460 and 470, you can modify STG membership by modifying the value in the StgId field to the desired STG. When you apply the changes, the selected VLAN is removed from the |

| Field | Description |
|---|---|
| | old STG group and moved to the new STG group. If the new STG group already has an existing VLAN with the same ID, the members are combined into the same VLAN. If the VLAN does not already belong to the STG group, the new VLAN ID is added to the STG. |
| VrfId | The VRF ID. |
| HighPriority | In a Passport 1000 Series switch, you can select HighPriority mode for all traffic in the VLAN. |
| QosLevel | In an Ethernet Routing Switch 8000 Series you can set the Quality of Service (QoS) level for traffic in the VLAN to a level between 0 and 7. |
| TosLevel | You can set the Type of Service level for traffic between 0 and 7. |
| IfIndex | Logical interface index assigned to the VLAN. This value can be in one of the following ranges:<br>• Passport (legacy) 1050/1100/1150/1200/1250 switch: 257 to 512<br>• Ethernet Routing Switch 8000 Series: 2049 to 4096<br>• Virtual Services Platform 9xxx: 2049 to 4096<br>**Important:**<br>This field does not apply to Ethernet Switch, Legacy BayStack, or Business Policy Switch 2000 switches. |
| IpAddress | IP address, if any, assigned to the VLAN for routing. |
| NetMask | Subnet mask associated with the VLAN IP address. |

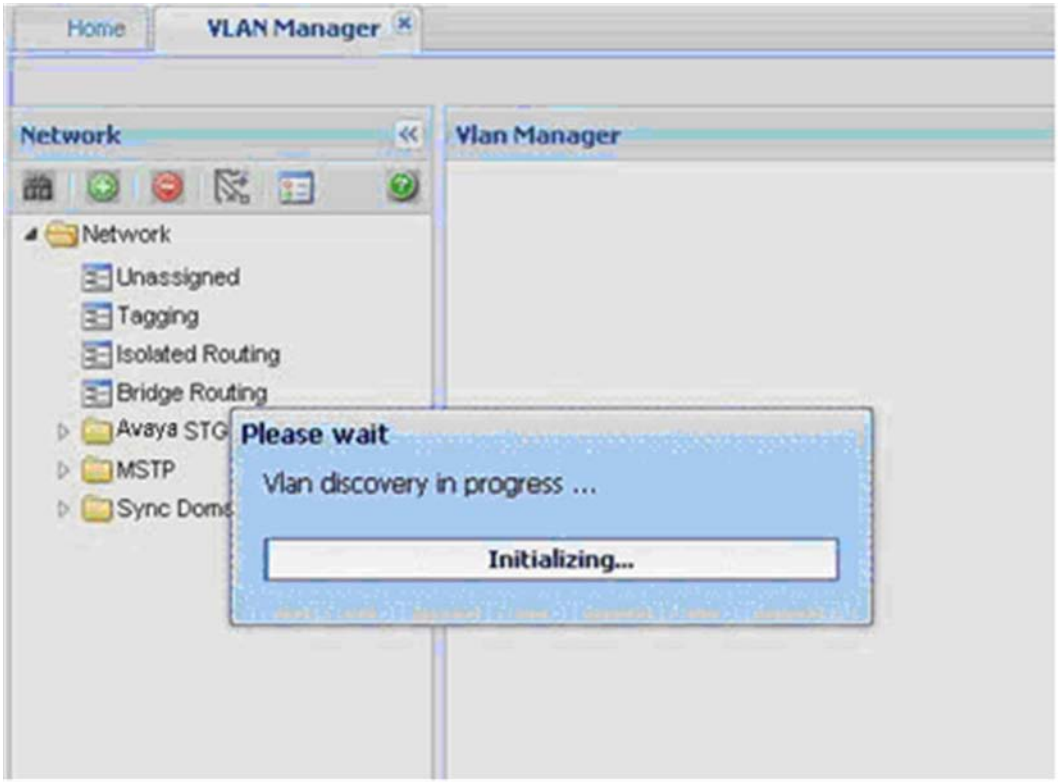
## Updating VLAN discovery information

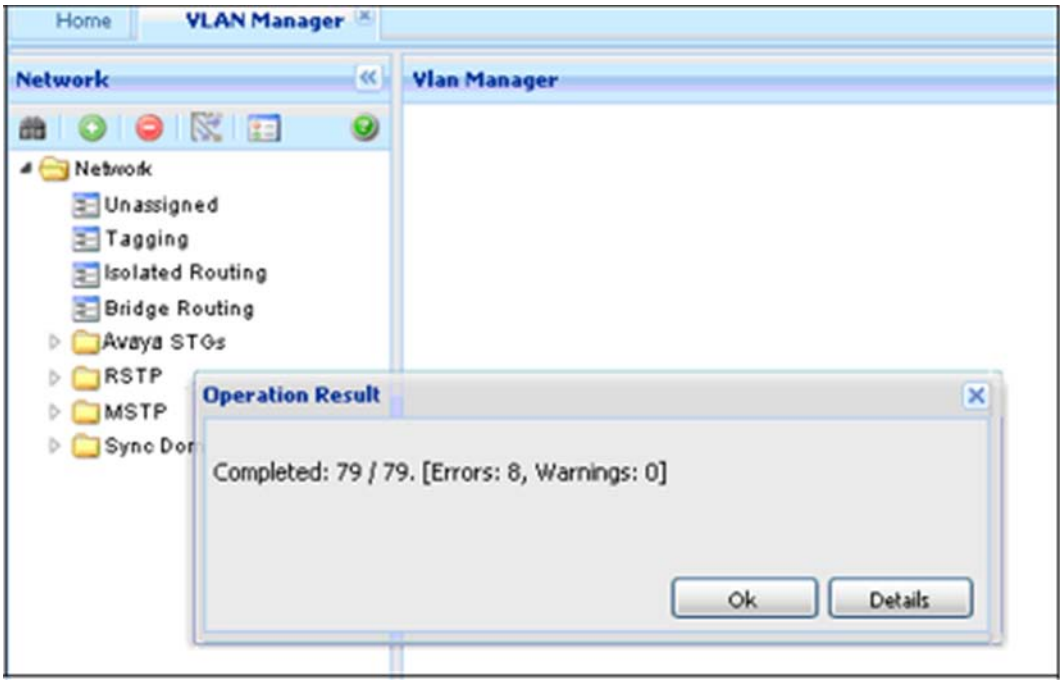
VLAN discovery polls VLAN and STG configuration from supported network devices and shows this information in the VLAN Manager window. You can use this feature to load any updated information that took effect since you opened VLAN Manager. Perform the following procedure to discover VLAN devices.

VLAN discovery runs when the VLAN Manager opens. You can also run VLAN discovery by manually running a Vlan discovery.

### Procedure steps

1. Click **Discover Vlans** on the Navigation pane, toolbar. An Operation Result information box appears when the discovery is complete.




2. Click **OK** to close the Operation Result information box.

# Viewing port membership information

You can use VLAN Manager to monitor the status of ports in a VLAN. VLAN Manager allows you to view the following information:

- Ports in the network that are configured as unassigned, tagging, or Isolated Routing Ports (IRPs) and brouter ports
- Ports that are assigned to a particular Spanning Tree Group (STG)
- Ports that are in the forwarding and blocking states and device that has the root of an STG
- Ports that are members of a VLAN or multiple VLANs.

This section contains describes how to perform the following tasks:


- Viewing the unassigned ports on page 82
- Viewing tagged ports on page 83
- Viewing isolated router ports on page 84
- Viewing bridge routing ports on page 85
- Viewing port members of an STG on page 86
- Viewing VLAN Port Members in MSTP on page 87

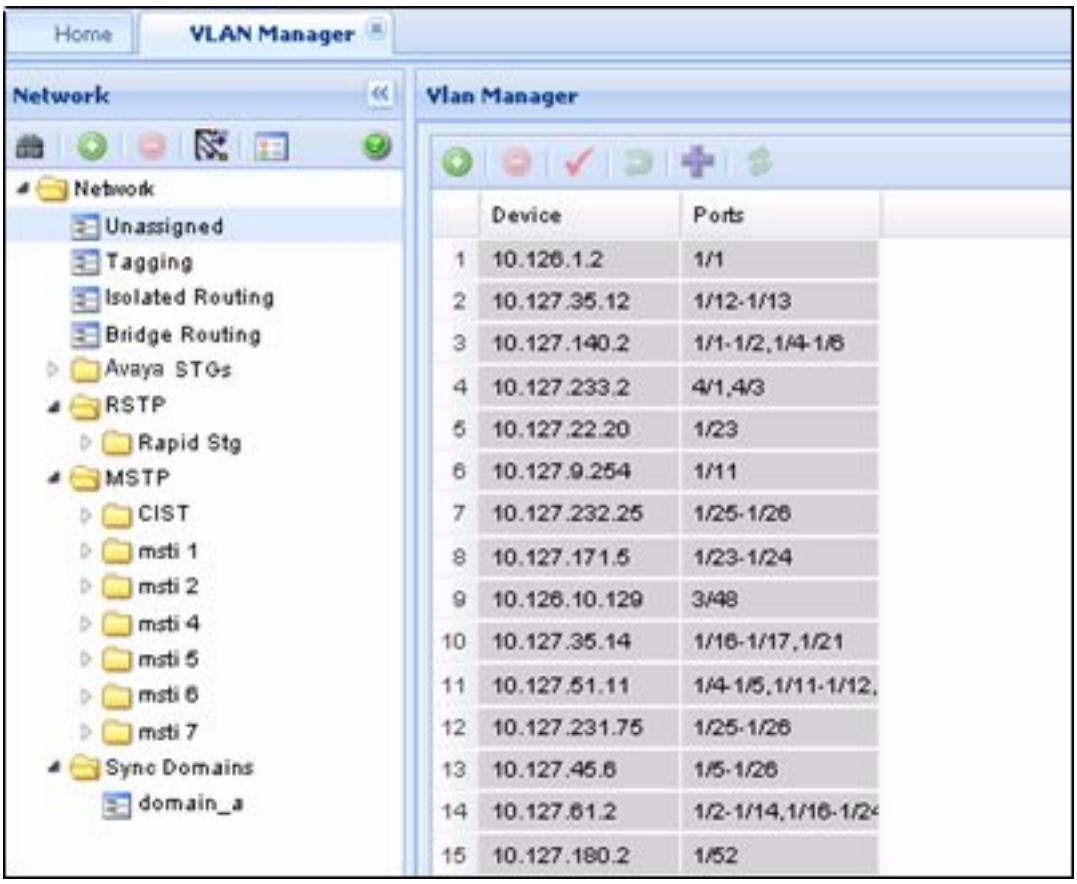

## Viewing the unassigned ports

Perform the following procedure to view the unassigned ports.

### Procedure steps

In the Navigation pane, click **Unassigned**.

The Unassigned Ports table appears in the contents pane.




### Job aid

The following table describes the Unassigned Ports table fields.

| Field | Description |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Ports | Ports not currently assigned to an STG. |

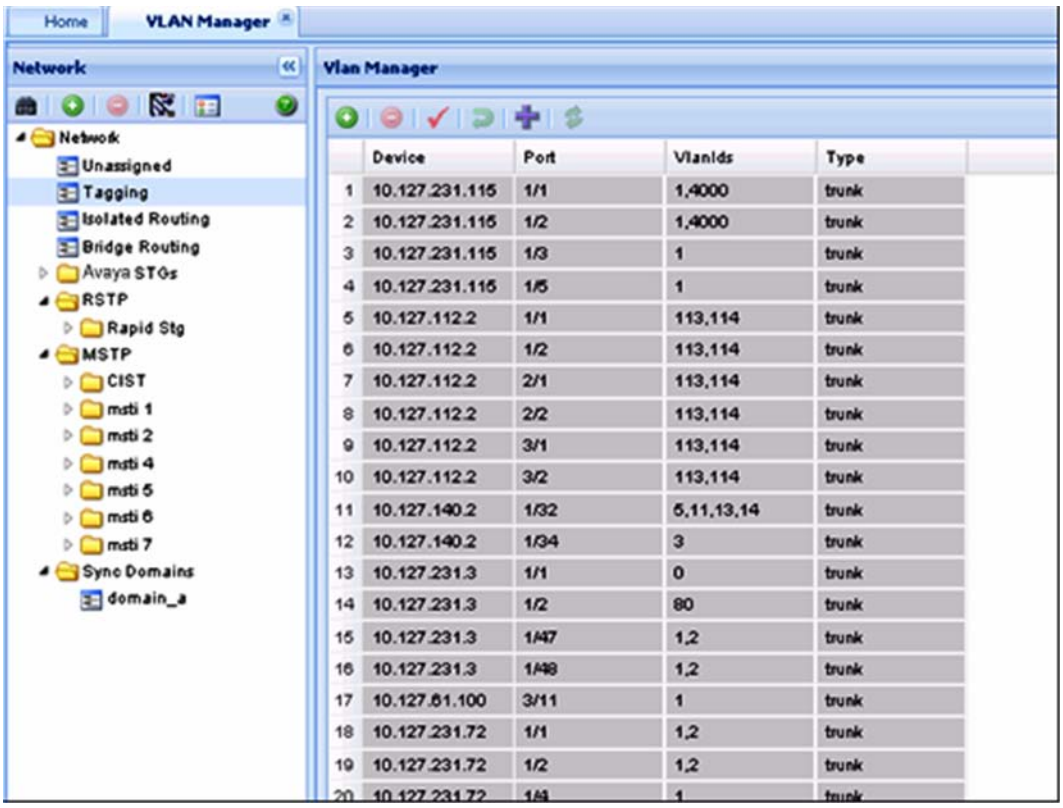
## Viewing tagged ports

Perform the following procedure to view tagged ports.

### Procedure steps

In the Navigation pane, select **Tagging**.

The Tagging Ports table appears in the contents pane.




### Job aid

The following table describes the fields in the Tagging Ports table.

| Field | Description |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Port | Port on which tagging is enabled. |
| VlanIds | VLAN IDs of which the port is a member. |
| Type | Type of port: access port or trunk port |

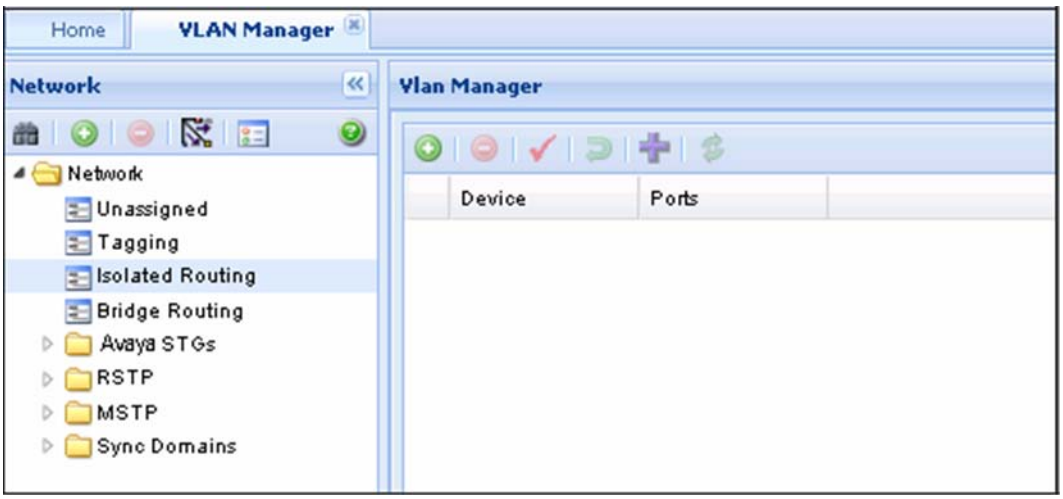
## Viewing isolated router ports

Perform the following procedure to view isolated router ports.

### Procedure steps

In the Navigation pane, select **Isolated Routing**.

The Isolated Routing Ports table appears in the contents pane.




### Job aid

The following table describes the fields in the Isolated Routing Ports table.

| Field | Descriptions |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Ports | Ports that route only IP packets. |

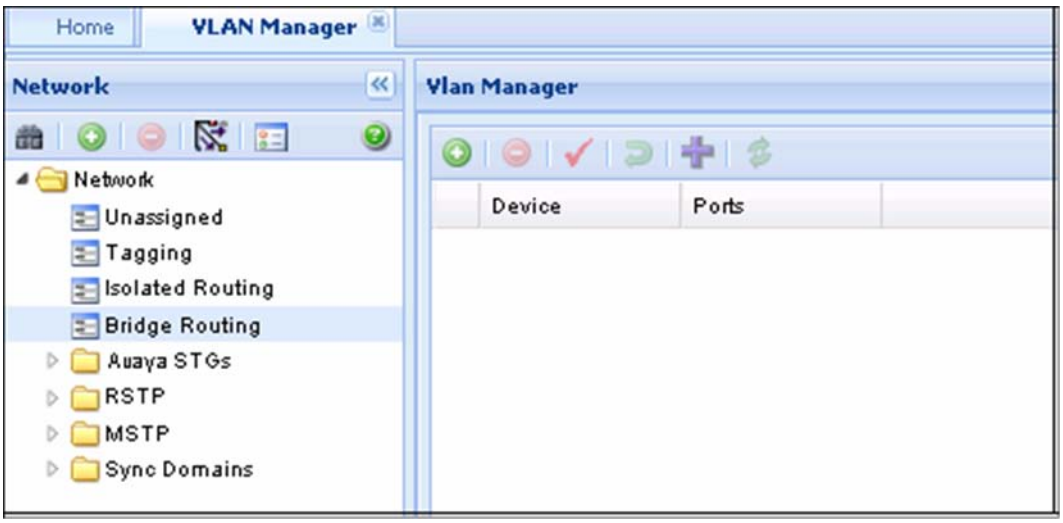
## Viewing bridge routing ports

Perform this procedure to view bridge routing (brouter) ports on Passport 1000 Series switches, Ethernet Routing Switch 8000 Series, and Virtual Services Platform 9xxx.

### Procedure steps

In the Navigation pane, click **Bridge Routing**.

The Bridge Routing Ports table appears in the contents pane.




### Job aid

The following table describes the fields in the Bridge Routing Ports table.

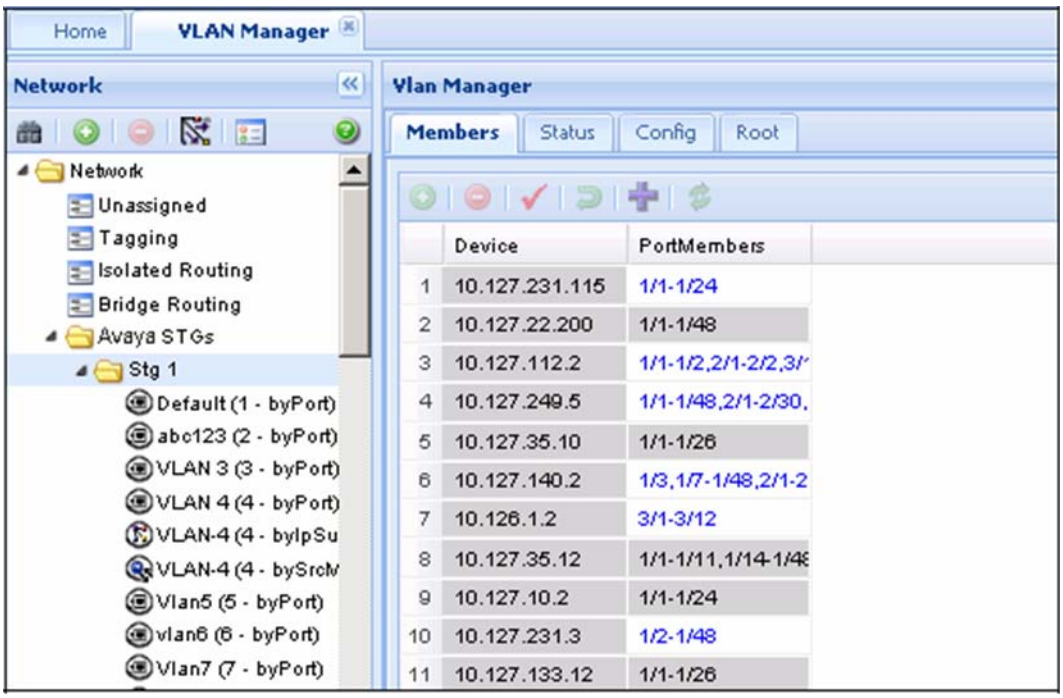
| Field | Descriptions |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Ports | Port numbers of the port on which frames are received. |

## Viewing port members of an STG

Use the Port Members table to view the ports that are members of the specified STG. Perform the following procedure to open the Port Members table.

### Procedure steps

In the Navigation pane, click an STG, and then select **Members** from the tab in the content pane.




### Job aid

The following table describes the member table fields.

| Field | Description |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Port Members | Ports on the device that are members of the STG. |

## Viewing VLAN Port Members in MSTP

Use the Port Members table to view the ports that are members of the specified MSTI or CIST instance.

Perform the following procedure to open the Port Members table.

### Procedure steps

1. From the navigation tree, select the **MSTP** folder.
2. Select the **CIST** folder or an **MSTI** folder.
3. Select a VLAN.

   The Members table appears in the contents pane.

# Highlighting information on the topology map

You can view VLAN information by highlighting it on the topology map. Highlighting information on the topology map is helpful in monitoring and troubleshooting VLANs in your network. This section provides information about the following topics:



## Viewing VLAN members on the topology map

Perform the following procedure to highlight the members of a VLAN on the topology map.

### Procedure steps

1. In the Navigation pane, choose a VLAN.

   The Ports table appears in the VLAN Manager contents pane.
2. On the VLAN Manager menu bar, click **Highligh on Topology**.

   The highlighted topology view appears in the COM contents pane.

## Viewing STG port members on the topology map

When you select an STG in the VLAN Manager Navigation pane, you can view the devices and ports associated with that STG in the COM network topology map. This view can assist you in troubleshooting by identifying which ports are already members of the STG selected.

Perform the following procedure to highlight the STG ports on the topology map.

### Procedure steps

1. In the VLAN Manager Navigation pane, choose an **STG Members** icon.

   The STG Members table appears in the VLAN Manager contents pane.
2. On the VLAN Manager menu bar, click **Highligh on Topology**.

   The devices containing STG ports are highlighted with a color and the device IP address.

## Viewing STG root configuration on the topology map

You can get a quick view of which device is the root of the Spanning Tree Group and which ports are in the forwarding and blocking state by selecting the STG root icon.

Perform the following procedure to highlight the STG root configuration on the topology map.

### Procedure steps

1. In the Navigation pane, select an **STG Root**.

   The Root table appears in the contents pane.

2. On the VLAN Manager menu bar, click **Highligh on Topology**.

   The highlighted topology view appears in the COM contents pane with the root displayed.

# Chapter 5: Using the MultiLink Trunking Manager

Multi-Link Trunking (MLT) allows the physical links between multiple ports to be treated as a single logical link so that they logically act like a single port with the aggregated bandwidth. Grouping multiple ports into one logical link allows you to achieve higher aggregate throughput on a switch-to-switch or server-to-server application. It also allows you to load balance the traffic across all available links.

With MLT, all the physical ports in the link aggregation group must reside on the same switch. The Split MultiLink Trunking (SMLT) protocol does not have this limitation. SMLT allows the physical ports to be split between two switches. The two switches between which the SMLT is split are known as aggregation switches and form a logical cluster which appears to the other end of the SMLT link as a single switch.

The split may be at one or at both ends of the MLT, allowing you to configure any of the following topologies:

- SMLT square—Both ends of the link are split, and there is no cross-connect between diagonally opposite aggregation switches.
- SMLT mesh— Each aggregation switch has a SMLT connection with both aggregation switches in the other pair.
- SMLT triangle— A topology in which only one end is split. In an SMLT triangle, the end of the link which is not split does not need to support SMLT. This allows non-Avaya devices to benefit from SMLT, as long as they support 802.3ad static mode.

The Inter-Switch Trunk (IST) is an important part of the operation of the SMLT. The IST is an MLT connection between the aggregation switches that allows the exchange of information about traffic forwarding and about the status of individual SMLT links.

This section describes how to use MultiLink Trunking Manager to configure MLTs, SMLTs, and ISTs.

**Note:**

Avaya Virtual Services Platform (VSP) devices work in a similar way as ERS8600 devices, except for the following:

- MLT IDs run from 1 to 512 MLTs.
- There is no SMLT ID in the VSP device. The MLT ID is used for both MLT and SMLT trunks.

WC devices work in a similar way as mERS5600 devices. The workflow of the MLT manager for these devices are similar to the mERS5600 devices, except that there are no SMLT IDs for WC devices.

### Navigation


- About MultiLink Trunking Manager on page 92
- Starting the MultiLink Trunking Manager on page 93

# About MultiLink Trunking Manager

The MultiLink Trunking Manager in COM allows you to create and manage MLTs across devices in a network. You can also use MultiLink Trunking Manager to manage Split MultiLink Trunking (SMLT) and to configure ISTs.

The following sections describe Multilink trunk types and features:



## MultiLink Trunks in different switch types

The following table lists the number of MLTs available with each supported switch type.

**Table 15: Maximum number of MLTs supported in different switches**

| Switch | Maximum number of MLTs |
|---|---|
| Passport 1000 Series switch | 8 |
| Ethernet Routing Switches 1424T/1648/1612/1624 | 6 |
| Ethernet Routing Switch 8100 | 6 |
| Ethernet Routing Switch 8600 and 8800 switches | 128 in R-mode |
| Virtual Services Platform | 512 |
| BayStack 350/380/410/420/450/460/470 | 6 |
| Business Policy Switch 2000 | 6 |
| Ethernet Switch 325/425/460/470 | 6 |
| Ethernet Routing Switch 5510, 5520, 5530 | 32 |
| OM 1000 | 1 |
| Ethernet Routing Switch 45xx, 25xx, 3510 | 6 |
| Ethernet Routing Switch 5600 | 32 |

| Switch | Maximum number of MLTs |
|---|---|
| Wireless Controller | 32 |
| Ethernet Routing Switch 8300 | 32 |

## MultiLink Trunking Manager features

MultiLink Trunking Manager supports devices that implement the Vlan and STG MIB groups.

MultiLink Trunking Manager allows you to:

- Create, delete, or modify MLTs/SMLTs across one or two devices.
- Configure an MLT/SMLT either before or after you physically connect the ports.
- View MLT/SMLT configuration information such as port and MLT membership.
- View MLT/SMLT links and ports in the network topology map.

# Starting the MultiLink Trunking Manager

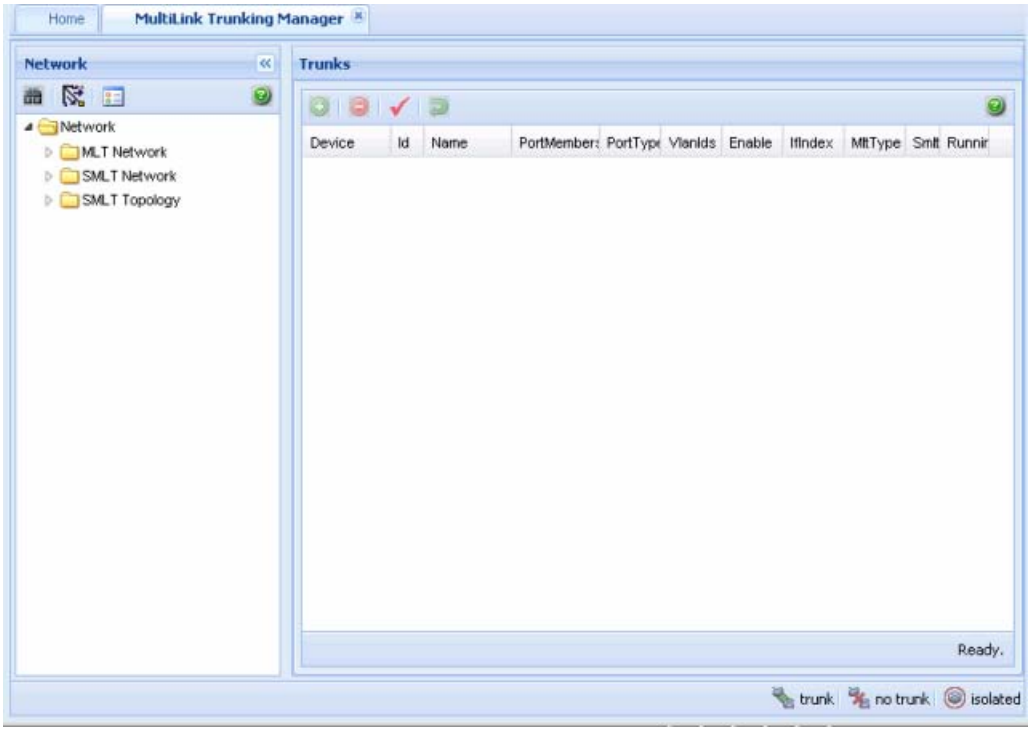
Perform the following procedure to start a MultiLink Trunking Manager.

### Procedure steps

1. From the Configuration and Orchestration Manager window Navigation pane, click **Managers**.

   The list of managers appears on the left side of the window.
2. Click the **Multilink Trunking Manager** icon in the navigation tree.

   The MultiLink Trunking Manager is launched and displayed in the content pane.




# Using the MultiLink Trunking Manager window

The MultiLink Trunking Manager window contains the parts identified in the following figure.

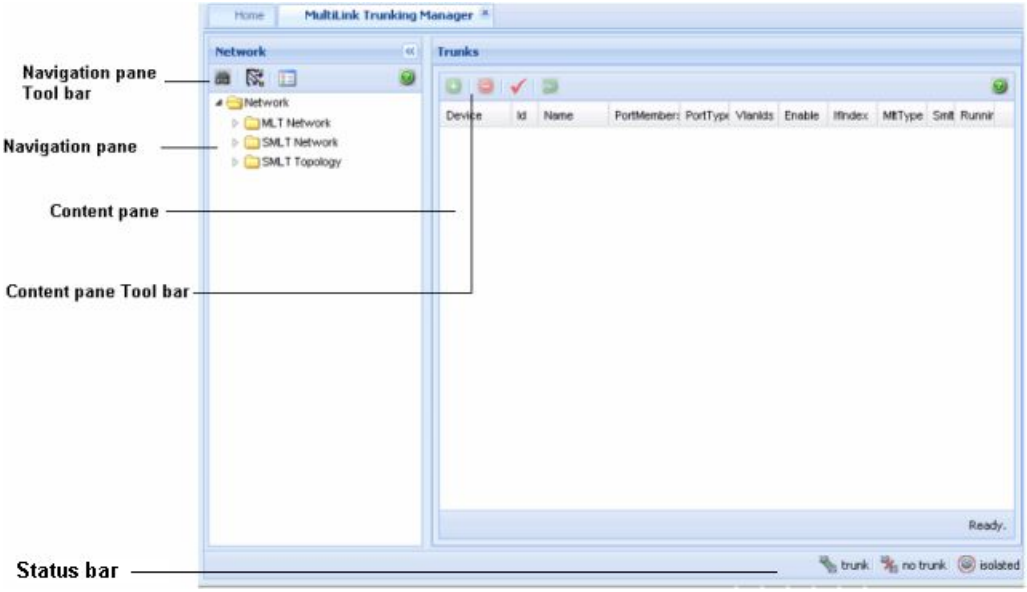



**Figure 8: MultiLink Trunking Manager window**

The following table describes the parts of the MultiLink Trunking Manager window.

**Table 16: MultiLink Trunking Manager window parts**

| Part | Description |
|---|---|
| Navigation pane | Provides a navigation tree showing MultiLink Trunking Manager network folder resources. |
| Navigation pane tool bar | Provides tools for MultiLink Trunking Manager. |
| Contents pane | Displays MultiLink Trunking Manager tables. |
| Contents pane toolbar | Provides quick access to commonly used MultiLink Trunking Manager commands. These commands apply only to the Content pane table. |

## Navigation pane

The MultiLink Trunking Manager navigation pane provides access to devices based on the type of multilink trunking, or SMLT. The Navigation pane has a Network folder. All the devices are identified by their IP address, as discovered by COM. Adjacent devices are listed in the device folder.

The following figure shows the Navigation pane.

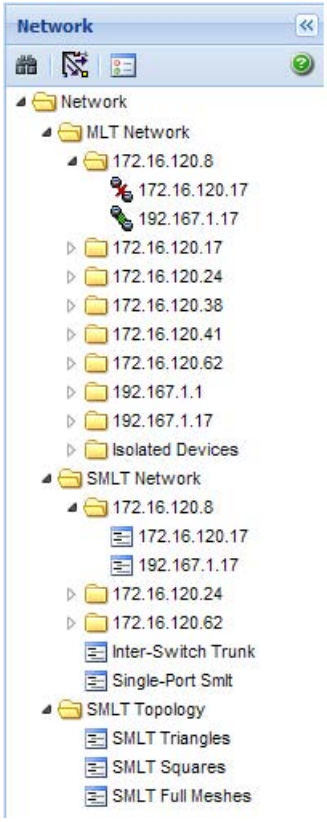


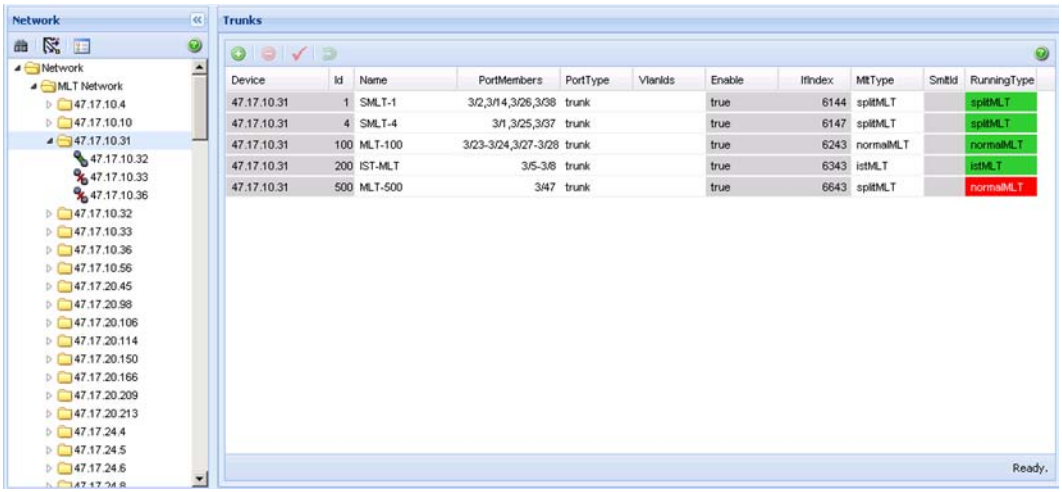

**Figure 9: MultiLink Trunking Manager navigation pane**

The Network folder has the following resources available in it.

- MLT Network folder on page 96
- SMLT Network folder on page 97
- SMLT Topology folder on page 99

## MLT Network folder

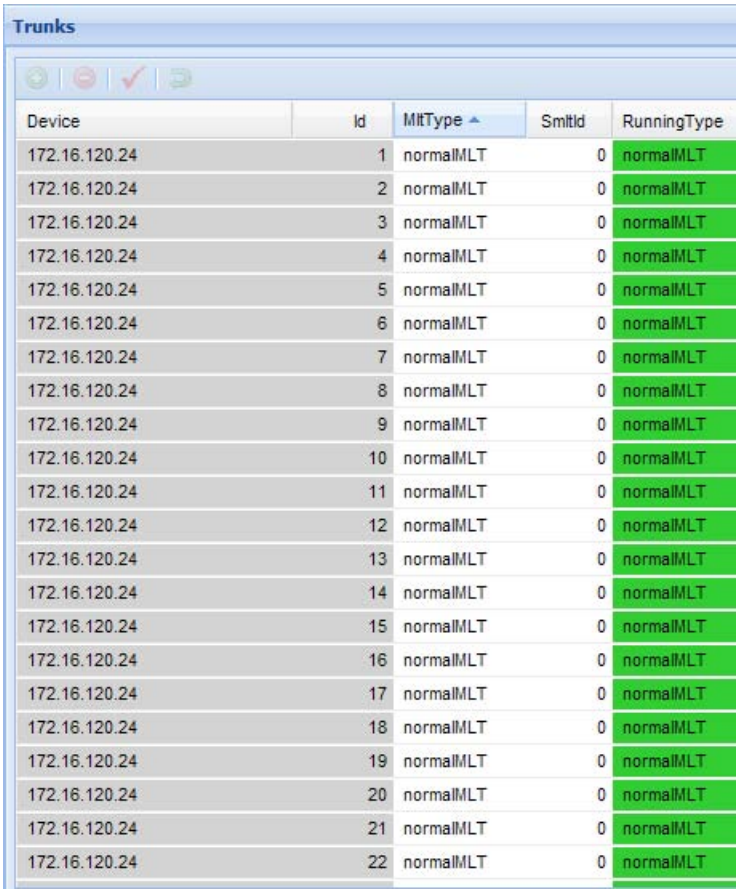
The MLT Network folder displays all the configured trunks of the devices. When you click on the nodes on the navigation pane inside the MLT Network folder, the contents pane displays all the configured tasks of the device. When you click on the child nodes which is connected to the parent devices, only the trunks connecting to the parent device appear. The following figure and table shows the MLT Network folder and its contents.




## SMLT Network folder

The SMLT Network folder contains only the devices that are SMLT capable, and their child nodes. The Inter-Switch Trunks (IST) contains a list of devices that have an SLT trunk configured. The Single-SMLT (SSMLT) contains a list of devices that have a single port SMLT trunk configured.

The following figure shows the SMLT Network folder and its contents.



Trunks

| Device | Id | MltType | SmltId | RunningType |
|---|---|---|---|---|
| 172.16.120.24 | 1 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 2 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 3 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 4 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 5 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 6 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 7 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 8 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 9 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 10 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 11 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 12 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 13 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 14 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 15 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 16 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 17 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 18 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 19 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 20 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 21 | normalMLT | 0 | normalMLT |
| 172.16.120.24 | 22 | normalMLT | 0 | normalMLT |

**Figure 10: SMLT Network**

The following figure shows the discovered Inter-Switch Trunks folder details.

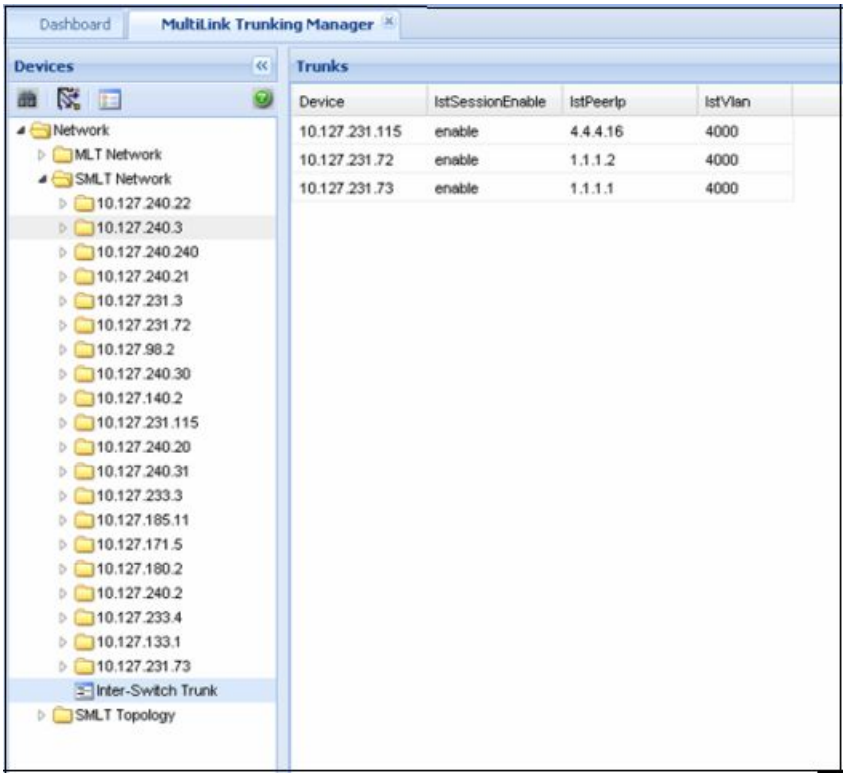


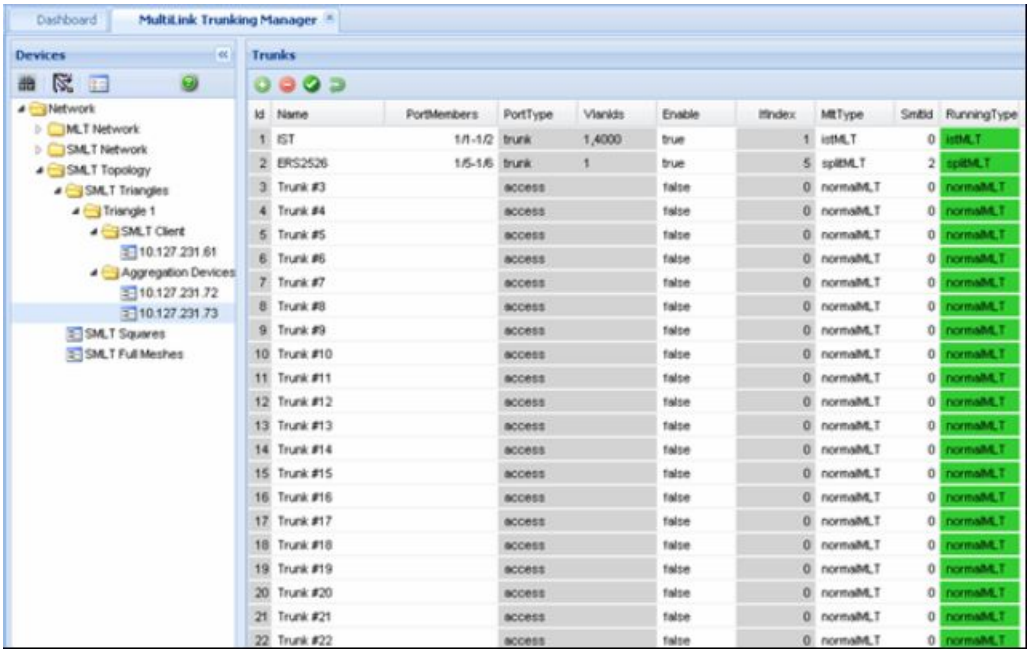

**Figure 11: SMLT Network IST**

## SMLT Topology folder

The SMLT Topology folder contains the following three subfolders. These folders are discovered at the time of launching the MultiLink Trunking Manager, or while performing a rediscovery of all the MLT information.

- SMLT Triangles—contains aggregation devices folder and their SMLT client folder.
- SMLT Squares—contains four core aggregation devices.
- SMLT Meshes—contains four or more core aggregation devices.

The following figures shows the SMLT topology triangle expanded, along with trunk details from one selected aggregation device folder.




| Id | Name | PortMembers | PortType | VlanIds | Enable | IfIndex | MltType | SmltId | RunningType |
|---|---|---|---|---|---|---|---|---|---|
| 1 | IST | 1/1-1/2 | trunk | 1,4000 | true | 1 | istMLT | 0 | istMLT |
| 2 | ERS2526 | 1/5-1/6 | trunk | 1 | true | 5 | splitMLT | 2 | splitMLT |
| 3 | Trunk #3 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 4 | Trunk #4 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 5 | Trunk #5 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 6 | Trunk #6 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 7 | Trunk #7 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 8 | Trunk #8 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 9 | Trunk #9 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 10 | Trunk #10 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 11 | Trunk #11 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 12 | Trunk #12 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 13 | Trunk #13 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 14 | Trunk #14 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 15 | Trunk #15 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 16 | Trunk #16 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 17 | Trunk #17 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 18 | Trunk #18 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 19 | Trunk #19 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 20 | Trunk #20 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 21 | Trunk #21 | | access | | false | 0 | normalMLT | 0 | normalMLT |
| 22 | Trunk #22 | | access | | false | 0 | normalMLT | 0 | normalMLT |

**Figure 12: SMLT Triangle**

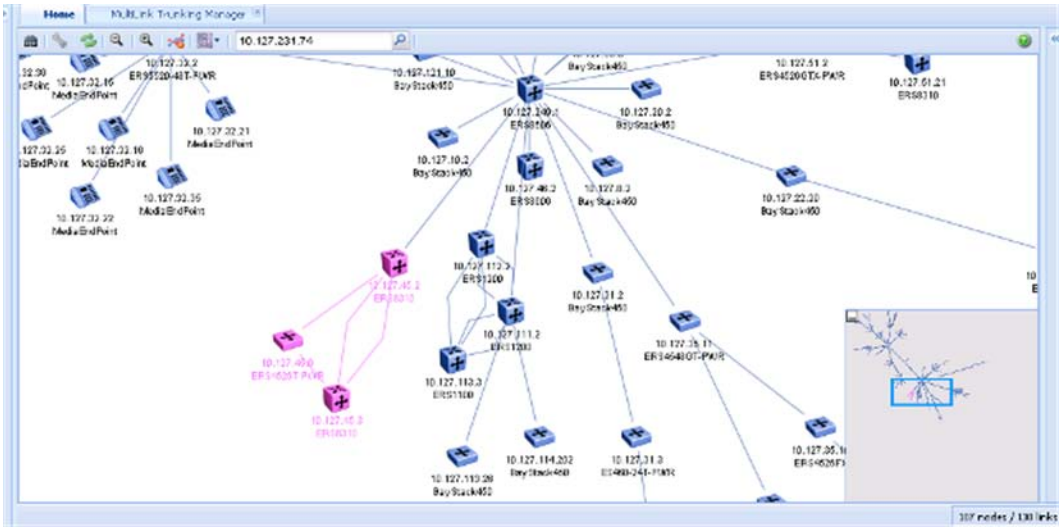



**Figure 13: SMLT Triangle Topology**

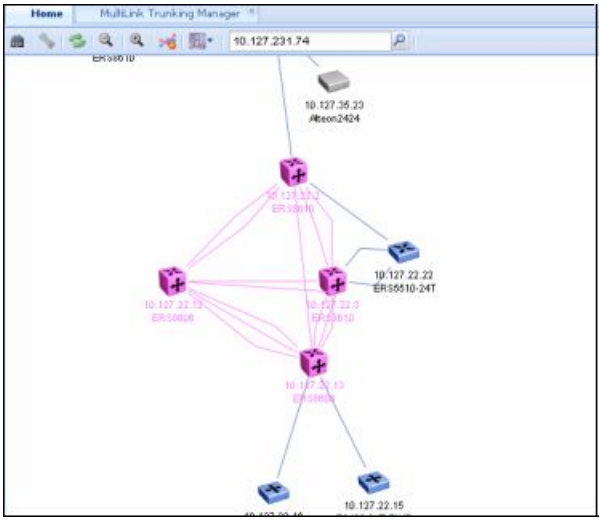



**Figure 14: SMLT Full mesh Topology**

## Navigation pane tool bar

The Navigation pane tool bar provide tools and commands to address discovery of trunks, Preferences and topology highlights.

The following table lists the MultiLink Trunking Manager Navigation pane tool bar buttons.

**Table 17: Navigation pane tool bar**

| Tools | Toolbar button | Description |
|---|---|---|
| Discover MultiLink Trunks | | Discovers the network and reloads MultiLink Trunking Manager with the latest information. |
| Highlight Topology | | Highlights MLT items in the MultiLink Trunking Manager contents pane. |
| Preferences | | Identifies specific devices for MultiLink Trunking Manager to configure and manage. |
| Help | | Opens the online Help. |

## Contents pane

When you choose a folder in the navigation pane, its contents are shown in the contents pane.

Perform the following procedure to view the folder in the contents pane.

### Procedure steps

1. In the COM Navigation pane, expand **Managers**, and then click **MultiLink Trunking Manager**.

   The MultiLink Trunking Manager window appears on the right side of the window.

2. In the Navigation pane of the MultiLink Trunking Manager window, select the **Network** folder.

   The list of devices appear in the Network folder.

3. Click on a device from the list in the **Network** folder.

   The contents of the folder are displayed as a table in the contents pane, as shown in the example.

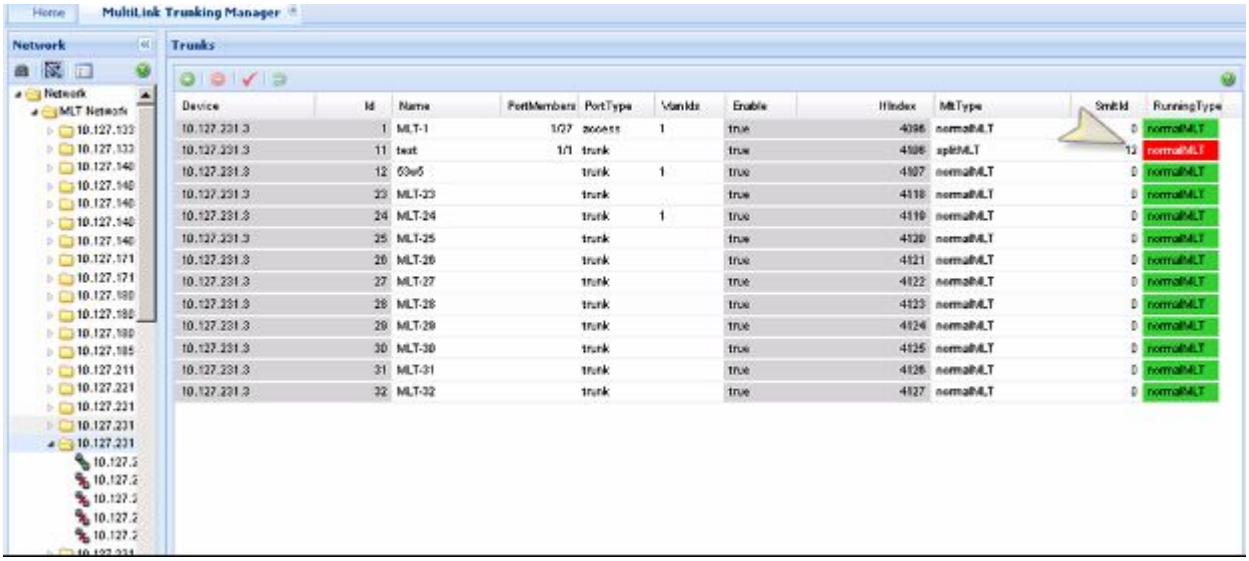



**Figure 15: MultiLink Trunking Manager contents pane**

## Content pane tool bar

The Content pane tool bar provide tools to add an MLT, delete an MLT, commit the changes, and undo the changes.

The following table lists out the tools available on Content pane tool bar.

**Table 18: Content pane tool bar**

| Tools | Toolbar button | Description |
|---|---|---|
| Insert |  | Opens the Insert dialog box, where you insert an MLT on a selected device. For more information, see Creating MLTs |

| Tools | Toolbar button | Description |
|---|---|---|
| | | on ERS 1424/16xx, ERS 8000, and VSP 9xxx devices on page 103. |
| Delete |  | Removes a selection and displays a message box to confirm deletion of the selected MLT. For more information, see Deleting an MLT from ERS 1424/16xx, ERS 8000 or VSP 9xxx on page 109. |
| Apply Changes |  | Applies any changes you have made to your MLT configuration. |
| Revert Changes |  | Allows you to undo the changes you have made to your MLT configuration. |
| Help |  | Opens the online Help. |

# Managing MultiLink Trunks

This following topics describe common operations you can perform using MultiLink Trunking Manager:

- Creating MLTs on ERS 1424/16xx, ERS 8000, and VSP 9xxx devices on page 103
- Viewing MLT port information on page 108
- Editing a port on an MLT on page 108
- Deleting an MLT from ERS 1424/16xx, ERS 8000 or VSP 9xxx on page 109
- Editing an MLT on page 109

## Creating MLTs on ERS 1424/16xx, ERS 8000, and VSP 9xxx devices

To create an MLT on Ethernet Routing Switch 1424/16xx, Ethernet Routing Switch 8000, and VSP 9xxx devices, the device must have more than one connection to another device. With MultiLink Trunking Manager, you can create an MLT on a device and then physically connect the ports, or you can connect the ports first and then configure the MLT.

**Important:**

The procedures in this section do not apply to Ethernet Switch, Ethernet Routing Switch 55xx/35xx/45xx/25xx, or Legacy BayStack devices which are preconfigured with six MLTs. You cannot delete or add MLTs to these switches.

## Insert MLT dialog box

The appearance of the Insert MLT dialog box differs depending on how you open it.

If you select a device folder and click Insert, the single-node Insert MLT dialog box appears. For more information, see Creating an MLT with one device for ERS 8000 or VSP 9xxx on page 104.

You can use the single-node Insert MLT dialog box to create MLT configurations even in situations where the physical connections are absent or have not been detected by COM.

The following sections describe how to create MLTs on single devices and pairs of devices:

- Creating an MLT with one device for ERS 8000 or VSP 9xxx on page 104
- Creating an MLT with one device for ERS 1424/16xx on page 106

## Creating an MLT with one device for ERS 8000 or VSP 9xxx

When you create an MLT with one device, MultiLink Trunking Manager considers only the ports that are available on the one device. After you create an MLT on one device, you must also configure and connect the ports in the second device before enabling the MLT.

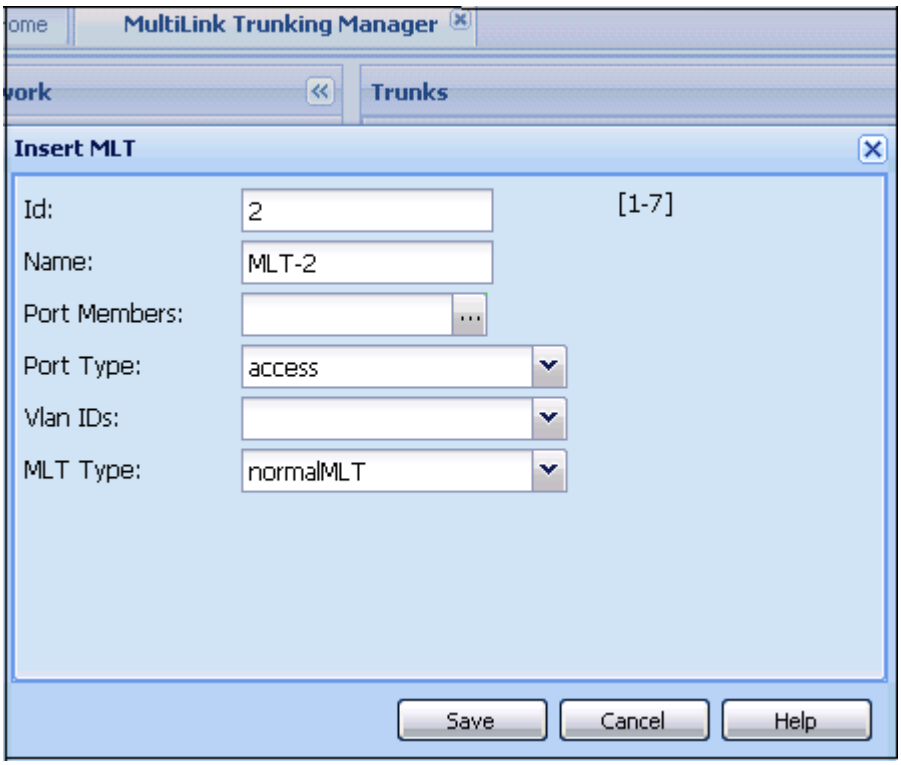
To configure a new MLT with one Ethernet Routing Switch 8000 or VSP 9xxx device selected:

### Procedure steps

1. Select a device from the first (folder) level of the MultiLink Trunking Manager navigation pane.

   The Device table appears in the contents pane.
2. For Ethernet Routing Switch 8000 devices or VSP 9xxx devices, On the Content Pane Toolbar, click **Add**.

   The Insert MLT dialog box appears.




3. In the **Id** field, select the Id number for the MLT.
4. In the **Name** field, type the name of the MLT.
5. In the **Port members** field, select the ports to be added to the MLT.

   Inactive ports in the Ports box specify that they are not available for creating any MLTs.
6. Select the **Port type** option.

   The default is **access**.
7. In the **VlanIds** field, select the VLAN IDs that belong to the MLT port.
8. For **MLT Type**, choose **normalMLT**.

   The istMLT and splitMLT types, and also the SMLT Id value, are used only for split multilink trunks. For more information, see Managing SMLT configurations on page 110.
9. Click **Save**.

## Insert MLT dialog box for ERS 8000 or VSP 9xxx

The following table describes the items in the Insert MLT dialog box.

**Table 19: Insert MLT dialog box items for ERS 8000**

| Item | Description |
|---|---|
| Id | Unique identifier for the MLT, which is automatically assigned by MultiLink Trunking Manager. |
| Name | User-defined name of the node on the MLT. |
| Port Members | Ports in the MLT. |
| Port Type | One of the following types of MLT:<br>• Access<br>• Trunk<br>The default is Access. |
| Vlan IDs | VLAN IDs found on the device. |
| MLT type | One of the following types of MLT links:<br>• normalMLT- Use for normal MLT that do not use SMLT features.<br>• istMLT- Use for IST (inter-switch trunk) links between peer devices in SMLT configurations.<br>• splitMLT- Use for SMLT links between peer devices and non-peer devices in SMLT configurations. |
| SMLT ID | Sets the SMLT ID number for IST links. |

**Note:**
In the VSP device there is no SMLT ID. The MLT ID is used for both MLT and SMLT trunks.

## Creating an MLT with one device for ERS 1424/16xx

When you create an MLT with one device, MultiLink Trunking Manager considers only the ports that are available on the one device. After you create an MLT on one device, you must also configure and connect the ports in the second device before enabling the MLT.

Perform the following procedure to configure a new MLT with one Ethernet Routing Switch 1424/16xx device selected.

### Procedure steps

1. Select a device from the first (folder) level of the MultiLink Trunking Manager navigation pane.

   The Device table appears in the contents pane.

2. For Ethernet Routing Switch 1424/16xx devices, On the Content Pane Toolbar, click **Add**.

The Insert MLT dialog box appears.

3. In the **Id** text box, select the Id number for the MLT.
4. In the **Name** text box, type the name of the MLT.
5. In the **Port Members** box, select the ports to be added to the MLT.

   Inactive ports in the Ports box specify that they are not available for creating any MLTs.
6. Select the **Port type** option.

   The default is **access**.
7. In the **VlanIds** field, select the VLAN IDs that belong to the MLT port.
8. For **MLT Type**, choose **normalMLT**.

   The istMLT and splitMLT types, and also the SMLT Id value, are used only for split multilink trunks. For more information, see Managing SMLT configurations on page 110.
9. Click **Save changes**.

## Insert MLT dialog box for ERS 1424/16xx

The following table describes the items in the Insert MLT dialog box.

**Table 20: Insert MLT dialog box for ERS 1424/16xx**

| Item | Description |
|---|---|
| Id | Unique identifier for the MLT, which is automatically assigned by MultiLink Trunking Manager. |
| Name | User-defined name of the node on the MLT. |
| Port Type | One of the following types of MLT:<br>• Access<br>• Trunk<br>The default is Access. |
| Vlan IDs | VLAN IDs found on the device. |
| MLT type | One of the following types of MLT links:<br>• normalMLT- Use for normal MLT that do not use SMLT features.<br>• istMLT- Use for IST (inter-switch trunk) links between peer devices in SMLT configurations.<br>• splitMLT- Use for SMLT links between peer devices and non-peer devices in SMLT configurations. |
| Ports | Ports in the MLT. The maximum number of ports for one trunk is four. |

## Viewing MLT port information

Perform the following procedure to view port information as you configure an MLT.

### Procedure steps

1. In the navigation pane, select an MLT.

   The MLT table appears in the contents pane.
2. In the table, double-click the **PortMembers** field.

   The PortMembers dialog box appears.


3. In the MLT Table, click **...** to view the port information.

To open the Insert MLT dialog box, see Creating an MLT with one device for ERS 8000 or VSP 9xxx on page 104.

The information displayed in the dialog box includes the VLAN(s) and STG(s) to which the port belongs and the port link status. The port link status information includes whether the port is up or down and what other device/ports the port is connected to.

## Editing a port on an MLT

Perform the following procedure to edit a port on an existing MLT.

### Procedure steps

1. In the navigation pane, select an MLT.

   The MLT table appears in the contents pane.
2. In the table, double-click the **PortMembers** field.

   The PortMembers dialog box appears.


3. Click the port numbers that you want to add or delete from the MLT.

   Port numbers that appear to be pressed in are already being used, and port numbers that are dimmed are inactive.

4. Click **Save**.

## Deleting an MLT from ERS 1424/16xx, ERS 8000 or VSP 9xxx

Perform the following procedure to delete an MLT from an Ethernet Routing Switch 1424/16xx or 8000, or VSP 9xxx.

### Procedure steps

1. In the navigation pane, select a device.

   The MLT table appears in the content pane.

2. Select a field you want to delete in the table.
3. Click **Delete** from the Content Pane toolbar..

   The Delete dialog box appears, asking you to confirm the deletion.

4. Click **Ok**.

## Editing an MLT

Perform the following procedure to edit an MLT.

### Procedure steps

1. In the navigation pane, select a device.

   The MLT table appears in the contents pane.

2. Double-click the field in the table.
3. Type information in the text boxes, or select from a list.

   Your changes are displayed in bold.

4. On the Content Pane Toolbar, click **Apply Changes**.

# Managing SMLT configurations

Mission critical networks require resiliency, and as a result, must be designed with a number of redundancy features. Within the Passport 8000 Series switch, such features include CPU redundancy and link redundancy using MLT.

In order to provide device redundancy, most enterprise networks are designed with redundant connections between aggregation (core) switches and user access switches. For networks with just one aggregation switch, MLT provides redundancy and load sharing.

SMLT improves the reliability of a Layer 2 (L2) network operating between a building user access switches and the network center aggregation switch. It does so by providing loadsharing among all the links and fast failover in case of link failures.

An Interswitch Trunk (IST) operates between the aggregation switches and allows them to exchange information. This permits the rapid detection of any faults and the modification of forwarding paths.

**Important:**

Although SMLT is primarily designed for layer 2 networks, it provides benefits for layer 3 networks as well.

To configure SMLT, you must establish three sets of configurations on the devices:

- On the two peer aggregation switches, you configure an IST (inter-switch trunk). For more information, see Configuring IST links on page 110.
- On the two peer aggregation switches, you configure SMLT links to the edge switch. For more information, see Configuring SMLT links on peer devices on page 111.
- On the nonpeer device, you configure normal MLT links to the two peer devices. For more information, see Configuring SMLT links on non peer devices on page 112.
- On the two peer devices, you configure the IST peers. For more information, see Configuring IST peers on page 113.

## Configuring IST links

You can configure IST links in SMLT configurations on a single device. When you configure IST links on a single device, you must also repeat the same procedure to configure the IST links on the device at the other end of the IST.

## Configuring IST links on a single device

The following procedure describes how to configure an IST link on a single device. You must also perform this procedure to configure the other end of the IST.

Perform the following procedure to configure an IST link on a single device.

### Procedure steps

1. In the MultiLink Trunking Manager navigation pane, select a folder for one of the devices on which you want to configure the IST.
2. On the Content Pane Toolbar, click **Add**.
3. The Add MLT dialog box for a single node appears.
4. In the **Id** box, enter an ID number.
5. In the **Name** box, enter a name for the IST. Use the same name as for the other end of the IST.
6. In the **Ports** areas, select the ports that will be part of the IST.
7. For **Port Type**, select **trunk**.
8. In the **VlanId** box, select the VLAN. All ports on the SMLT configuration must belong to the same VLAN.
9. For the MLT Types, choose **istMLT**.
10. Click **Save**.

## Configuring SMLT links

When you configure SMLT links, you must configure the two ends of the link separately:

- You configure a splitMLT link on the peer device. For more information, see Configuring SMLT links on peer devices on page 111.
- You configure a normalMLT link on the non-peer device. For more information, see Configuring SMLT links on non peer devices on page 112.

### Configuring SMLT links on peer devices

Perform the following procedure to configure SMLT links on peer devices.

### Procedure steps

1. In the MultiLink Trunking Manager navigation pane, select a folder for the peer device on which you are configuring the link.
2. On the Content Pane Toolbar, click **Add**. The Add MLT dialog box for a single node appears. For more information, see Insert MLT dialog box for ERS 8000 or VSP 9xxx on page 105
3. In the **Id** box, enter a MLT ID. For SMLT links on peer devices, the MLT ID is ignored.
4. In the **Smlt Id** box, enter an SMLT ID number.

   The SMLT ID for the SMLT links on both peer devices must be the same.
5. In the **Name** box, enter a name for the MLT.
6. In the **Ports** area, select the ports on the peer device that are part of the SMLT link.
7. In the **VlanIds** box, select the VLAN. All ports on the SMLT configuration must belong to the same VLAN.
8. For the **MLT Type**, choose **splitMLT**.
9. In the **SMLT Id** field, enter the SMLT Id.
10. Click **Save**.

## Configuring SMLT links on non peer devices

You can configure all of the ports for both SMLT links of an SMLT configuration at the same time. For the MLT type, you choose normalMLT.

Perform the following procedure to configure SMLT links on a nonpeer device.

### Procedure steps

1. In the MultiLink Trunking Manager navigation pane, select a folder for the non-peer device on which you are configuring the link.
2. On the Content Pane Toolbar, click **Add**.

   The Add MLT dialog box for a single node appears.
3. In the **Id** box, enter an MLT ID.
4. In the **Name** box, enter a name for the MLT.
5. In the **Ports** area, select all of the ports on the non-peer device that will be part of the SMLT configuration.
6. In the **VlanIds** box, select the VLAN. All ports on the SMLT configuration must belong to the same VLAN.
7. For the **MLT Type**, choose **normalMLT**.
8. Click **Save**.

## Configuring IST peers

After configuring the IST links using the procedure in Configuring IST links on page 110, you must configure the IST peers.

Perform the following procedure to configure IST peers.

### Procedure steps

1. In the MultiLink Trunking Manager navigation pane, open the **Smlt Network** folder.
2. In the **Smlt Network** folder, click the **Inter-Switch Trunk** folder.

   The contents pane shows all of the devices with inter switch trunks configured.
3. For the **IstPeerIp** of each peer device, enter the IP address associated with the VLAN on the other peer in the SMLT configuration.
4. For the **IstVlanId** of both peer devices, enter the VLAN ID of the SMLT configuration.
5. All ports in an SMLT configuration must be in the same VLAN.
6. Click **Apply**.
7. For the **IstSessionEnable** of both peer devices, click the entry to select **true**.
8. Click **Apply**.

## Configuring a single port SMLT

Ports that are already configured as MLT or MLT-based SMLT cannot be configured as single port SMLT. You must first remove the split trunk and then reconfigure the ports as a single port SMLT.

Perform the following procedure to configure a single port SMLT.

### Procedure steps

1. In the MultiLink Trunking Manager navigation pane, under the **SMLT Network** folder, select the **Single-Port Smlt** folder.
2. On the Content Pane Toolbar, click **Add**.
3. The **Add Single-Port MLT** dialog box appears.
4. In the **IP Address** field, choose a device IP from the list.
5. Enter an **SMLT Id**.
6. In the **Port** field, choose a port.
7. Click **Save**.

## Job aid

The following table describes the items in the Insert SSmlt dialog box.

| Item | Description |
|---|---|
| IP Address | IP address of the network device. |
| Smlt Id | The Split MLT ID, an integer from 1 to 512.<br>• A read-only field with a value of 1 to 512 indicates the port single port SMLT ID assignment.<br>• A blank field indicates the port is not configured for single port SMLT. Find an unused SMLT ID by viewing the currently-used IDs. |
| Port | The slot or port number on the card. |

## Deleting a single port SMLT

Perform the following procedure to delete a single-port SMLT.

### Procedure steps

1. In the navigation pane, select the **single-port SMLT** folder.
2. On the Content Pane Toolbar, click **Delete**.

   The Delete dialog box appears, asking you to confirm the deletion.
3. Click **Yes**.

# Viewing MultiLink Trunking configurations

In the MultiLink Trunking Manager navigation pane, the navigation tree shows the IP addresses of discovered devices. Icons associated with IP addresses on the branches indicate the following types of MLTs:

- Trunk—a switch that links to another device in the network and has MLT configurations.
- No trunk—a switch that links to another device in the network but does not have an active MLT configured.
- Isolated—a switch connected only to a hub.

The following sections describe how to use MultiLink Trunking Manager:



## Viewing trunk connections

You can view the trunk connections for an MLT and configure new trunks to increase bandwidth.

Perform the following procedure to view trunk connections.

### Procedure steps

In the navigation pane, select a device that is represented by a trunk icon.

The Trunk table appears in the contents pane.

## Job aid

The following table describes the fields in the Trunk table.

| Field | Description |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Id | Number of the MLT (assigned by MultiLink Trunking Manager). |
| Name | Allows you to enter a name for the MLT. |
| PortMembers | Ports that are assigned to the MLT. |
| PortType | Type of port on the MLT (access or trunk). |
| VlanIds | VLAN to which the ports belong. |
| Enable | Indicates whether the MLT is enabled (true) or disabled (false). |
| IfIndex | Interface index, a number from 96 to 4097, that identifies the MLT to the software. |

| Field | Description |
|---|---|
| MltType | One of the following types of MLT links:<br>• normalMLT—used for normal MLT that do not use SMLT features.<br>• istMLT—used for IST (Inter-Switch Trunk) links between peer devices in SMLT configurations.<br>• splitMLT—used for SMLT links between peer devices and non-peer devices in SMLT configurations. |
| SmltId | Shows the SMLT ID number for split MLTs. |
| RunningType | Read only field displaying the MLT operational type:<br>• normalMLT<br>• istMLT<br>• splitMLT |

## Viewing no trunk configurations

No trunk configurations are links between two devices that are not MLTs. To have an MLT or trunk connection, there must be more than one connection between two devices. Often No trunk configurations are single links between two devices.

Perform the following procedure to view No trunk configurations.

### Procedure steps

In the MultiLink Trunking Manager navigation pane, select a device IP address above the IP address represented by a no trunk icon.

## Job aid

The following table describes the fields in the No Trunk table.

| Fields | Description |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Id | Number of the MLT. |
| Name | Name given to the MLT. |
| PortMembers | Ports that are assigned to the MLT. |
| PortType | Type of port on the MLT (access or trunk). |

| Fields | Description |
|---|---|
| VlanIds | VLAN(s) to which the ports belong. |
| Enable | Whether the MLT is enabled (true) or disabled (false). |
| IfIndex | Interface index, a number that identifies the MLT to the software. The range is:<br>• 512–519 for Passport (legacy) 1050, 1150, 1200, and 1250 devices<br>• 4096–4127 for Ethernet Routing Switch 8000 family devices |
| MltType | For SMLT configurations, shows one of the following types of MLT links:<br>• normalMLT—used for normal MLT that do not use SMLT features.<br>• istMLT—used for IST (inter-switch trunk) links between peer devices in SMLT configurations.<br>• splitMLT—used for SMLT links between peer devices and nonpeer devices in SMLT configurations. |
| SmltId | Shows the SMLT ID number for split multilink trunk links. |
| RunningType | Read only field displaying the MLT operational type:<br>• normalMLT<br>• istMLT<br>• splitMLT |

## Viewing isolated devices

Isolated devices have one or more connections to a hub or bus, but are not connected to another switch.

Perform the following procedure to view the isolated devices.

### Procedure steps

In the MultiLink Trunking Manager navigation tree, expand the Isolated folder, and then select an isolated device.

The Isolated Device table appears in the contents pane.

## Job aid

The following table describes the fields in the Isolated Device table.

| Field | Description |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Id | Number of the MLT. |
| Name | Name given to the MLT. |
| PortMembers | Ports that are assigned to the MLT. |
| PortType | Type of port on the MLT (access or trunk). |
| VlanIds | VLAN(s) to which the ports belong. |
| Enable | Indicates whether the MLT is enabled (true) or disabled (false). |
| IfIndex | Interface index, a number that identifies the MLT to the software. The range is:<br>• 512–519 for Passport (legacy) 1050, 1150, 1200, and 1250 devices<br>• 4096–4127 for Ethernet Routing Switch 8000 family devices |
| MltType | For SMLT configurations, shows one of the following types of MLT links:<br>• normalMLT—used for normal MLT that do not use SMLT features.<br>• istMLT—used for IST (inter-switch trunk) links between peer devices in SMLT configurations.<br>• splitMLT—used for SMLT links between peer devices and non-peer devices in SMLT configurations. |
| SmltId | Shows the SMLT ID number for split multilink trunk links. |
| RunningType | Read only field displaying the MLT operational type:<br>• normalMLT<br>• istMLT<br>• splitMLT |

## Viewing interswitch trunks

Inter-switch trunks are links between peer devices in SMLT configurations.

Perform the following procedure to view interswitch trunks.

### Procedure steps

In the MultiLink Trunking Manager navigation tree, select the **Interswitch Trunk** under the Smlt Network folder. The inter-switch trunk table appears in the contents pane.

## Job aid

The following table describes the fields in the inter-switch trunk table.

| Field | Description |
|---|---|
| Device | Identifies the device on which the IST is configured. |
| IstSession Enable | Lets you enable or disable the IST session. |
| IstPeerIp | Lets you enter the IP address of the peer device at the other end of the IST. |
| IstVlanId | Lets you enter the VLAN ID for the IST. |

## Viewing SMLTs

An SMLT improves the reliability of a Layer 2 (L2) network operating between a building's user access switches and the network center aggregation switch. It does so by providing loadsharing among all the links and fast failover in case of link failures. For more information about configuring single port SMLTs, see Viewing single port SMLTs on page 120.

Perform the following procedure to view SMLT.

### Procedure steps

In the MultiLink Trunking Manager navigation pane, select the any device node under **SMLT** folder. The SMLT table appears in the contents pane.

## Job aid

The following table describes the fields in the SMLT table.

| Field | Description |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Id | Number of the MLT (assigned by MultiLink Trunking Manager). |
| MltType | One of the following types of MLT links: |

| Field | Description |
|---|---|
| | • normalMLT–Use for normal MLT that do not use SMLT features.<br>• istMLT– Use for IST (inter-switch trunk) links between peer devices in SMLT configurations.<br>• splitMLT–Use for SMLT links between peer devices and non-peer devices in SMLT configurations. |
| SmltId | Shows the SMLT ID number for split MLTs. |
| RunningType | Read only field displaying the MLT operational type:<br>• normalMLT<br>• istMLT<br>• splitMLT |

## Viewing single port SMLTs

Perform the following to view single-port SMLT.

### Procedure steps

In the MultiLink Trunking Manager navigation pane, select the **Single-port SMLT** under the Smlt Network folder. The single-port SMLT table appears in the contents pane.

## Job aid

The following table describes the fields in the Single-port SMLT table.

| Field | Description |
|---|---|
| Device | IP address, system name, or host name of the device. |
| Smlt ID | The Split MLT ID, an integer from 1 to 512.<br>• A read-only field with a value of 1 to 512 indicates the port's single port SMLT ID assignment.<br>• A blank field indicates the port is not configured for single port SMLT. Find an unused SMLT ID by viewing the currently-used IDs. |
| Port | The slot/port number for the port. |
| OperType | Read only field displaying the MLT operational type: |

| Field | Description |
|---|---|
| | • normalMLT<br>• istMLT<br>• splitMLT |
| VlanIDs | VLAN IDs for the single-port SMLT. |

## Updating information in the MultiLink Trunking Manager

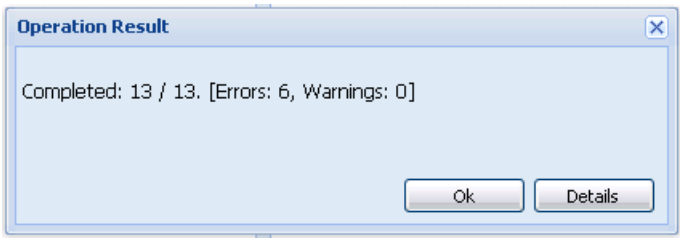
You can discover the devices in the MultiLink Trunking Manager window with MultiLink trunk information polled from the network devices. You can use this feature to load any updated information that took effect since you opened MultiLink Trunking Manager.

Perform the following procedure to discover the MultiLink trunk information.

### Procedure steps

1. On the MultiLink Trunking Manager window, click **Discover MultiLink Trunks** on Navigation pane tool bar.

   COM rediscovers all trunks, and the operation result dialog box appears.




2. Click **Ok** to view the MultiLink Trunking Manager window.

   **OR**

   Click **Details** to view the errors and warnings, if any.

## Viewing devices and MLT links on the topology map

COM displays the topology information from MultiLink Trunking Manager in the contents pane.

Perform the following procedure to highlight devices and their MLTs in COM.

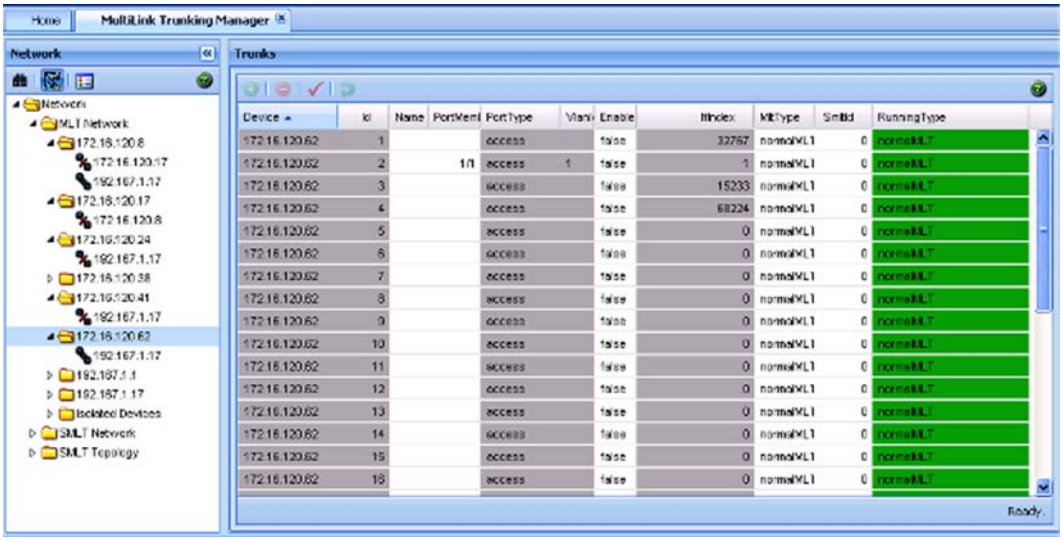
### Procedure steps

1. In the navigation pane, select a device with a trunk connection.

The Trunk table appears in the MultiLink Trunking Manager contents pane.

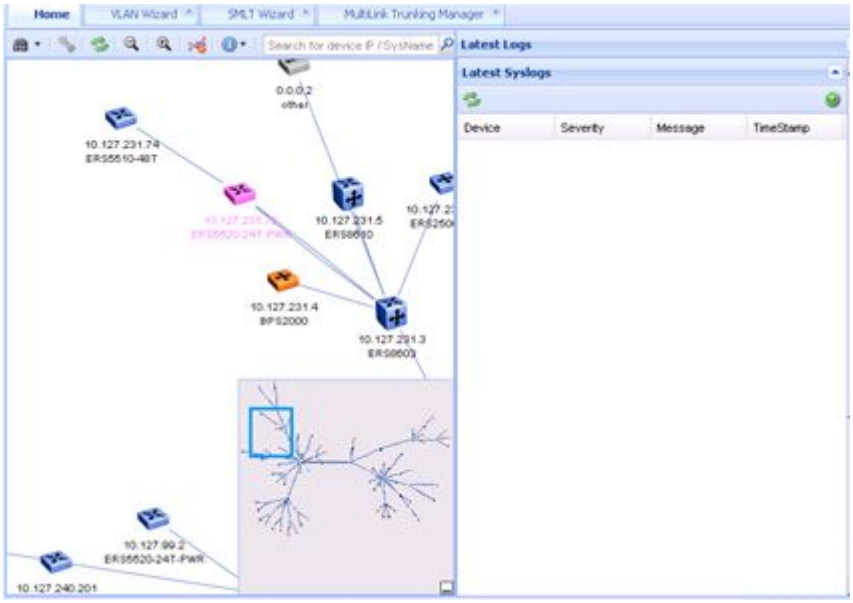
2. From the MultiLink Trunking Manager menu bar, choose **Highlight On Topology**.

   The trunk table is highlighted.




3. Return to the MultiLink Trunking window.

   The topology view appears in the COM contents pane with devices connected to the MLT highlighted in blue and the ports in the MLT or SMLT highlighted in green.



# Chapter 6: Using Security Manager

This section describes Security Manager and how to use it to manage access to the devices in your network.

**Navigation**



## About Security Manager

Security Manager provides a centralized location where you can manage access to the devices in your network. You can use Security Manager to:

- group together devices to which you want to apply to same passwords and access policies
- choose the authentication method for a security group (either RADIUS or TACACS authentication)
- choose different types of management access (such as CLI, Web, SNMP, or SSH access)
- create access policies and apply them to security groups, or to individual devices within a security group
- synchronize, change, and view passwords and access policies

**Important:**

This functionality is not to be confused with the Device and Server Credentials offered through UCM-CS services. The functionality described in this chapter addresses adding/deleting/changing the passwords on the device itself.

**Note:**

Security Manager functionality for VSP 9xxx works the same as ERS 8600. SSH device groupings include VSP 9xxx devices with the ERS 8000 family of devices. IPv6 support for

Radius server is not supported. The tab for IPv6 Radius Server is present, but the add functionality filters out VSP devices.

## Supported devices

The following table lists the devices that are supported by Security Manager.

**Table 21: Devices supported by the Security Manager**

| Type of access | Device type |
|---|---|
| CLI and Web | Passport 1050/1150/1200/1250 |
| | Ethernet Routing Switch 8xxx |
| | Ethernet Routing Switch 16xx 2.0 or later (WEB only) |
| | Virtual Services Platform 9xxx |
| Access Policy and RADIUS server | Passport 1050/1150/1200/1250 |
| | Ethernet Routing Switch 8xxx |
| | Ethernet Routing Switch 16xx 2.0 or later |
| | Virtual Services Platform 9xxx |
| SNMP | Ethernet Routing Switch 8xxx (except for 83xx) earlier than 3.7 |
| | Passport 1050/1150/1200/1250 |
| SNMPv3 | Ethernet Switch 325, 425, 460, 470 |
| | Ethernet Routing Switch 55xx 56xx |
| | Ethernet Routing Switch 45xx |
| | Ethernet Routing Switch 25xx |
| | Ethernet Routing Switch 8xxx 3.3 and up (8300 all) |
| | Ethernet Routing Switch 16xx 2.0 or later |
| | Virtual Services Platform 9xxx |
| | Wireless Controller 8xxx |
| SSH | Ethernet Routing Switch 8300 2.1.1 and up |
| | Ethernet Routing Switch 16xx 2.0 or later |
| | Ethernet Routing Switch 8xxx (excluding 8300) 3.2.1 and up |
| | Business Policy Switch 2000 2.5.0 and up |
| | Ethernet Switch 460, 470 2.5.0 and up |

| Type of access | Device type |
|---|---|
| | Ethernet Routing Switch 55xx 56xx 4.0.0 and up |
| | Ethernet Switch 425/420/325 3.0 and up |
| | Ethernet Routing Switch 45xx 4th version digit odd |
| | Virtual Services Platform 9xxx |
| | Wireless Controller 8xxx |
| TACACS | Ethernet Routing Switch 8600 5.1 and up |
| | Ethernet Routing Switch 8300 2.2 and up |
| | Virtual Services Platform 9xxx |

# Starting Security Manager

Perform the following procedure to start Security Manager.

### Procedure steps

1. In the Configuration and Orchestration Manager window Navigation pane, click the **+** sign to open the list of Managers.
2. Click on the **Security Manager** icon in the navigation tree.

   The Security Manager dialog box appears.

# Using the Security Manager window

The following figure shows the Security Manager window.

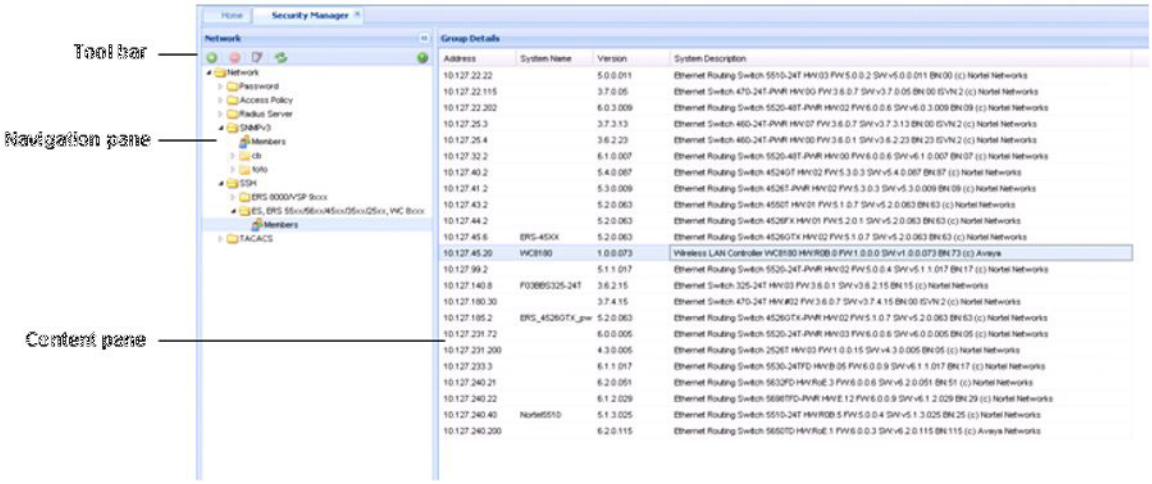



**Figure 16: Security Manager window**

The following table describes the parts of the Security Manager window.

**Table 22: Parts of the Security Manager window**

| Part | Description |
|---|---|
| Tool bar | Provides quick access to commonly used Security Manager commands. For more information, see Toolbar and Contents pane buttons on page 126. |
| Navigation pane | Allows you to navigate security settings for the current network devices. For more information, see Navigation pane on page 127. |
| Contents pane | Displays elements of the folder or element selected on the navigation pane. For more information, see Contents pane on page 128. |

# Toolbar and Contents pane buttons

The following table describes the Security Manager menu bar commands and toolbar buttons.

**Table 23: Security Manager Menu bar commands and toolbar buttons**

| Command | Tool bar button | Description |
|---|---|---|
| Add |  | Creates a new security group that contains devices of the current domain type (CLI, WEB, SNMP, Access Policy, Radius Server, SSH, TACACS). |
| Delete |  | Removes the selected security group from Security manager. |

| Command | Tool bar button | Description |
|---|---|---|
| Edit | | Modifies the current device list contained inside the security group. |
| Reload | | Rediscovers the network and reloads Security Manager with the latest information. For more information, see Reloading Security Manager on page 131. |
| Revert Changes | | Undo any unapplied change you made to a record. |
| Apply Changes | | Applies your settings to all of the devices in the security group. |

## Navigation pane

The Security Manager navigation pane displays a hierarchical folder tree that you can use to navigate to security groups.

The following figure shows the navigation pane of the Security Manager window.


**Figure 17: Security Manager navigation pane**

**Note:**

Not all device groupings are supported on all devices that COM supports. If you select a device grouping that is not supported, the tab appears, but no further data appears because the MIB attributes are not present. Therefore you are not permitted to add a device.

## Contents pane

The content pane only displays detailed information for each device selected in the navigation pane. For each device you select in the navigation pane, the contents pane displays the Address, System Name, Version, and System Description.

# Creating and managing security groups

The following sections describe how to use Security Manager to create and modify security groups:


- Creating security groups on page 128
- Adding new devices to a security group on page 129
- Saving security group settings on page 130
- Reloading Security Manager on page 131
- Editing Security Groups on page 131
- Deleting security groups on page 132


## Creating security groups

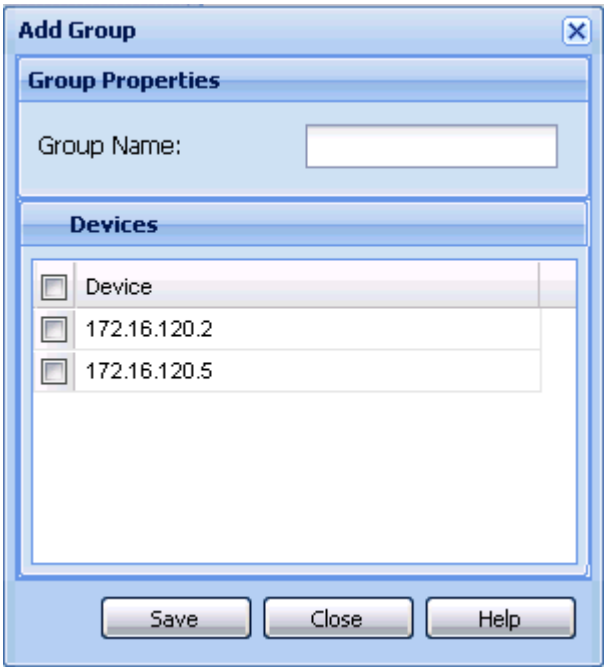
Perform the following procedure to create a security group.

### Procedure steps

1. In the navigation pane, browse and select one of the following application folders:
   - Access Policy
   - Radius Server
   - SNMPv3
   - SSH
   - TACACS

   **OR** Under the Password folder, select **CLI**, **WEB** or **SNMP**.
2. On the Toolbar, click **Add** (the + sign).

   The Add Group dialog box appears.




3. In the **Group Name** field, type a new group name.
4. In the device list, choose the devices that you want to include in the new security group. **OR** Click the device check box to select all devices at the same time.
5. Click **Save**.

   The Security Manager creates a new security group containing the selected devices.

## Job aid

The following table describes the Add Group dialog box.

| Part | Description |
|---|---|
| Group Name | Allows you to enter a name for the new security group. The new security group should have a unique name. |
| Device list | Displays a list of devices that you can add to the new security group. |

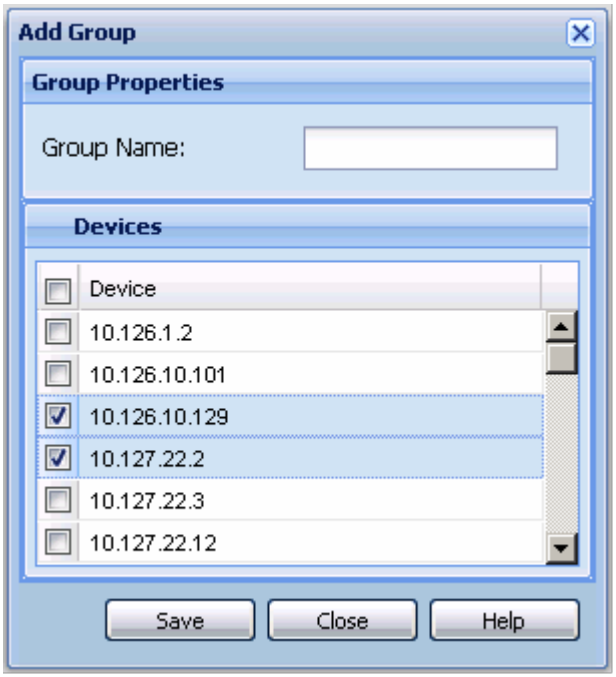
## Adding new devices to a security group

Perform the following procedure to add additional devices to an already existing security group.

### Procedure steps

1. Open the folder for the security group to which you want to add a device.
2. Click **Add**.

   The Add group dialog box appears.




3. If you want to change the name of the group, type the new name in the Group Name field.
4. Select the check box corresponding to the devices you want to add to the group.
5. Click **Save**. The device gets added to the group and appears on the Navigation pane under the group.

   If you do not want to add the device, click **Close**.

## Saving security group settings

Security Manager saves all security group information to the local hard disk when you close the Security Manager window. When you restart Security Manager, it reloads the saved security group settings.

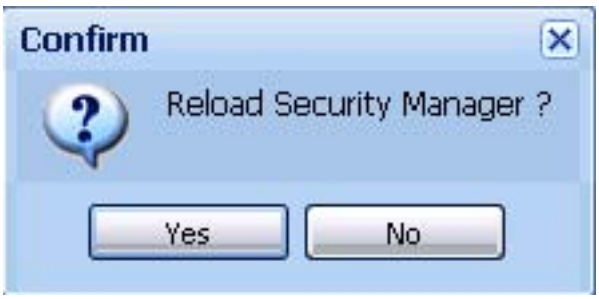
## Reloading Security Manager

Security Manager allows you to refresh the information in the window with security information polled from the network devices. You can use this feature to load any updated information that took effect since you opened Security Manager.

Perform the following procedure to reload the security information.

### Procedure steps

1. On the Security Manager tool bar, click **Reload Security manager**. A dialog box appears asking for confirmation to reload the Security Manager.




2. Click **Yes** to reload the Security Manager.

   COM reloads topology information from the network devices and refreshes the Security Manager window with it.

3. If you do not want to reload the Security Manager, click **No**.

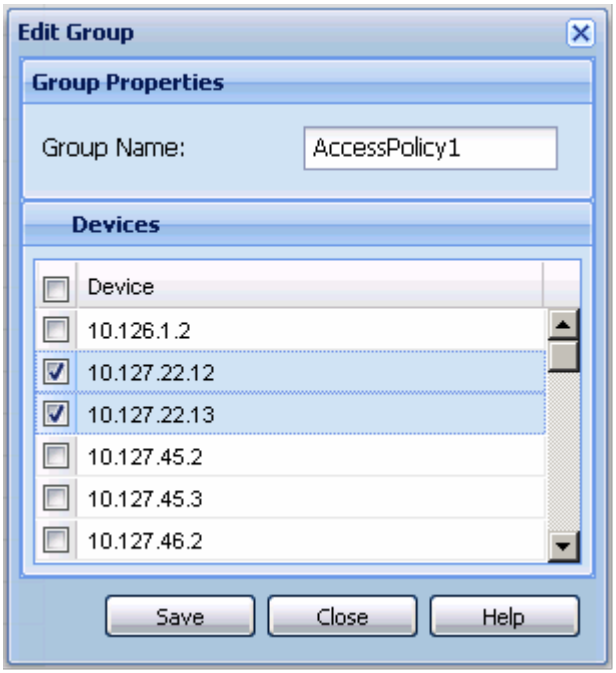
## Editing Security Groups

Perform the following procedure to edit selected devices in a security group.

### Procedure steps

1. In the navigation pane, browse and select one of the following application folders:
   - Access Policy
   - Radius Server
   - SNMPv3
   - SSH
   - TACACS

   **OR** Under the Password folder, select **CLI**, **WEB** or **SNMP**.
2. Click the device in the security group folder that requires editing..
3. Click **Edit**. The Edit group dialog box appears.




4. If you want to change the name of the group, type the new name in the Group Name field.
5. Click **Save**.

## Deleting security groups

Perform the following procedure to delete a security group.

### Procedure steps

1. In the navigation pane, select the security group that you want to delete.
2. On the Tool bar, click **Delete** (the - symbol). A dialog box appears asking for confirmation to delete security group.
3. Click **Yes** to delete the security group.

# Configuring the authentication method

You can specify a centralized server—such as a RADIUS server or a TACACS server—to authenticate the credentials of users that access devices in a security group. If you do not specify a centralized server, users are authenticated locally on the device by default.

The following sections describe how to use Security Manager to configure the authentication method used by security groups in your network:



# Configuring RADIUS authentication

The following sections provide information about using a RADIUS server with a security group.



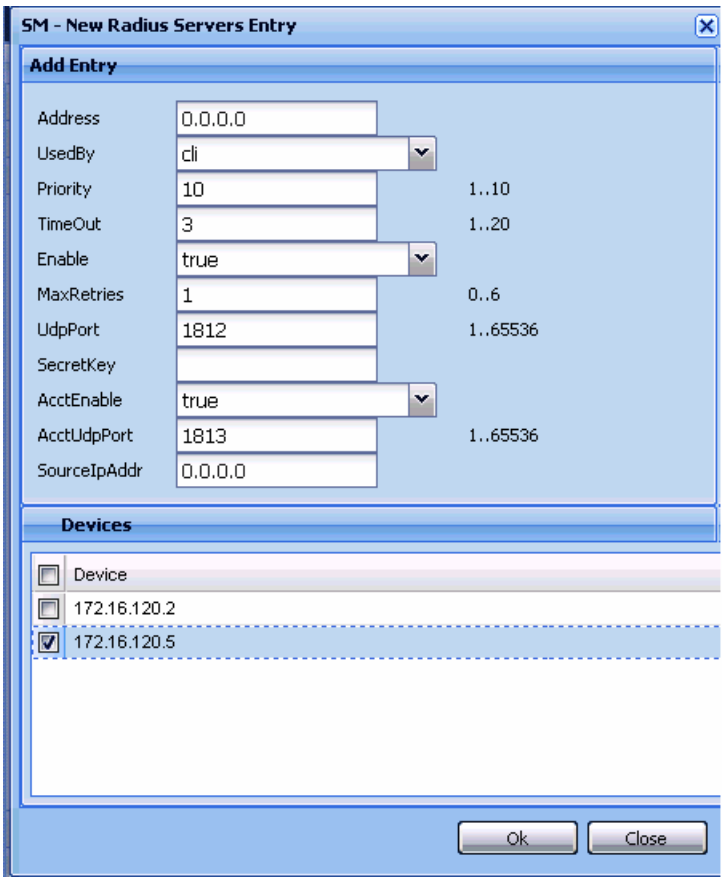
## Adding RADIUS servers

Perform the following procedure to add a RADIUS server to a security group.

### Procedure steps

1. Under the **Radius Server** folder in the navigation pane, click the folder for the security group for which you want to add a RADIUS server.
2. In the contents pane, click the **Radius Servers** tab.
3. On the Tool bar, click **Add** (the + symbol).

   The New Radius Servers Entry dialog box appears.




**Important:**

The default values for the RADIUS port (UdpPort) and the RADIUS accounting port (AccUdpPort) are 1812 and 1813, respectively. Many legacy servers use default ports 1645 and 1646, respectively. You must ensure that the ports specified in this table match the ports on which your RADIUS servers are listening.

4. Set the dialog box parameters as appropriate.
5. Click **OK**.

   The Security Manager creates a new entry on the Radius Server tab.

   Security Manager applies your changes only to the changed devices in the security group.

## Job aid

The following table describes the New Radius Servers Entry dialog box.

| Part | Description |
|---|---|
| Address | Specifies the IP address of the new server. |

| Part | Description |
|---|---|
| UsedBy | Configures accesses for cli, igap, snmp and eap as they require RADIUS server authentication. |
| Priority | Specifies the priority between 1 and 10 of the new RADIUS server. |
| TimeOut | Specifies the number of seconds, between 1 and 10, between retransmissions from the client to the RADIUS server. |
| Enable | Enables the RADIUS server. |
| MaxRetries | Specifies the maximum number of retries, between 1 and 6, to allow requests to the server. |
| UdpPort | Specifies the UDP port number, between 1 and 65536, that the client will use to send requests to the server.<br>The default value is 1812. |
| SecretKey | Specifies the secret key of the authentication client. |
| AccEnable | Allows you to enable accounting on the RADIUS server. |
| AccUdpPort | Allows you to enter the UDP port number of the RADIUS accounting server.<br>The default value is 1813. |
| SourceIpAddr | Configures the source IP address for RADIUS packets. |

The following table describes the Radius Servers tab.

**Table 24: Radius Servers tab of the Attributes folder**

| Part | Description |
|---|---|
| Address | Allows you to enter the IP address of the new server. |
| UsedBy | Configures accesses for cli, igap, snmp and eap as they require RADIUS server authentication. |
| Priority | Allows you to enter the priority between 1 and 10 of the RADIUS server. |
| TimeOut | Allows you to enter the number of seconds, between 1 and 10, that you require between retransmissions from the client to the RADIUS server. |
| Enable | Allows you to enable the RADIUS server. |
| MaxRetries | Allows you to enter the maximum number of retries, between 1 and 6, that you require to allow requests to the server. |
| UdpPort | Allows you to enter the UDP port number, between 1 and 65536, that the client will use to send requests to the server.<br>**Important:**<br>The UDP port value set for the client must be the same as the value set for the RADIUS server. |

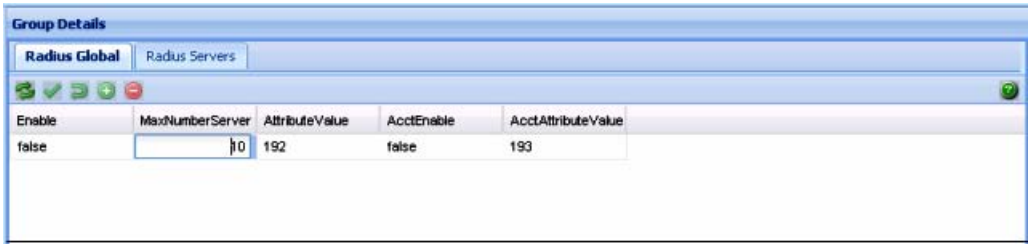
| Part | Description |
|---|---|
| SecretKey | Allows you to enter the secret key of the authentication client. |
| AccEnable | Allows you to enable accounting on this RADIUS server. |
| AccUdpPort | Allows you to enter the UDP port number of the RADIUS accounting server. |
| SourceIpAddr | Configures the source IP address for RADIUS packets. |

## Setting global RADIUS server parameters

Perform the following procedure to set global RADIUS server parameters.

### Procedure steps

1. Under the **Radius Server** folder in the navigation pane, open the folder for the security group for which you want to set global RADIUS server parameters.
2. In the contents pane, click the **Radius Global** tab.




3. Set the parameters as appropriate.
4. On the Security Manager tool bar, click **Apply Changes**.

   Security Manager applies your changes only to the changed devices in the security group.

## Job aid

The following table describes the Radius Global tab.

| Part | Description |
|---|---|
| Enable | Allows you to enable or disable the RADIUS authentication feature globally. |
| MaxNumber Server | Allows you to set the maximum number of servers, between 1 and 10, that you want to use. |
| Attribute Value | Allows you to set the value for Access-Priority attribute. The default is 192. |

| Part | Description |
|---|---|
| AcctEnable | Allows you to enable or disable accounting on this RADIUS server. |
| AcctAttribute Value | Allows you to set the account attribute value, ranging from 192 to 240. This attribute is vendor-specific and is different from the attribute value used for authentication. |

## Removing RADIUS servers

Perform the following procedure to remove a RADIUS server from a security group.

### Procedure steps

1. Under the **Radius Server** folder in the navigation pane, open the folder for the security group for which you want to remove a RADIUS server.
2. In the contents pane, click the **Radius Servers** tab.
3. Click any cell of the entry for the RADIUS server that you want to remove.
4. On the Tool bar, click **Delete** (the - symbol).

   The system asks for confirmation on deleting the entry.
5. Click **Yes** to delete the selected entry.

   Security Manager deletes the selected entry in the RADIUS server table.

# Configuring TACACS authentication

You can use Security Manager to add, delete, and modify attributes for TACACS servers for all the devices in a security group.

The following topics are covered in this section:



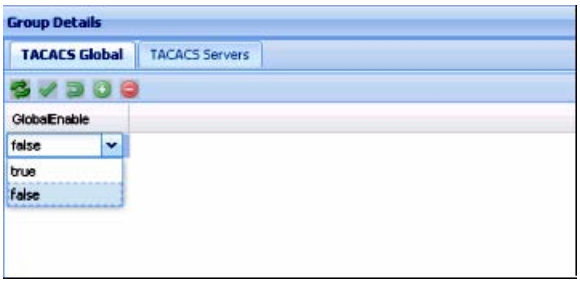
## Enabling or disabling TACACS Global

Security Manager allows you to enable and disable TACACS globally within a security group.

Perform the following procedure to enable or disable TACACS globally within a security group.

### Procedure steps

1. Click on the required security group.
2. Click **TACACS Global** tab.
3. Select **True** to enable and **False** to disable the TACACS globally within the security group.




## Adding TACACS servers

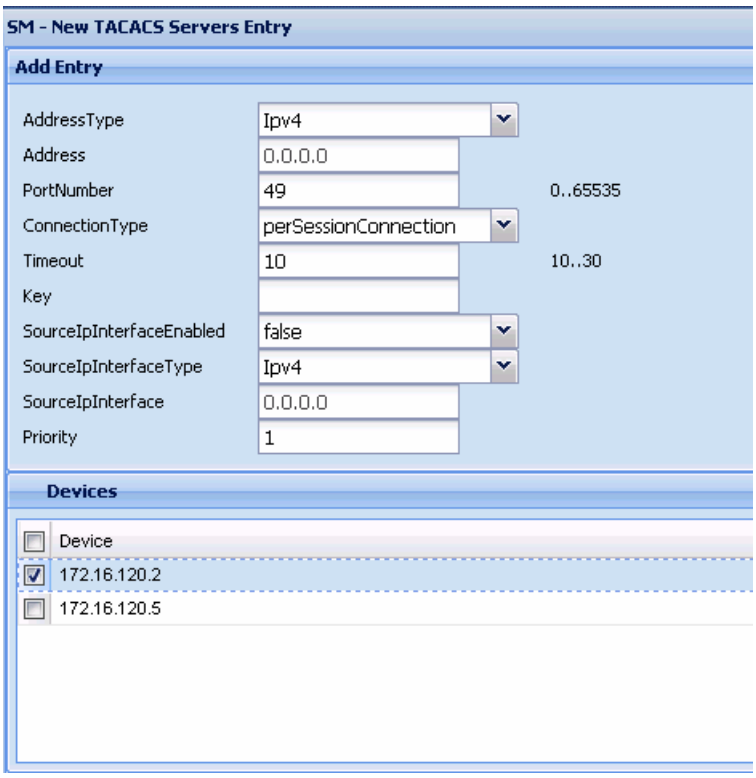
You can add TACACS servers using the Security Manager.

Perform the following procedure to add a TACACS server:

### Procedure steps

1. In the navigation pane, click the folder for the security group for which you want to configure TACACS.
2. Select the required device.
3. In the Contents pane, click the **TACACS Servers** tab.
4. On the Toolbar, click **Insert** (the plus symbol).

   The New TACACS Servers Entry dialog box appears.




5. Select appropriate settings for the TACACS server to be added.
6. Click **OK**.

   The Security Manager adds the new TACACS server.

## Job aid

The following table describes New TACACS Server dialog box.

**Table 25: New TACACS Server dialog box fields**

| Part | Description |
|---|---|
| Address Type | Specifies the type of address of the TACACS server. |
| Address | Specifies the server address. |
| Port number | Specifies the port number to access the server. |
| Connection type | Specifies the single connection or per session connection to the server. |
| Timeout | Specifies the number of seconds, between 1 and 10, between retransmissions from the client to the RADIUS server. |
| Key | Specifies the key. |

| Part | Description |
|---|---|
| SourceIPInterfaceEnabled | Specifies the IP address of the interface whether it is enabled. |
| SourceIPInterfaceType | Specifies the type of the IP address. |
| SourceIPInterface | Specifies the IP address of the interface. |
| Priority | Specifies the priority, between 1 and 10, of the new TACACS server. |

## Deleting TACACS server entries

Perform the following procedure to delete a TACACS server entry.

### Procedure steps

1. Click the folder for the security group from which you want to delete a TACACS entry.
2. In the security group folder, click the desired device.
3. In the Contents pane, click the **TACACS Servers** tab.
4. On the TACACS Servers tab, click the cell of the TACACS Server that you want to delete (entire row is deleted).
5. On the Toolbar, click **Delete**(the - symbol).
6. Click **Yes** to delete the security group.

   Security Manager deletes the TACACS server entry.

# Configuring management access

You can use Security Manager to configure how management applications can access the devices in a security group.

The following sections describe how to configure the type of access permitted for devices in a security group:


- Configuring a security group for SSH access on page 141
- Configuring a security group for CLI access on page 146
- Configuring a security group for Web access on page 148
- Configuring a security group for SNMP v1/v2c access on page 149
- Configuring a security group for SNMP v3 access on page 150

# Configuring a security group for SSH access

This section describes how to configure SSH security groups, SSH Bulk passwords, and related properties.



## Creating SSH security groups

Perform the following procedure to create an SSH security group.

### Procedure steps

1. In the navigation pane, click the **SSH** folder.

   SSH contains two subtype domains, one to group devices from ERS8600 family and VSP 9xxx family, and the other for ES/ERS55xx/ERS45xx/35xx/25xx and WC 8xxx compatible devices.
2. Select a subdomain.
3. Click **Add** button (the + sign from Navigation Pane tool bar).

   The Add Group dialog box appears.
4. In the **Group Name** field, type a new group name.
5. Select devices (not all SSH capable devices are in Devices list, just the ones filtered to be compliant to the current selected subgroup).
6. Click **Save**.

   The Security Manager creates a new SSH security group containing the selected devices.

## Configuring SSH Bulk Passwords

In Security Manager, you can use Secure Shell (SSH) to configure the CLI user name and password for all the devices in a security group. You can also use SSH to configure the SNMP communities for the security group on ERS 55xx/35xx/45xx/25xx, Ethernet Switch devices, and VSP 9xxx devices. Using an SSH connection to make these configuration changes

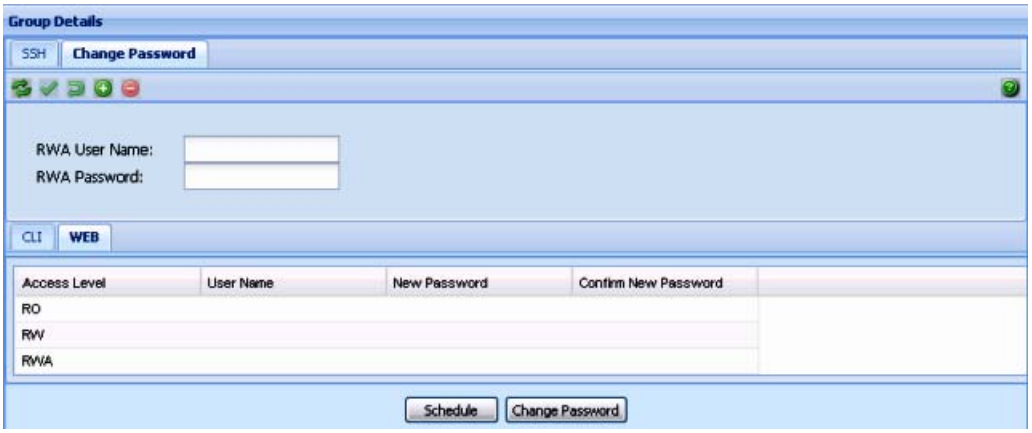
ensures the confidentiality of the user names and passwords of the devices in the security group.

Perform the following procedure to configure SSH access for a security group.

### Procedure steps

1. Under the SSH folder in the navigation pane, click the folder for the security group for which you want to configure SSH access.
2. In the contents pane, click the **Change Password** tab.

   The Change Password tab appears.




3. For ERS 8000 and VSP 9xxx devices, enter the current user name for the devices in the **RWA Username** field.
4. Enter the current password for the devices in the **RWA Password** field.
5. Update the CLI and WEB passwords as follows:
   - To update the password for the CLI for ERS 55xx/35xx/45xx/25xx or Ethernet Switch devices:
     - Click the **CLI** tab.
     - In the **Password** column, double-click a password cell to activate it.
     - Enter the desired password.
     - In the adjacent **Confirm Password** cell, re-enter the desired password.
   - To update the SNMP community string for ERS 55xx/35xx/45xx/25xx or Ethernet Switch devices.
     - Click the **WEB** tab.
     - Update the required fields in the table.

       You can update the user name and password for the following three access levels:

       - RO

- RW
- RWA

- To update the password for the CLI for non-ERS 55xx/35xx/45xx/25xx devices:
  - Choose the **CLI** tab.
  - In the **User ID** column, double-click a user ID cell to activate it.
  - Enter the desired UserName.
  - In the **Old Password** field, enter the old password.
  - In the **Confirm Old Password** field, reenter the old password.
  - In the **New Password** field, enter the new password.
  - In the **Confirm New Password** field, reenter the new password.

6. Initiate the password change:
   - To initiate the password change immediately, click **Change Password**. The status bar shows the current status. After all devices have finished the password change, the status is displayed as Done.
   - To initiate the password change at a later time, click **Schedule**, and complete the **Schedule Password Change** dialog box.

   **Important:**

   Password change is applicable only to fields with data. Empty fields are not considered. All passwords are shown as asterisks (***), not plain text.
7. In the **Name** box, enter a name to assign to the task. The name distinguishes this task from other scheduled tasks for easy identification.
8. Use the **Schedule** option to set a schedule for the task.
   - When you choose **One Time Only**, Scheduler Server executes the task only once at the time you specify.
   - When you choose **Every Month on the __ Day**, Scheduler Server executes the task every month on the day of the month and at the time you specify.
   - When you choose **Every Week on __**, Scheduler Server executes the task every week on the day of the week and at the time you specify.
   - When you choose **Every __ Days**, Scheduler Server executes the task at the interval and time you specify.
   - When you choose **Every Day**, Scheduler Server executes the task every day at the time you specify.
9. In the **Date** box, set the date and time you want Scheduler Server to execute the task.
10. Click **Set**.

    Scheduler Server schedules the task and executes it at the set time.

### Job aid

The following table describes the Schedule Password Change dialog box.

| Part | Description |
|---|---|
| Id | Specifies the ID of this schedule. |
| Name | Specifies the name of this schedule. |
| Log File | Specifies the name of the Log file. |
| Schedule-One time only | Specifies a password change scheduled only once. |
| Schedule-Every Month on The nth Day | Specifies a password change for every month on the specified day. |
| Schedule-Every week on | Specifies a password change for every week on the specified day |
| Schedule-Every n days | Specifies a password change for every n days. |
| Schedule-Every Day | Specifies a password change every day. |
| Select date/time | Specifies the date and time from which the scheduler should be activated. |
| Set | Fixes the time at which the password must change. |

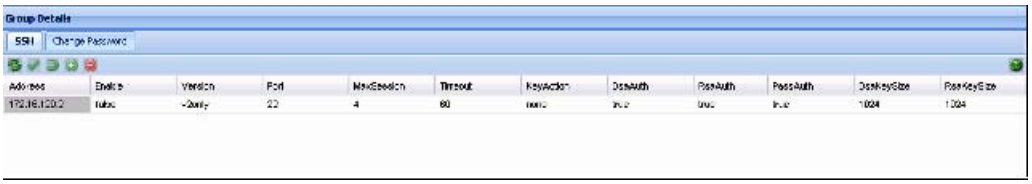
## Configuring SSH properties for ERS 8000 and VSP 9xxx security groups and devices

Perform the following procedure to configure SSH properties for an ERS 8000 or VSP 9xxx security group.

### Procedure steps

1. Under the SSH folder in the navigation pane, click the folder for the security group for which you want to configure SSH properties.
2. In the contents pane, click the **SSH** tab.

   The SSH tab appears.



3. Select and modify any of the fields in the table. See the job aid below for descriptions on each field.
4. Click **Apply Changes**.

### Job aid

The following table describes the SSH tab.

| Part | Description |
|---|---|
| Address | Specifies the IP address for the device. |
| Enable | Enables or disables SSH. Set to false to disable SSH services. Set to true to enable SSH services. Set to secure to enable SSH and disable insecure services SNMP, TFTP, and Telnet. The secure mode will take effect after restart. Default is false. |
| Version | Sets the SSH version. Set to both or v2only. Default is v2only. |
| Port | Sets the SSH connection port number. Default is 22. |
| Max Session | Sets the maximum number of SSH sessions allowed.<br>The value can be from 0 to 8. Default is 4. |
| Timeout | Sets the SSH authentication connection timeout in seconds. Default is 60 seconds. |
| KeyAction | Sets the SSH key action. |
| DsaAuth | Enables or disables DSA authentication. Default is enabled. |
| RsaAuth | Enables or disables RSA authentication. Default is enabled. |
| PassAuth | Enables or disables password authentication. Default is enabled. |
| DsaKeySize | Specifies the DSA key size. Value can be from 512 to 1024. Default is 1024. |
| RsaKeySize | Specifies the RSA key size. Value can be from 512 to 1024. Default is 1024. |

## Configuring SSH properties for ERS 55xx/35xx/45xx/25xx and Ethernet Switch security groups

Perform the following procedure to configure SSH properties for an ERS 55xx/35xx/45xx/25xx or Ethernet Switch security group.

### Procedure steps

1. Under the **SSH** folder in the navigation pane, click the folder for the security group for which you want to configure SSH properties.
2. In the contents pane, click the **SSH** tab.

   The SSH tab appears.

3. Select and modify any of the fields in the table. See the job aid below for descriptions on each field.
4. Click **Apply Changes**.

### Job aid

The following table describes the SSH tab:

| Part | Description |
|---|---|
| Device Address | Specifies the IP address for the device. |
| Enable | Enables or disables SSH. Set to false to disable SSH services. Set to true to enable SSH services. Set to secure to enable SSH and disable insecure services SNMP, TFTP, and Telnet. The secure mode will take effect after reboot. Default is false. |
| Version | Sets the SSH version. Set to both or v2only. Default is v2only. |
| Port | Sets the SSH connection port number. Default is 22. |
| Timeout | Sets the SSH authentication connection timeout in seconds. Default is 60 seconds. |
| KeyAction | Sets the SSH key action. |
| DsaAuth | Enables or disables DSA authentication. Default is enabled. |
| PassAuth | Enables or disables password authentication. Default is enabled. |

## Deleting SSH security groups

Perform the following procedure to delete an SSH security group.

### Procedure steps

1. In the navigation pane, select the SSH security group that you want to delete.
2. On the Tool bar, click **Delete** (the - symbol).

   The system asks for confirmation on deleting the security group.
3. Click **Yes** to delete the security group.

   Security Manager delete the selected security group.

   If you do not wish to delete the security group, click **No**.

# Configuring a security group for CLI access

You can use Security Manager to configure the Command Line Interface (CLI) user names and passwords for all of the devices in a security group.

Perform the following procedure to configure CLI access for a security group.

### Procedure steps

1. Under the CLI folder in the navigation pane, click the folder for the security group for which you want to configure CLI access.
2. Click any field in the Content pane and edit the contents of the field.

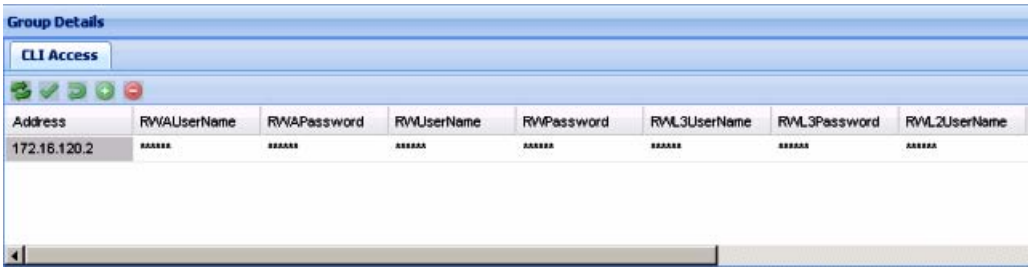



**Figure 18: CLI Access tab**

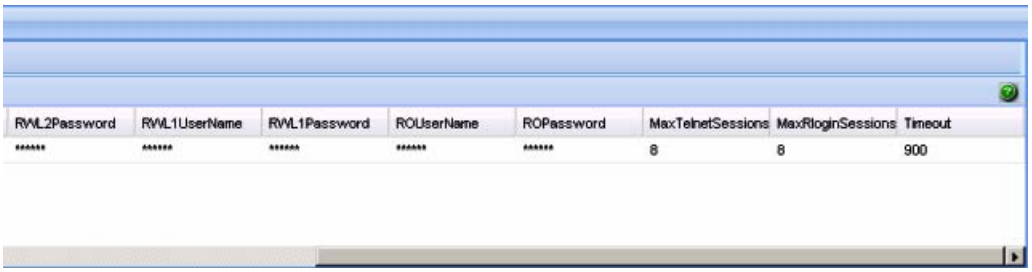



**Figure 19: CLI Access tab (contd.)**

3. On the Security Manager tool bar, click **Apply Changes**.

   Security Manager applies your changes only to the changed devices in the security group.

## Job aid

The following table describes the CLI Access tab.

| Part | Description |
|---|---|
| Address | Specifies the IP address of the CLI account. |
| RWAUserName | Specifies the user name for the read/write/all CLI account. |
| RWAPassword | Specifies the password for the read/write/all CLI account. |
| RWUserName | Specifies the user name for the read/write CLI account. |
| RWPassword | Specifies the password for the read/write CLI account. |
| RWL3UserName | Specifies the user name for the Layer 3 read/write CLI account. |

| Part | Description |
|---|---|
| RWL3Password | Specifies the password for the Layer 3 read/write CLI account. |
| RWL2UserName | Specifies the user name for the Layer 2 read/write CLI account. |
| RWL2Password | Specifies the password for the Layer 2 read/write CLI account. |
| RWL1UserName | Specifies the user name for the Layer 1 read/write CLI account. |
| RWL1Password | Specifies the password for the Layer 1 read/write CLI account. |
| ROUserName | Specifies the user name for the read-only CLI account. |
| ROPassword | Specifies the password for the read-only CLI account. |
| MaxTelnet Sessions | Specifies the maximum number of concurrent Telnet sessions that are allowed (from 0 to 8). |
| MaxRlogin Sessions | Specifies the maximum number of concurrent Rlogin sessions that are allowed (from 0 to 8). |
| Timeout | Specifies the number of seconds of inactivity for a Telnet or Rlogin session before automatic timeout and disconnect (30 to 65535 seconds). |

The CLI Access tab also lets you specify the number of allowed Telnet sessions and remote login (Rlogin) sessions. To prohibit Telnet or rlogin access to the devices, specify zero (0) as the number of allowed sessions. Ports are in the forwarding and blocking states.

# Configuring a security group for Web access

You can use Security Manager to manage access to the Web interfaces for all devices in the security group.

Perform the following procedure to configure Web access for a security group.

### Procedure steps

1. Under the **WEB** folder in the navigation pane, click the folder for the security group for which you want to configure Web access.
2. In the contents pane, click the **Web Access** tab.

   The fields appear on the Contents pane.


3. On the Web Access tab, edit the Web access user names and passwords.

**Important:**
In Web Access only the ROPassword can be changed.

4. On the Security Manager toolbar, click **Apply Changes**.

   Security Manager applies your changes only to the changed devices in the security group.

## Job aid

The following table describes the parts of the Web Access tab.

| Part | Description |
|---|---|
| Address | Specifies the IP address of the security group. |
| RWAUserName | Specifies the user name of the RWAUserName Web access account for the security group. |
| RWAPassword | Specifies the password of the RWAPassword Web access account for the security group. |
| RWUserName | Specifies the user name of the RWUserName Web access account for the security group. |
| RWPassword | Specifies the password of the RWPassword Web access account for the security group. |
| ROUserName | Specifies the user name of the ROUserName Web access account for the security group. |
| ROPassword | Specifies the password of the ROPassword Web access account for the security group. |
| DefaultDisplay Rows | Displays the number of default display rows on the Web management interface. |
| HttpPort | Displays the HTTP port for Web management access. |
| Enable Server | Allows you to enable or disable the Web access server. |

## Configuring a security group for SNMP v1/v2c access

You can use Security Manager to configure the SNMP community strings for all of the devices in a security group.

Perform the following procedure to configure SNMP community strings for a security group.

### Procedure steps

1. Under the **SNMP** folder in the navigation pane, click the folder to configure SNMP access for the security group.
2. Click the **SNMP Access** tab.
3. On the **SNMP Access** tab, edit the SNMP community strings.
4. On the Security Manager toolbar, click **Apply Changes**.

   Security Manager applies your changes only to the changed devices in the security group.

## Job aid

The following table describes the parts of the SNMP Access tab.

| Part | Description |
|---|---|
| ReadWriteAll | Specifies the SNMP ReadWriteAll community string for the security group. |
| ReadWrite | Specifies the SNMP ReadWrite community string for the security group. |
| ReadOnly | Specifies the SNMP ReadOnly community string for the security group. |
| ReadWrite Layer3 | Specifies the SNMP ReadWriteLayer3 community string for the security group. |
| ReadWrite Layer2 | Specifies the SNMP ReadWriteLayer2 community string for the security group. |
| ReadWrite Layer1 | Specifies the SNMP ReadWriteLayer1 community string for the security group. |

# Configuring a security group for SNMP v3 access

You can use Security Manager to configure the SNMP v3 access for all of the devices in a security group.

Before you begin to use Security Manager to configure access parameters, you must configure SNMP v3 credentials on the device that you wish to manage. You must also enter the SNMP v3 credentials in the Device and Server Credentials Manager in the UCM.

After you have configured the SNMP v3 credentials on the device, and in the UCM platform, COM allows users to connect to devices in a security group using SNMP v3. To manage the level of access for each user, you must configure the following parameters in Security Manager:

- create the user in the USM table; see Configuring USM access on page 151 and Adding a USM user on page 152
- add the user to the VACM group; see Configuring VACM group members on page 154
- assign access levels to the USM group; see Configuring VACM group access on page 153
- create a VACM MIB view; see Configuring the VACM MIB view on page 155

These parameters allow you to assign a user to a MIB view; when the user connects to a device through SNMP v3, the MIB view specifies the read/write access for the user.

In addition to these required parameters, you can also configure the following optional parameters:

- Community Table
- Target Table
- Target Params Table
- Notify Table
- Notify Filter Table
- Notify Filter Profile Table

For further information about configuring SNMP for your device, refer to technical documentation for the device.

## Configuring USM access

You can use Security Manager to configure User-based Security Model (USM) access for devices in a security group. Perform the following procedure to view USM access for a device.

### Procedure steps

1. Under the SNMPv3 folder in the navigation pane, click the folder for the security group for which you want to configure USM access.
2. In the security group folder, click the desired device.
3. In the contents pane, click the USM Access tab.
4. Enter the parameters for USM access, as described in the table below.

**Table 26: Job aid**

| Part | Description |
|---|---|
| Engine ID | Indicates the administratively-unique identifier for the SNMP engine. |
| Name | The name of the new user. |
| SecurityName | Creates the name used as an index to the table. The range is 1 to 32 characters. |
| AuthProtocol | Identifies the Authentication protocol used. |
| PrivProtocol | Identifies the privacy protocol used. |

## Adding a USM user

Perform the following procedure to add a USM user.

### Procedure steps

1. Click the **USM Access** tab.
2. On the Toolbar, click **Create Entry** (the plus sign).

   The **New USM User** dialog box appears.
3. In the **SM - New USM Access Entry** dialog box, edit the USM user names and passwords, as described in the table below.
4. To apply the changes to multiple devices in the group, choose the devices for which you want to apply the changes from the **Devices** list.
5. Click **Ok**.

   The Security Manager creates a new USM entry in the selected devices under the device list.

**Table 27: Job aid**

| Part | Description |
|---|---|
| Engine ID | Indicates the administratively-unique identifier for the SNMP engine. |
| New User Name | Creates the new entry with this security name. The name is used as an index to the table. The range is 1 to 32 characters. |
| Clone From User | Specifies the security name from which the new entry must copy privacy and authentication parameters. The range is 1 to 32 characters. |
| Auth Protocol (Optional) | Assigns an authentication protocol (or no authentication) from a drop-down menu. If you select an authentication |

| Part | Description |
|---|---|
| | protocol, you must enter the cloned user's authentication password and specify a new authentication password for the new user. |
| Cloned User's Auth Password | Enter the cloned user's authentication password. |
| New User's Auth Password | Enter a new authentication password for the new user. |
| Priv Protocol (Optional) | Assigns a privacy protocol (or no privacy) from a drop-down menu.If you select a privacy protocol, you must enter the cloned user's privacy Pass and specify a new privacy password for the new user. |
| Cloned User's Priv Password | Enter the cloned user's privacy password. |
| New User's Priv Password | Enter a new privacy password for the new user. |
| OK | Adds the devices to the security group and closes the dialog box. |
| Close | Closes the dialog box without applying your settings. |

## Configuring VACM group access

Perform the following procedure to configure VACM Group Access for a device.

### Procedure steps

1. Click the **VACM Group Access** tab.
2. On the Toolbar, click **Create Entry** (the plus sign).

   The SM - New VACM Group Access dialog box appears.
3. In the **SM - New VACM Group Access Entry** dialog box, edit the VACM Group Access properties, as described in the table below.
4. To apply the changes to multiple devices in the group, choose the devices for which you want to apply the changes from the **Devices** list.
5. Click **Ok**.

   The Security Manager creates a new VACM Group Access entry in the selected devices under the device list.

**Table 28: Job aid**

| Part | Description |
|---|---|
| GroupName | The name of the new group name in the VACM table. The name is a numeral. The range is 1 to 32 characters. |

| Part | Description |
|---|---|
| AccessContextPrefix | The contextName of an incoming SNMP packet must match exactly or partially the value of the instance of this object. The range is an SnmpAdminString, 1 to 32 characters. |
| AccessSecurityModel | The security model of the entry, either SNMPv1, SNMPv2, or SNMPv3. |
| AccessSecurityLevel | The minimum level of security required to gain access rights. The security levels are:<br>noAuthNoPriv<br>authNoPriv<br>authpriv |
| AccessReadViewName | Specifies the MIB view to which read access is authorized. |
| AccessWriteViewName | Specifies the MIB view to which write access is authorized. |
| AccessNotifyViewName | Specifies the MIB view name to which notification access is authorized. |
| OK | Adds the devices to the security group and closes the dialog box. |
| Close | Closes the dialog box without applying your settings. |

### Viewing VACM group members

Perform the following procedures to view VACM Group Members for a device.

#### Procedure steps

1. Under the **SNMPv3** folder in the navigation pane, click the folder for the security group.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **VACM Group Members** tab.

**Table 29: Job aid**

| Part | Description |
|---|---|
| SecurityModel | The security model currently in use. |
| SecurityName | The name representing the user in usm user. The range is 1 to 32 characters. |
| GroupName | The name of the group to which this entry (combination of securityModel and securityName) belongs. |

### Configuring VACM group members

You can use Security Manager to configure VACM Group Members for devices in a security group. Perform the following procedure to add VACM Group Members to a device.

### Procedure steps

1. In the contents pane, click the **VACM Group Members** tab.
2. On the Toolbar, click **Create Entry** (the plus sign). The VACM Group Member dialog box appears.
3. In the **SM - VACM Group Member Entry** dialog box, edit the VACM Group Member properties.
4. To apply the changes to multiple devices in the group, choose the devices for which you want to apply the changes from the **Devices** list.
5. Click **Ok**.

   The Security Manager creates a new VACM entry in the selected devices under the device list.

**Table 30: Job aid**

| Part | Description |
|---|---|
| SecurityModel | The security model currently in use. |
| SecurityName | The name representing the user in usm user. The range is 1 to 32 characters. |
| GroupName | The name of the group to which this entry (combination of securityModel and securityName) belongs. |
| OK | Adds the devices to the security group and closes the dialog box. |
| Close | Closes the dialog box without applying your settings. |

## Configuring the VACM MIB view

Perform the following procedure to configure a VACM MIB view.

### Procedure steps

1. In the contents pane, click the **VACM MIB View** tab.
2. On the Toolbar, click **Create Entry** (the plus sign).

   The SM - New VACM MIB View Entry dialog box appears.
3. In the **SM - New VACM MIB View Entry** dialog box, edit the VACM MIB View properties, as described in the table below.
4. To apply the changes to multiple devices in the group, choose the devices for which you want to apply the changes from the **Devices** list.
5. Click **Ok**.

   The Security Manager creates a new VACM MIB view entry in the selected devices under the device list.

**Table 31: Job aid**

| Part | Description |
|---|---|
| ViewName | The group name. The range is 1 to 32 characters. |
| Subtree | Any valid object identifier that defines the set of MIB objects or MIB node name accessible by this SNMP entity. For example 1.3.6.1.1.5 or Org, ISO 8802. |
| Mask | Specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree. |
| Type | Determines whether access to a mib object is granted (Included) or denied (Excluded). Included is the default. |

### Accessing the VACM MIB view

You can use Security Manager to display VACM Management Information Base (MIB) views for devices in a security group. Perform the following procedure to display VACM MIB views for a device.

#### Procedure steps

1. Under the **SNMPv3** folder in the navigation pane, click the folder for the security group for which you want to display VACM MIB views.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **VACM MIB View** tab.

   The table below lists the information displayed on the VACM MIB view tab.

**Table 32: Job aid**

| Part | Description |
|---|---|
| ViewName | The group name. The range is 1 to 32 characters. |
| Subtree | Any valid object identifier that defines the set of MIB objects or MIB node name accessible by this SNMP entity. For example 1.3.6.1.1.5 or Org, ISO 8802. |
| Mask | Specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree. |
| Type | Determines whether access to a mib object is granted (Included) or denied (Excluded). Included is the default. |

### Viewing the community table

You can use Security Manager to configure the Community Table for devices in a security group. Perform the following procedure to configure the Community Table for a device.

### Procedure steps

1. Under the **SNMPv3** folder in the navigation pane, click the folder for the security group.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **Community Table** tab.

   The table below lists the information displayed on the Community Table tab.

**Table 33: Job aid**

| Part | Description |
|---|---|
| Index | The unique index value of a row in this table. SnmpAdminString 1-32 characters. |
| Name | The community string for which a row in this table represents a configuration. |
| SecurityName | The security name assigned to this entry in the Community table. The range is 1 to 32 characters. |
| ContextEngineID | The contextEngineID indicating the location of the context in which management information is accessed. |
| TransportTag | The transport endpoints that are associated with the community string. The community string is only valid when found in an SNMPv1 (or SNMPv2c) message received from one of these transport endpoints, or when used in an SNMPv1 (or SNMPv2c) message to be sent to one of these transport endpoints. The value of this object identifies a set of entries in the snmpTargetAddrTable. If the value of this object has zero-length, transport endpoints are not checked when attempting to choose an entry in the snmpCommunityTable (that is, the community string is valid for use with any transport endpoint). |

## Configuring the community table

Perform the following procedure to configure the Community Table.

### Procedure steps

1. In the contents pane, click the **Community Table** tab.
2. On the Toolbar, click **Create Entry** (the plus sign).

   The SM - New Community Table Entry dialog box appears.
3. In the **SM - New Community Table Entry** dialog box, edit the Community Table properties, as described in the table below.
4. To apply the changes to multiple devices in the group, choose the devices for which you want to apply the changes from the **Devices** list.
5. Click **Ok**.

The Security Manager creates a new Community Table entry in the selected devices under the device list.

**Table 34: Job aid**

| Part | Description |
|---|---|
| Index | The unique index value of a row in this table. SnmpAdminString 1-32 characters. |
| Name | The community string for which a row in this table represents a configuration. |
| SecurityName | The security name assigned to this entry in the Community table. The range is 1 to 32 characters. |
| ContextEngineID | The contextEngineID indicating the location of the context in which management information is accessed. |
| TransportTag | The transport endpoints that are associated with the community string. The community string is only valid when found in an SNMPv1 (or SNMPv2c) message received from one of these transport endpoints, or when used in an SNMPv1 (or SNMPv2c) message to be sent to one of these transport endpoints. The value of this object identifies a set of entries in the snmpTargetAddrTable. If the value of this object has zero-length, transport endpoints are not checked when attempting to choose an entry in the snmpCommunityTable (that is, the community string is valid for use with any transport endpoint). |
| OK | Adds the devices to the security group and closes the dialog box. |
| Close | Closes the dialog box without applying your settings. |

### Viewing the target table

You can use Security Manager to display the Target Table for devices in a security group. Perform the following procedure to display the Target Table for a device.

## Procedure steps

1. Under the **SNMPv3** folder in the navigation pane, click the folder for the security group.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **Target Table** tab.

   The table below lists the information displayed on the Target Table tab.

**Table 35: Job aid**

| Part | Description |
|---|---|
| Name | The unique identifier to index this table. |

| Part | Description |
|---|---|
| TDomain | The transport type of the address in the snmpTargetAddr TAddressobject. |
| TAddress | The transport address whose format depends on the value of the snmpTargetAddrTAddressobject. |
| Timeout | The maximum round trip time required for communicating with the transport address defined by this row. |
| RetryCount | The number of retries to be attempted when a response is not received for a generated message. |
| TagList | Specifies a list of tag values. A tag value refers to a class of targets to which the messages may be sent. |
| Params | The value of SnmpAdminString identifies snmpTargetParamsTable entries. |

### Configuring the target table

Perform the following procedure to configure the Target Table for a device.

#### Procedure steps

1. In the contents pane, click the **Target Table** tab.
2. On the Toolbar, click **Create Entry** (the plus sign). The SM - Target Table Entry dialog box appears.
3. In the **SM - New Target Table Entry** dialog box, edit the Target Table properties, as described in the table below.
4. To apply the changes to multiple devices in the group, choose the devices for which you want to apply the changes from the **Devices** list.
5. Click **Ok**.

   The Security Manager creates a new Target Table entry in the selected devices under the device list.

**Table 36: Job aid**

| Part | Description |
|---|---|
| Name | The unique identifier to index this table. |
| TDomain | The transport type of the address in the snmpTargetAddr TAddressobject. |
| TAddress | The transport address whose format depends on the value of the snmpTargetAddrTAddressobject. |
| Timeout | The maximum round trip time required for communicating with the transport address defined by this row. |
| RetryCount | The number of retries to be attempted when a response is not received for a generated message. |

| Part | Description |
|---|---|
| TagList | Specifies a list of tag values. A tag value refers to a class of targets to which the messages may be sent. |
| Params | The value of SnmpAdminString identifies snmpTargetParamsTable entries. |
| OK | Adds the devices to the security group and closes the dialog box. |
| Close | Closes the dialog box without applying your settings. |

### Viewing the target parameters table

You can use Security Manager to display the Target Params Table for devices in a security group. Perform the following procedure to display the Target Params Table for a device.

#### Procedure steps

1. Under the **SNMPv3** folder in the navigation pane, click the folder for the security group.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **Target Params Table** tab.

   The table below lists the information displayed on the Target Params Table tab.

**Table 37: Job aid**

| Part | Description |
|---|---|
| Name | The community string for which a row in this table represents a configuration. |
| MPModel | Specifies the Message Processing model, SNMPv1, SNMPv2c, or SNMPv3/USM. |
| SecurityModel | Specifies the security model, SNMPv1, SNMPv2c, or SNMPv3/USM. |
| SecurityName | The security name identifies the principal to generate SNMP messages using security name entry. |
| SecurityLevel | The minimum level of security required to gain access rights. The security levels are:<br>• noAuthNoPriv<br>• authNoPriv<br>• authpriv |

### Configuring the target parameters table

Perform the following procedure to configure the Target Params Table for a device.

### Procedure steps

1. In the contents pane, click the **Target Params Table** tab.
2. On the Toolbar, click **Create Entry** (the plus sign). The SM - New Target Params Table Entry dialog box appears.
3. In the **SM - New Target Params Table Entry** dialog box, edit the Target Params Table properties.
4. To apply the changes to multiple devices in the group, choose the devices for which you want to apply the changes from the **Devices** list.
5. Click **Ok**.

   The Security Manager creates a new Target Params entry in the selected devices under the device list.

**Table 38: Job aid**

| Part | Description |
|---|---|
| Name | The community string for which a row in this table represents a configuration. |
| MPModel | Specifies the Message Processing model, SNMPv1, SNMPv2c, or SNMPv3/USM. |
| SecurityModel | Specifies the security model, SNMPv1, SNMPv2c, or SNMPv3/USM. |
| SecurityName | The security name identifies the principal to generate SNMP messages using security name entry. |
| SecurityLevel | The minimum level of security required to gain access rights. The security levels are:<br>• noAuthNoPriv<br>• authNoPriv<br>• authpriv |
| Clear All | Deselects all devices on the device list. |
| Select All | Selects all devices on the device list. |
| OK | Adds the devices to the security group and closes the dialog box. |
| Close | Closes the dialog box without applying your settings. |

## Viewing the notify table

You can use Security Manager to display the Notify Table for devices in a security group. Perform the following procedure to display the Notify Table for a device.

### Procedure steps

1. Under the **SNMPv3** folder in the navigation pane, click the folder for the security group.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **Notify Table** tab.

   The table below lists the information displayed on the Notify Table tab.

**Table 39: Job aid**

| Part | Description |
|---|---|
| Name | The community string for which a row in this table represents a configuration. |
| Tag | The tag value used to select the entries in snmpTargetAddrTable. |
| Type | The type assigned to the community string name. Choices are:<br>• trap<br>• inform |

## Configuring the notify table

Perform the following procedure to configure the Notify Table for a device.

### Procedure steps

1. In the contents pane, click the **Notify Table** tab.
2. On the Toolbar, click **Create Entry** (the plus sign). The SM - New Notify Table Entry dialog box appears.
3. In the **SM - New Notify Table Entry** dialog box, edit the Notify Table properties, as described in the table below.
4. To apply the changes to multiple devices in the group, choose the devices for which you want to apply the changes from the **Devices** list.
5. Click **Ok**.

   The Security Manager creates a new Notify Table entry in the selected devices under the device list.

**Table 40: Job aid**

| Part | Description |
|---|---|
| Name | The community string for which a row in this table represents a configuration. |
| Tag | The tag value used to select the entries in snmpTargetAddrTable. |

| Part | Description |
|---|---|
| Type | The type assigned to the community string name. Choices are:<br>• trap<br>• inform |
| Clear All | Deselects all devices on the device list. |
| Select All | Selects all devices on the device list. |
| OK | Adds the devices to the security group and closes the dialog box. |
| Close | Closes the dialog box without applying your settings. |

### Viewing the notify filter table

You can use Security Manager to display the Notify Filter Table for devices in a security group. Perform the following procedure to display the Notify Filter Table for a device.

#### Procedure steps

1. Under the **SNMPv3** folder in the navigation pane, click the folder for the security group.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **Notify Filter Table** tab.

**Table 41: Job aid**

| Part | Description |
|---|---|
| ProfileName | The name of the filter profile used while generating notifications in snmpTargetAddrTable. |
| Subtree | MIB subtree with the corresponding instance of snmpNotifyFilterMask defines a family of subtrees. |
| Mask | Bit mask in combination with snmpNotifyFilterMask defines a family of subtrees. |
| Type | Indicates whether the family of filter subtrees defined by this entry are included or excluded from a filter. The valid options are included and excluded. |

### Configuring the notify filter table

Perform the following procedure to configure the Notify Filter Table for a device.

#### Procedure steps

1. In the contents pane, click the **Notify Filter Table** tab.
2. On the Toolbar, click **Create Entry** (the plus sign).

The SM - New Notify Filter Table Entry dialog box appears.

3. In the **SM - New Notify Filter Table Entry** dialog box, edit the Notify Filter Table properties.
4. To apply the changes to multiple devices in the group, choose the devices for which you want to apply the changes from the **Devices** list.
5. Click **Ok**.

   The Security Manager creates a new Notify Filter entry in the selected devices under the device list.

**Table 42: Job aid**

| Part | Description |
|---|---|
| ProfileName | The name of the filter profile used while generating notifications in snmpTargetAddrTable. |
| Subtree | MIB subtree with the corresponding instance of snmpNotifyFilterMask defines a family of subtrees. |
| Mask | Bit mask in combination with snmpNotifyFilterMask defines a family of subtrees. |
| Type | Indicates whether the family of filter subtrees defined by this entry are included or excluded from a filter. The valid options are included and excluded. |
| Clear All | Deselects all devices on the device list. |
| Select All | Selects all devices on the device list. |
| OK | Adds the devices to the security group and closes the dialog box. |
| Close | Closes the dialog box without applying your settings. |

### Viewing the notify filter profile table

You can use Security Manager to display the Notify Filter Profile Table for devices in a security group. Perform the following procedure to display the Notify Filter Profile Table for a device.

#### Procedure steps

1. Under the **SNMPv3** folder in the navigation pane, click the folder for the security group.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **Notify Filter Profile Table** tab.

**Table 43: Job aid**

| Part | Description |
|---|---|
| TargetParams Name | The unique identifier associated with this entry. This value is an SnmpAdminString of 1-32 characters. |

| Part | Description |
|---|---|
| NotifyFilterProfile Name | The name of the filter profile used while generating notifications in snmpTargetAddrTable. |

### Configuring the notify filter profile table

Use the following procedure to configure the Notify Filter Profile Table for a device.

#### Procedure steps

1. In the contents pane, click the **Notify Filter Profile Table** tab.
2. On the Toolbar, click **Create Entry** (the plus sign).

   The SM - New Notify Filter Profile Table Entry dialog box appears.
3. In the **SM - New Notify Filter Profile Table Entry** dialog box, edit the Notify Filter Profile Table properties.
4. To apply the changes to multiple devices in the group, choose the devices for which you want to apply the changes from the **Devices** list.
5. Click **Ok**.

   The Security Manager creates a new Notify Filter Profile entry in the selected devices under the device list.

**Table 44: Job aid**

| Part | Description |
|---|---|
| TargetParams Name | The unique identifier associated with this entry. This value is an SnmpAdminString of 1-32 characters. |
| NotifyFilterProfile Name | The name of the filter profile used while generating notifications in snmpTargetAddrTable. |
| OK | Adds the devices to the security group and closes the dialog box. |
| Close | Closes the dialog box without applying your settings. |

# Creating and configuring access policies

You can use Security Manager to add, delete, monitor, and synchronize access policies for all the devices in a security group.

Security Manager allows you to enable and disable access policies at a variety of levels within a security group. See the following topics for more information:


- Adding access policies on page 166
- Enabling or disabling access policies for devices in a security group on page 168
- Enabling or disabling individual access policies on page 169
- Deleting access policies on page 171


## Adding access policies

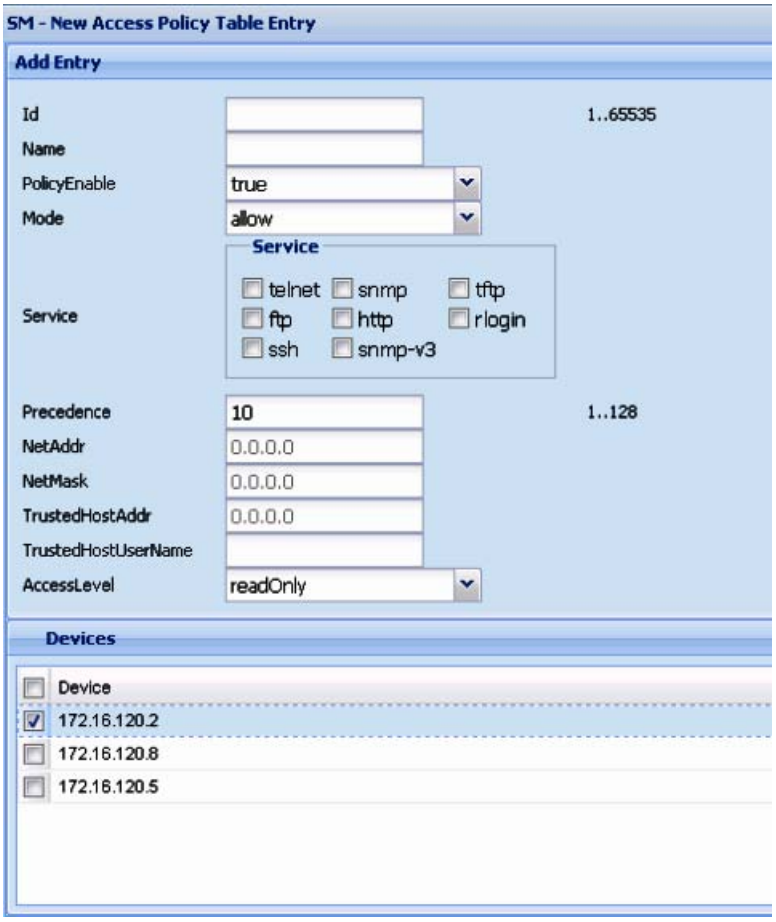
You can control access to Passport and Accelar devices in the security group with access policies. The access policy specifies the hosts or networks that can access the switch through various services.

Perform the following procedure to add an access policy.

### Procedure steps

1. Under the **Access Policy** folder in the navigation pane, click the folder for the security group for which you want to configure access policies.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **Access Policy Table** tab.
4. On the tool bar, click **Create Entry** (the plus symbol).

   The New Access Policy Table Entry dialog box appears.




5. Select appropriate access policy settings.
6. Click **OK**.

   The Security Manager creates the New Access Policy entry in the selected devices in the device list.

## Job aid

The following table describes the New Access Policy Table Entry dialog box.

| Part | Description |
|---|---|
| Id | Specifies the ID of this policy. |
| Name | Specifies the Name of this policy. |
| PolicyEnable | Activates the access policy. |
| Mode | Indicates whether a packet having a source IP address that matches this entry should be permitted to enter the device or denied access. |
| Service | Selects the protocol to which this entry should be applied. |

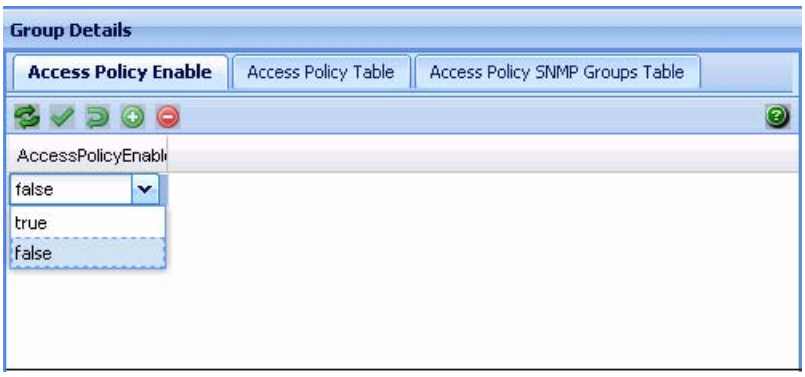
| Part | Description |
|---|---|
| Precedence | Indicates the precedence of the policy. The lower the number, the higher the precedence (1 to 128). |
| NetAddr | Specifies the source network IP address. An address of 0.0.0.0 specifies any address on the network. |
| NetMask | Specifies the source network masks. |
| TrustedHost Addr | Specifies the trusted IP address of the host performing rlogin or rsh into the device. Applies only to rlogin and rsh.<br>**Important:**<br>You cannot use wildcard entries. |
| TrustedHost UserName | Specifies the user name assigned to the trusted host. Applies only to rlogin and rsh.<br>**Important:**<br>You cannot use wildcard entries. The user must already be logged in with the user name to be assigned to the trusted host. |
| AccessLevel | Specifies the access level of the trusted host (readOnly, readWrite, or readWriteAll). |
| Clear all | Deselects all of the devices on the device list. |

# Enabling or disabling access policies for devices in a security group

Perform the following procedure to enable or disable access policies for a device in a security group.

### Procedure steps

1. Under the **Access Policy** folder in the navigation pane, open the folder for the security group for which you want to set access policies.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **Access Policy SNMP Groups Table** tab for devices supporting SNMPv3.
4. Enter the **Policy Id, Name**, and **Model** for the SNMP group.
5. In the contents pane, click the **Access Policy Enable** tab.




6. Click the drop-down box in the **Enable** column and choose **True** to enable access policies or **False** to disable access policies.
7. On the Security Manager tool bar, click **Apply Changes** to save the changes.

## Job aid

The following table describes the Access Policy SNMP Groups Table tab.

| Part | Description |
|---|---|
| AccessPolicyId | Specifies the Policy ID for the SNMP access group. |
| AccPolSnmpGrpName | Specifies the Access policy SNMP group name. |
| AccPolSnmpGrpModel | Specifies the Model of the SNMP group. |

The following table describes the Access Policy Enable tab.

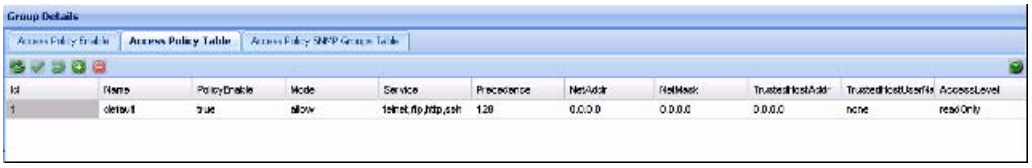
| Part | Description |
|---|---|
| AccessPolicyEnable | Enables or disables access policies for the security group. The available settings are true and false. |

## Enabling or disabling individual access policies

Perform the following procedure to enable or disable individual access policies in a security group.

### Procedure steps

1. Under the **Access Policy** folder in the navigation pane, open the folder for the security group for which you want to set access policies.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **Access Policy Table** tab.




4. Go to the row for the access policy that you want to enable or disable.
5. In the **Enable** column, click the entry for the access policy and choose **True** to enable the access policy or **False** to disable the access policy.
6. On the Security Manager tool bar, click **Apply**.

## Job aid

The following table describes the Access Policy Table.

| Part | Description |
|---|---|
| Id | Identifies the entry in the table. |
| Name | Displays the name of the policy. |
| Policy Enable | Allows you to activate or deactivate the access policy. See Enabling or disabling individual access policies on page 169 for more information. |
| Mode | Indicates whether a packet having a source IP address that matches this entry should be permitted to enter the device or denied access. |
| Service | Selects the protocol to which this entry should be applied. |
| Precedence | Indicates the precedence of the policy. The lower the number, the higher the precedence (1 to 128). |
| NetAddr | Specifies the source network IP address. An address of 0.0.0.0 specifies any address on the network. |
| NetMask | Specifies the source network masks. |
| TrustedHostAddr | Specifies the trusted IP address of the host performing rlogin or rsh into the device. Applies only to rlogin and rsh.<br>**Important:**<br>You cannot use wildcard entries. |
| TrustedHostUser Name | Specifies the user name assigned to the trusted host. Applies only to rlogin and rsh.<br>**Important:**<br>You cannot use wildcard entries. The user must already be log on with the user name to be assigned to the trusted host. |
| AccessLevel | Specifies the access level of the trusted host (readOnly, readWrite, or readWriteAll). |

# Deleting access policies

Perform the following procedure to delete an access policy from a security group.

### Procedure steps

1. Under the **Access Policy** folder in the navigation pane, click the folder for the security group from which you want to delete an access policy.
2. In the security group folder, click the desired device.
3. In the contents pane, click the **Access Policy Table** tab.
4. On the **Access Policy Table** tab, click any cell of the access policy that you want to delete.
5. On the Tool bar, click **Delete** (the - symbol).

   The system asks for a confirmation on deleting the selected entry.
6. Click **Yes** to delete the entry.

   Security Manager deletes the selected access policy.

# Chapter 7: Configuration of Routing Manager

You can configure routing parameters for devices across a network discovered by COM. Routing Manager supports the following protocols:

- IPv4 Routing
- RIP
- OSPF
- ARP
- VRRP
- IPv6 Routing
- IPv6 OSPF
- IPv6 VRRP

For information about which devices support the protocols in the preceding list, see Supported devices for Routing Manager on page 179.

### Navigation

# Starting Routing Manager

Perform the following procedure to start the Routing Manager.

### Procedure steps

In the Configuration and Orchestration Manager window Navigation pane, click **Routing Manager** button. The Routing Manager window appears.

# Job aid

The following table describes the parts of the Routing Manager tool bar.

| Toolbar button | Menu | Description |
|---|---|---|
|  | Discover Routing | It discovers Routing Manager with the latest information. The assigned devices in the Admin/ Access control tab are used in the discovery process. These devices are then filtered based on the specific manager user preferences. |
|  | Add devices | Opens the Add devices dialog box, where you can add a device for a selected tree node. It is used for the circuit less tree node and for all other nodes that have less devices than the number of available devices. |
|  | Remove device | The user can remove a selected device from the tree. This device will appear in the add devices dialog box after this operation. |
|  | Preferences | The user can select the required configuration by clicking on this button. |

## Navigation pane

Routing Manager displays devices and adjacent devices in a tree structure. The Routing Manager navigation tree is located on the left side of the window and contains branches with the IP address of devices discovered by COM.

The following figure shows Routing Manager navigation pane.

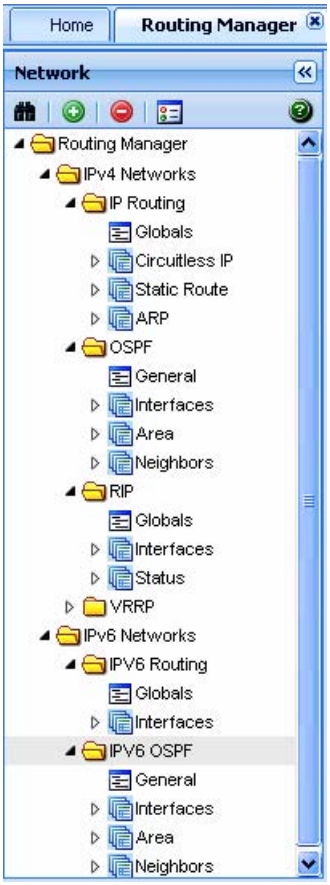



**Figure 20: Routing Manager navigation pane**

From the navigation tree in the navigation pane, select the folder for which you want to view routing information.

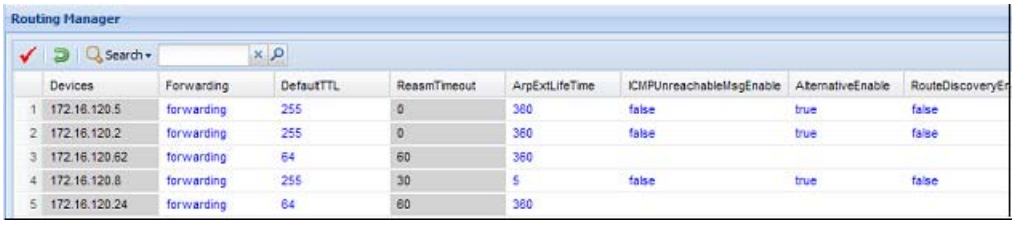
## Contents pane

When you choose a folder in the navigation pane, its contents appear in the contents pane.

Perform the following procedure to view the folder in the contents pane.

### Procedure steps

In the COM navigation pane, expand Routing Manager and select a Routing folder. The contents of the folder appear as a table in the contents pane, as shown in the following figure.




## Job aid

The following table describes the Content pane toolbar.

| Toobar button | Menu | Description |
|---|---|---|
|  | Add Entry | The user can add a row to the specific table. A dialog box appears and the user can add the desired data; each dialog box is specific to its corresponding table. It is applicable only for protocol specific tables. |
|  | Delete Entry | The user can delete a row from the table by selecting a row and pressing the Delete Entry button. This is applicable only for protocol specific tables. |
|  | Apply Changes | The user can modify the editable data in the table; after the editing is finished, the changes are applied to the device. |
|  | Revert Changes | If the user wants to return to the initial state of the table this button should be pressed. |
|  | Search | The user can search the information in the table by selecting the columns to be searched and enter the information in the form near the search button. |

## Rediscovering Routing Manager

You can refresh the information in the Routing Manager window with routing information polled from the network devices. You can use this feature to load any updated information that takes effect after you open Routing Manager.

Perform the following procedure to rediscover the routing information.

### Procedure steps

1. In the COM navigation pane, expand the Routing Manager toolbar, and click **Discover Routing**.
2. Click **OK** when the operation has completed.

# Discover Routing

When the user opens the routing manager an automatic discovery is performed for the available devices. After this step, the user can obtain again the changes in the network by pressing the discovery button. While the discovery is being performed, there is a progress manager bar that shows the discovery progress.

This progress shows the total number of devices and the number of the discovered devices; also the user can see in here the possible warnings or errors that might appear in the discovery process. For more information, about these warnings and errors refer to the log file.

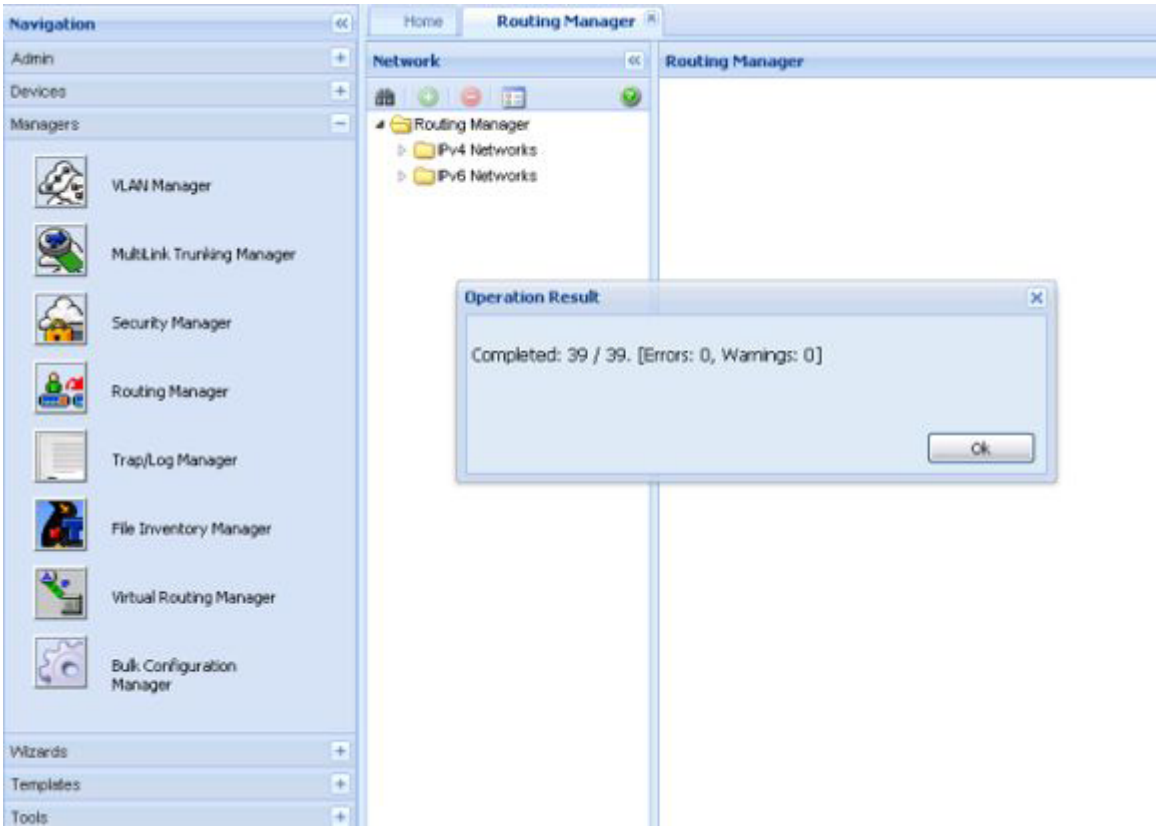



**Figure 21: Routing Manager discovery progress**

# Adding devices

The add devices dialog box appears when pressing the toolbar Add Devices button. The available devices for the selected tree node appear in the dialog box; the available devices can be:

- Devices that have support for the specific protocol (like IP Routing/Circuitless).
- Devices that were previously removed from the tree for the specific protocol.

The user can select the desired devices and they get added to the left side tree.

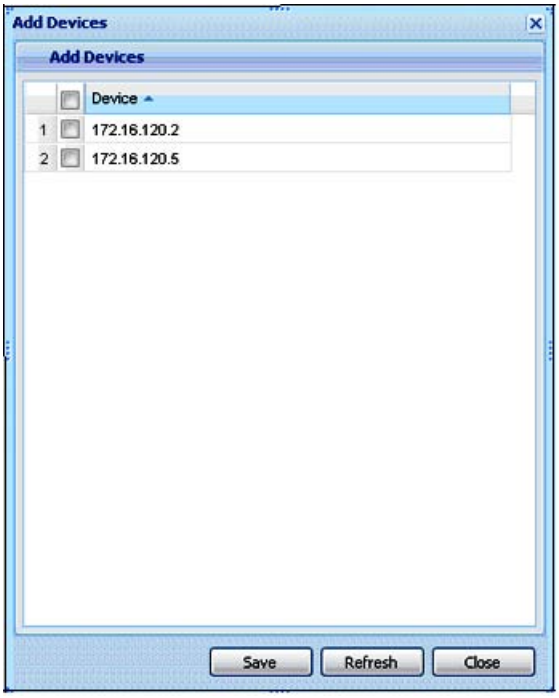



**Figure 22: Add Devices**

# Preferences

The Routing Manager preferences box appears when clicking the toolbar Preferences button. The user can select the specific set of assigned devices to be used in the Routing Manager discovery process, based on several criteria. More details about manager preferences can be found in the Preferences section.

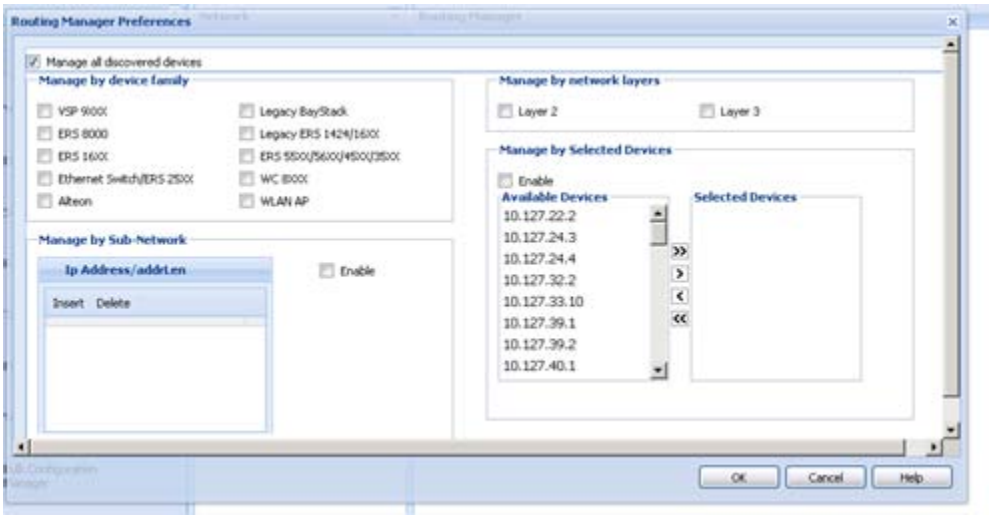



**Figure 23: Routing Manager Preferences**

# Routing Manager features

You can use Routing Manager to perform the following tasks:

- Create, delete, or modify routes across multiple devices.
- View and configure routes and properties for IP, RIP, OSPF, VRRP, IPv6, and IPv6 OSPF.

For information about which devices support specific Routing Manager features, see Supported devices for Routing Manager on page 179.

# Supported devices for Routing Manager

The following table provides a feature/device matrix for the Routing Manager for the ERS 8800, ERS 8600, and ERS 8300 devices.

| Features | | Supported devices | | |
|---|---|---|---|---|
| | | ERS 8800 | ERS 8600 | ERS 8300 |
| **IPv4 Routing** | Circuitless IP | v3.3 and up | v3.3 and up | v2.2 and up |
| | Static Route | All versions | All versions | All versions |
| | ARP | All versions | All versions | All versions |
| **OSPF** | Interfaces | All versions | All versions | v3.0 and up |

| Features | | Supported devices | | |
|---|---|---|---|---|
| | | ERS 8800 | ERS 8600 | ERS 8300 |
| | Area | All versions | All versions | v3.0 and up |
| | Neighbors | All versions | All versions | v3.0 and up |
| **RIP** | Interfaces | All versions | All versions | All versions |
| | Status | All versions | All versions | All versions |
| **VRRP** | Interfaces | v7 and up | All versions | v3.0 and up |
| **IPv6 Routing** | Interfaces | v7 and up | v4.1 and up | not supported |
| **IPv6 OSPF** | Interfaces | v7 and up | v4.1 and up | not supported |
| | Area | v7 and up | v4.1 and up | not supported |
| | Neighbors | v7 and up | v4.1 and up | not supported |
| **IPv6 VRRP** | Interface | 3.3 and up | 3.3 and up | not supported |

The following table provides a feature/device matrix for the Routing Manager for the ERS 55xx, ERS 45xx, and ERS 16xx devices.

| Features | | Supported devices | | |
|---|---|---|---|---|
| | | ERS 55xx | ERS 45xx | ERS 16xx |
| **IPv4 Routing** | Circuitless IP | not supported | not supported | v2.0 and up |
| | Static Route | v4.0 and up | v5.5 and up | v2.1 and up |
| | ARP | v3.0 and up | v5.5 and up | v2.1 and up |
| **OSPF** | Interfaces | v5.0 and up | v5.5 and up | v2.1 and up |
| | Area | v5.0 and up | v5.5 and up | v2.1 and up |
| | Neighbors | v5.0 and up | v5.5 and up | v2.1 and up |
| **RIP** | Interfaces | v5.0 and up | v5.5 and up | v2.1 and up |
| | Status | v5.0 and up | v5.5 and up | v2.1 and up |
| **VRRP** | Interfaces | v5.0 and up | v5.5 and up | v2.1 and up |
| **IPv6 Routing** | Interfaces | not supported | not supported | not supported |
| **IPv6 OSPF** | Interfaces | not supported | not supported | not supported |
| | Area | not supported | not supported | not supported |
| | Neighbors | not supported | not supported | not supported |
| **IPv6 VRRP** | Interface | not supported | not supported | not supported |

The following table provides a feature/device matrix for the Routing Manager for VSP and WC devices.

| Features | | Supported devices | |
|---|---|---|---|
| | | VSP 9xxx | WC 8xxx |
| **IPv4 Routing** | Circuitless IP | v3.0.0 | not supported |
| | Static Route | v3.0.0 | v1.0.0 |
| | ARP | v3.0.0 | v1.0.0 |
| **OSPF** | Interfaces | v3.0.0 | not supported |
| | Area | v3.0.0 | not supported |
| | Neighbors | v3.0.0 | not supported |
| **RIP** | Interfaces | v3.0.0 | not supported |
| | Status | v3.0.0 | not supported |
| **VRRP** | Interfaces | v3.0.0 | not supported |
| **IPv6 Routing** | Interfaces | v3.0.0 | not supported |
| **IPv6 OSPF** | Interfaces | not supported | not supported |
| | Area | not supported | not supported |
| | Neighbors | not supported | not supported |
| **IPv6 VRRP** | Interface | not supported | not supported |

# Viewing and configuring IPv4 routing

In the Routing Manager navigation pane, the navigation tree shows the IP addresses of discovered devices. Icons associated with IPv4 addresses on the branches indicate the following types of routes:

- IP routes (circuitless IP, static and ARP)
- OSPF routes
- RIP routes
- VRRP routes

This section contains information about configuring routes for IPv4 routes and protocols.

# Configuring IPv4 routing

This section contains information about the following topics:



# Configuring IPv4 routing Globals

Perform the following procedure to configure the IPv4 routing global properties.

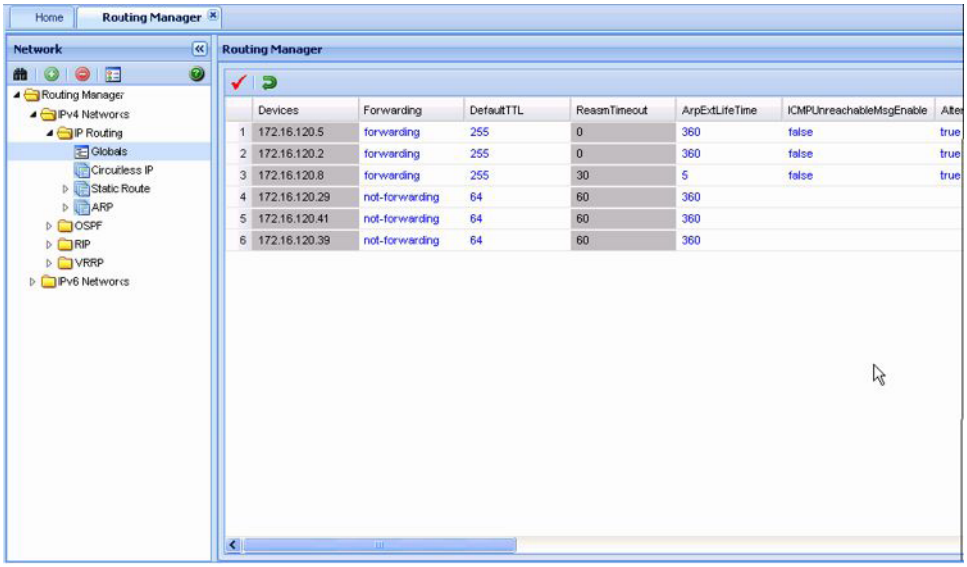
### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select the node under **IPv4 Networks, IP ROUTING, Globals**.

   The Globals table appears in the contents pane.

2. To modify any of the configurable global routing properties, modify the fields directly in the contents pane and click **Apply Changes**.

   The following table describes the fields in the IPv4 routing – Globals table.



## Job aid

The following table describes the fields in IP Routing Globals table.v4

| Field | Description |
|---|---|
| Devices | Identifies the device. |
| Forwarding | Sets the switch for forwarding (routing) or not-forwarding. |
| DefaultTTL | Sets the default time-to-live (TTL) value for a routed packet. TTL indicates the maximum number of seconds elapsed before a packet is discarded. Enter an integer between 1 and 255. The default value of 255 is inserted in the TTL field whenever one is not supplied in the datagram header. |
| ReasmTimeout | The maximum number of seconds that received fragments are held while they wait for reassembly at this entity. The default value is 30 seconds. |
| ArpExtLifeTime | The lifetime in minutes of an ARP entry within the system. |
| ICMPUnreachableMsg | Enable If selected, enables the generation of Internet Control Message Protocol (ICMP) net unreachable messages if the destination network is not reachable from this router. These messages assist in determining if the routing switch is reachable over the network. The default is disabled (not selected). |
| ICMPRedirectMsgEnable | Enables or disables the switch from sending ICMP destination redirect messages. |
| AlternativeEnable | Enables or disables the alternative-route feature globally. If the alternative-route parameter is disabled, all existing alternative routes are removed. When the parameter is enabled, all alternative routes are re-added. |
| RouteDiscoveryEnable | If selected, enables the ICMP Route Discovery feature. |
| AlowMoreSpecificNonLocal RouteEnable | Enables or disables a more specific nonlocal route. |
| UdpCheckSumEnable | Enables or disables UDP checksum calculation. |

| Field | Description |
|---|---|
| EcmpEnable | Globally enables or disables the Equal Cost Multipath (ECMP) feature. Note: When ECMP is disabled, the EcmpMaxPath is reset to the default value of 1. |
| EcmpMaxPath | Used to globally configure the maximum number of ECMP paths.<br>• When the switch is in R mode, the interval is 1 to 8.<br>• When the switch is not in R mode, the interval is 1 to 4.<br>• The default value is 1.<br>You cannot configure this feature unless ECMP is enabled globally on the switch. |
| Ecmp<1-4>PathList | Used to select a preconfigured ECMP path. |
| EcmpPathListApply | Set this field to true to apply any changes in the ECMP path list configuration or in the prefix lists configured to be used as path lists. |

# Configuring circuitless IP

You can configure circuitless IP (Clip) interfaces on the following devices: ERS 1600 v2.0 and up, ERS 8300 v2.2 and up, ERS 8600 v3.3 and up, ERS 8800 v3.3 and up, and VSP 9xxx v3.0.0.

Perform the following procedure to configure circuitless IP and to add or delete circuitless IP interfaces.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select the node under **IPv4 Networks, IP ROUTING, Circuitless IP**.
2. Select the device for which you want to configure CLIP.
3. From the Routing Manager toolbar, select **Add**.

   The Circuitless IP Insert dialog box appears.
4. Enter the required information.

   Field descriptions follow this procedure.
5. Click **Save**.

The new CLIP interface appears in the contents pane.

6. To delete a CLIP interface, in the contents pane click in the row for that interface and select **Delete entry** from the Routing Manager Edit menu.

   You cannot modify CLIP interface fields in the contents pane.

### Job aid

The following table describes the fields in the IPv4 Routing - Insert Circuitless IP field.

| Field | Description |
|---|---|
| IfIndex | The interface index. |
| Addr | The IP address of the Clip interface. |
| NetMask | The network mask of the Clip interface. |

## Configuring IPv4 routing Static Route

Perform the following procedure to configure static routes.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select the node under **IPv4 Networks, IP ROUTING, Static Route**.

   The Static Route table appears in the contents pane.

2. To add a route, from the tool bar, click **Add entry** . The Add entry dialog box appears.
3. Complete the fields as required, and select the devices for which the static route applies.
4. Click **OK**.

   The new entry appears in the contents pane.

5. To modify any of the configurable static route properties of an entry, modify the fields directly in the contents pane and click **Apply Changes**.

## Configuring IPv4 routing ARP

Perform the following procedure to configure ARP routes.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select the node under **IPv4 Networks, IP ROUTING, ARP**.

   The ARP table appears in the contents pane.
2. To add a route, from the tool bar, click **Add entry**.

   The Insert ARP dialog box appears.
3. Complete the fields as required, and select the devices for which the ARP route applies.
4. Click **OK**.

   The new entry appears in the contents pane.

## Job aid

The following table describes the fields in the IPv4 routing ARP.

| Field | Description |
|---|---|
| Interface | The router interface for this ARP entry:<br>• Brouter interfaces are identified by the slot or port number of the brouter port.<br>• For virtual router interfaces, the brouter slot/port and the name of the VLAN followed by the (VLAN) designation are specified. |
| MacAddress | The Ethernet MAC address. |
| IpAddress | The IP address corresponding to the MAC address. |
| Type | The type of ARP entry:<br>• local—a locally configured ARP entry<br>• static—a statically configured ARP entry<br>• dynamic—a learned ARP entry |

# Configuring OSPF

This section contain information about the following topics:

- Configuring OSPF Area on page 193
- Configuring OSPF Neighbors on page 194

For a list of devices that support OSPF, see Supported devices for Routing Manager on page 179.

## Configuring OSPF General

Perform the following procedure to configure general OSPF properties.

### Procedure steps

1. In the COM navigation pane, expand managers, click on Routing Manager and select a node under **IPv4 Networks, OSPF, General**.

   The OSPF – General table appears in the contents pane.
2. To modify any of the configurable OSPF properties, modify the fields directly in the contents pane and click **Apply Changes**.

## Job aid

The following table describes the fields in the OSPF – General table.

| Field | Description |
|---|---|
| Devices | Identifies the device. |
| RouterId | The Router ID, which in OSPF has the same format as an IP address but identifies the router independent of other routers in the OSPF domain. |
| AdminStat | The administrative status of OSPF in the router. The value enabled denotes that the OSPF process is active on at least one interface; disabled disables the OSPF process on all interfaces. The default is disabled. |
| VersionNumber | Current version number of OSPF. |
| AreaBdrRtrStatus | A flag to note if this router is an area border router (ABR).<br>**Important:**<br>The AreaBdrRtrStatus value must be true to create a virtual router interface. |
| ASBdrRtrStatus | When the ASBdrRtrStatus option is selected, the router is configured as an autonomous system boundary router (ASBR). |
| ExternLsaCount | The number of external (LS type 5) link state advertisements in the link state database. |

| Field | Description |
|---|---|
| ExternLsa CksumSum | The 32-bit unsigned sum of the link state checksums of the external link state advertisements contained in the link state database. This sum is used to determine if a changed occurred in a router link state database and to compare the link state databases of two routers. |
| OriginateNewLsas | The number of new link state advertisements that have been originated. This number is incremented each time the router originates a new link state area (LSA). |
| RxNewLsas | The number of link state advertisements received that are determined to be new instances. This number does not include newer instances of self-originated link state advertisements. |
| DefaultMetric 10MegPort | Indicates the default cost to be applied to the 10 Mb/s interface (port). |
| DefaultMetric 100MegPort | Indicates the default cost to be applied to the 100 Mb/s interface (port). |
| DefaultMetric 1000MegPort | Indicates the default cost to be applied to the 1000 Mb/s interface (port). |
| DefaultMetric10000MegPort | Indicates the default cost to be applied to the 10000 Mb/s interface (port). |
| TrapEnable | Indicates whether to enable traps relating to the OSPF. |
| AutoVirtLink Enable | Enables or disables automatic creation of virtual links. |
| SpfHoldDown Time | Allows you to change the OSPF hold-down timer value (3 to 60 seconds). |
| Action | Allows you to initiate a new SPF run to update the routing table. |
| Rfc1583 Compatibility | Allows you to control the preference rules used when choosing among multiple AS-External LSAs advertising the same destination. When you enable this setting, the preference rule is the same as specified by RFC 1583. When you disable the setting, the new preference rule as described in RFC 2328 is applicable, which potentially prevents the routing loops when AS-External LSAs for the same destination originate from different areas. |
| LastSpfRun | Used to indicate the time (SysUpTime) since the last SPF calculated by OSPF. |

## Configuring OSPF Interfaces

Perform the following procedure configure OSPF interfaces.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select a node under **IPv4 Networks, OSPF, Interfaces**.

   The OSPF – Interfaces table appears in the contents pane.

   **Important:**
   By default, OSPF Interfaces tab parameter appears.
2. To add an interface, from the menu bar, click **Add Entry**.

   The Add entry dialog box appears.
3. Complete the fields as required.
4. Click **Save**.

   The new entry appears in the contents pane.
5. To modify any of the configurable OSPF interface properties for an entry, modify the fields directly in the contents pane and click **Apply** .

## Job aid

The following table describes the fields in the OSPF – Interfaces table.

| Field | Description |
|---|---|
| IpAddress | IP address of the current OSPF interface. |
| AddressLessIf | Designates whether an interface has an IP address. Interfaces with an IP address = 0 Interfaces without IP address = ifIndex |
| AreaId | Dotted decimal value to designate the OSPF area name. VLANs that maintain the default area setting on the interface cause the link-state database (LSDB) to be inconsistent.<br>**Important:**<br>The area name is not related to an IP address. You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200). |
| AdminStat | Current administrative state of the OSPF interface (enabled or disabled). |
| State | Current designated router (DR) state of the OSPF interface (DR, BDR, OtherDR) |
| RtrPriority | OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become the designated router |

| Field | Description |
|---|---|
| | or the backup. The priority is used only during election of the designated router and backup designated router. The range is 0 to 255. The default is 1. |
| Designated Router | IP address of the router elected by the Hello Protocol to send link state advertisements on behalf of the NBMA network. |
| Backup Designated Router | IP address of the router elected by the Hello Protocol to send link state advertisements on behalf of the NBMA network if the designated router fails. |
| IfType | Type of OSPF interface (broadcast, nbma, or passive) |
| AuthType | Type of authentication required for the interface.<br>• none—No authentication required.<br>• simple password—All OSPF updates received by the interface must contain the authentication key specified in the interface AuthKey field.<br>• MD5 authentication—All OSPF updates received by the interface must contain the md5 key. |
| AuthKey | Key (up to 8 characters) required when simple password authentication is specified in the interface AuthType field. |
| Primary Md5Key | The primary MD5 key used for encrypting outgoing packets. |
| Hello Interval | Length of time, in seconds, between Hello packets. This value must be the same for all routers attached to a common network. The default is 10 seconds.<br>**Important:**<br>When you change the Hello interval values, you must save the configuration file and reboot the switch for the values to be restored and checked for consistency. |
| TransitDelay | Length of time, in seconds between 1 and 3600, required to transmit an LSA update packet over the interface. |
| RetransInterval | Length of time, in seconds between 1 and 3600, required between LSA retransmissions. |
| Dead Interval | Interval used by adjacent routers to determine if the router was removed from the network. This interval must be identical on all routers on the subnet and a minimum of four times the Hello interval. To avoid interpretability issues, the RtrDeadInterval value for the OSPF interface must match the RtrDeadInterval value for the OSPF virtual interface. The default is 40 seconds. |
| AdvertiseWhen Down | If true, the network on this interface is advertised as up, even if the port is down. |

| Field | Description |
|---|---|
| MtuIgnore | Specifies whether the interface MTU flag ignores the MTU setting. |
| Events | Number of state changes or error events that occurred through all interfaces. |
| PollInterval | Length of time, in seconds, between Hello packets sent to an inactive OSPF router. |

## Configuring OSPF advanced interfaces

Perform the following procedure to configure OSPF interfaces on Avaya ERS 8300 devices.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select a node under **IPv4 Networks, OSPF, Interfaces**.
2. Click the **OspfAdvancedInterfaces** tab and select the device you wish to configure.
3. To modify any of the configurable OSPF interface properties for an entry, modify the fields directly in the contents pane and click **Apply Changes**.

   The table below lists the properties that you can configure.

**Table 45: Job aid**

| Field | Description |
|---|---|
| IfIndex | Read-only. It is a unique value to identify a physical interface or a logical interface (VLAN). |
| IP Address | IP address of the current OSPF interface. |
| Enable | Enables or disables the OSPF routing on the specified interface. |
| IfType | Read-only. OSPF interface type. It can be broadcast or passive. |
| AuthType | Type of authentication required for the interface:<br>• none—no authentication required.<br>• simple password—all OSPF updates received by the interface must contain the authentication key specified in the interface AuthKey field.<br>• MD5 authentication—all OSPF updates received by the interface must contain the md5 key. |

| Field | Description |
|---|---|
| AuthKey | Specify key if the simple password is selected in the interface AuthType field. The key can be up to 8 characters. |
| IfAreaID | Dotted-decimal value to designate the OSPF area name.<br>**Important:**<br>The link state database (LSDB) is inconsistent if the settings is default area for VLAN. |
| Advertise WhenDown | Indicates when the interface advertises.<br>**Important:**<br>Indicates even when it is non-operational. |
| HelloInterval | It is the length of time between the hello packets. The time is mentioned in seconds. This value must be the same for all routers attached to a common network. The default is 10 seconds. |
| RtrDead Interval | Interval used by adjacent routers to check if the router is removed from the network. On the subnet the interval must be identical on all routers. It also needs to be minimum of four times the hello interval. To avoid interpretability issues, the RtrDeadInterval value for the OSPF interface needs to match with the RtrDeadInterval value for the OSPF virtual interface. The default is 40 seconds. |
| RtrPriority | It is used only during the election and backup of the designated router.<br>The OSPF priority for the interface during the election process for the designated route:<br>• designated router—interface with the highest priority number<br>• backup designated router—interface with the second highest priority<br>**Important:**<br>The priority range is from 0 to 255 and the default is 1. The interface is not designated if the priority is 0. |
| Metric | It is the metric value applied to the indicated type of service. By default, this equals the least metric at the type of service among the interfaces to other areas. |

## Configuring OSPF CLIP interfaces

Before you can enable OSPF on a circuitless IP (CLIP) interface, you must configure the CLIP interface on the device.

Perform the following procedure to configure OSPF on a CLIP interface.

### Procedure steps

1. In the navigation pane, select the required device under **IPv4 Networks > OSPF > Interfaces**.
2. In the contents pane, select the **OspfClipInterfaces** tab.
3. To modify any of the configurable OSPF interface properties for an entry, modify the fields directly in the contents pane and click **Apply Changes**.

   The table below lists the properties that you can configure.

**Table 46: Job aid**

| Field | Description |
|---|---|
| Interface | Read-only. The slot/port number or VLAN identification of the interface. |
| Ip Address | Read-only. The IP address of the Clip interface. |
| Enable | Enables or disables OSPF routing on the specified interface. |
| IfAreaId | Dotted-decimal value to designate the OSPF area name. |

## Configuring OSPF Area

Perform the following procedure configure OSPF areas.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select a node under **IPv4 Networks, OSPF, Area**.

   The OSPF – Area table appears in the contents pane.
2. To add an area, from the menu bar, click **Add Entry**.

   The Add entry dialog box appears.
3. Complete the fields as required and select the devices for which the area applies.
4. Click **OK**.

   The new entry appears in the contents pane.

## Job aid

The following table describes the fields in the OSPF – Area table.

| Field | Description |
|---|---|
| AreaId | A 32-bit integer uniquely identifying an area. Area ID 0.0.0.0 is used for the OSPF backbone. VLANs that maintain the default area setting on the interface cause the LSDB to be inconsistent. |
| ImportAsExtern | The area support for importing AS-external link-state advertisements (LSA). Options include importExternal (default), importNotExternal, or importNssa (not so stubby area). |
| SpfRuns | Used to indicate the number of SPF calculations performed by OSPF. |
| AreaBdrRtrCount | The total number of area border routers reachable within this area. The value, initially zero, is calculated in each SPF Pass. |
| AsBdrRtrCount | The total number of autonomous system border routers reachable within this area. The value, initially zero, is calculated in each SPF pass. |
| AreaLsaCount | The total number of link state advertisements in the link state database for this area, excluding AS-external LSAs. |
| AreaLsa CksumSum | The 32-bit unsigned sum of the link state advertisements. This sum excludes external (LS type 5) link state advertisements. The sum is used to determine if a change occurred in a router link state database and to compare the link state database of two routers. |
| AreaSummary | The support for Summary advertisements in a stub area. |
| ActiveIfcount | The number of active interfaces in the area. |

## Configuring OSPF Neighbors

Perform the following procedure configure OSPF neighbors.

### Procedure steps

1. In the COM navigation pane, expand managers, click Routing Manager and select a node under **IPv4 Networks, OSPF, Neigbors**.

   The OSPF – Neighbors table appears in the contents pane.
2. To add a neighbor entry, from the menu bar, click **Add Entry**.

   The Add Entry dialog box appears.
3. Complete the fields as required.
4. Click **Save**.

## Job aid

The following table describes the fields in the OSPF – Neighbors table.

| Field | Description |
|---|---|
| IpAddr | The neighbor IP address. |
| AddressLess Index | On an interface having an IP address, this value is zero. On addressless interfaces, this value is the corresponding value of ifIndex in the Internet standard management information base (MIB). On row creation, this value is derived from the instance. |
| RtrId | The router ID of the neighboring router, which in OSPF has the same format as an IP address but identifies the router independent of its IP address. |
| Options | A bit mask corresponding to the options field of the neighbor. |
| Priority | Indicates the preferential treatment assignment, which places the transmitted packets into queues. The priority field also indicates the possible selection of the priority field in the data link header when the switch forwards the packet. |
| State | The OSPF interface state. |
| Events | The number of state changes or error events that occurred between the OSPF router and the neighbor router. |
| LsRetransQLen | The number of elapsed seconds between advertising retransmissions of the same packet to a neighbor. |
| ospfNbmaNbr Permanence | Indicates whether the neighbor is a manually configured NBMA neighbor. |
| HelloSuppressed | This variable indicates whether Hellos to a neighbor are suppressed. |

# Configuring RIP

This section contains information about the following topics:

- Configuring RIP Globals on page 196
- Configuring RIP interface parameters on page 196
- Configuring RIP Advanced Interface parameters on page 197
- Viewing RIP status on page 199

For a list of devices that support RIP, see Supported devices for Routing Manager on page 179.

## Configuring RIP Globals

Perform the following procedure configure global RIP properties.

### Procedure steps

1. In the COM navigation pane, expand managers, click on Routing Manager and select **IPv4 Networks, RIP, Globals**.

   The RIP–Globals table appears in the contents pane.

2. To modify any of the configurable RIP global properties, modify the fields directly in the contents pane and click **Apply Changes**.

## Job aid

The following table describes the fields in the RIP – Globals table.

| Field | Description |
|---|---|
| Devices | Identifies the device. |
| Operation | Enables or disables the operation of RIP on all interfaces. The default is disabled. |
| UpdateTime | The time interval between RIP updates on all interfaces. This is a global parameter for the switch and it applies to all interfaces. You cannot set this parameter individually for each interface. |
| RouteChanges | The number of route changes RIP made to the IP route database, excluding the refresh of a route age. |
| Queries | The number of responses sent to RIP queries from other systems. |
| HoldDownTime | Sets the length of time that RIP continues to advertise a network after determining it is unreachable. |
| TimeOutInterval | Sets the RIP timeout interval in seconds. |
| DefImportMetric | Sets the value of the default import metric to import a route into a RIP domain. For announcing OSPF internal routes into a RIP domain, if the policy does not specify a metric value, the default import metric must be used. For OSPF external routes, the external cost is used. |

## Configuring RIP interface parameters

Perform the following procedure configure RIP interface parameters.

### Procedure steps

1. In the COM navigation pane, expand managers, click on Routing Manager and select a node under **IPv4 Networks, RIP, Interfaces**.

   The Interfaces tab appears in the contents pane.

2. To modify any of the configurable RIP interface properties, modify the fields directly in the contents pane, and click **Apply**.

## Job aid

The following table describes the fields in the RIP Interfaces tab.

| Field | Description |
|---|---|
| Address | The IP address of the router interface. |
| Send | What the router sends on this interface (selected from a menu):<br>• DoNotSend—no RIP updates sent on this interface<br>• ripVersion1—RIP updates compliant with RFC 1058<br>• rip1Compatible—broadcast RIP2 updates using RFC 1058 route subsumption rules<br>• ripVersion2—multicasting RIP2 updates |
| Receive | Indicates which versions of RIP updates are accepted:<br>• rip1<br>• rip2<br>• rip1OrRip2<br>The rip2 and rip1OrRip2 imply reception of multicast packets. |

## Configuring RIP Advanced Interface parameters

Perform the following procedure configure advanced RIP interface parameters.

### Procedure steps

1. In the COM navigation pane, expand managers, click on Routing Manager and select a node under **IPv4 Networks, RIP, Interfaces**.

   The Interfaces tab appears in the contents pane.

2. Click the **RipAdvancedInterfaces** tab.

   The Interfaces Advance table appears.

3. To modify any of the configurable RIP advance interface properties, modify the fields directly in the contents pane, and click **Apply**.

## Job aid

The following table describes the fields in the Interfaces Advance tab.

| Field | Description |
|---|---|
| Address | Displays the address of the entry in the IP RIP interface table. |
| Interface | The index value of the RIP interface. |
| Enable | Displays if the RIP interface is enabled or disabled. |
| Supply | Enables (true) or disables (false) the switch to send out RIP updates on this interface. |
| Listen | What the router sends on this interface (selected from a menu). The default is rip1compatible. |
| Poison | Sets whether (true) or not (false) RIP routes on the interface learned from a neighbor are advertised back to the neighbor. If disabled, split horizon is invoked and IP routes learned from an immediate neighbor are not advertised back to the neighbor. If enabled, the RIP updates sent to a neighbor from which a route is learned are poisoned with a metric of 16. Therefore, the receiver neighbor ignores this route because the metric 16 indicates infinite hops in the network. |
| DefaultSupply | Enables (true) or disables (false) an advertisement of a default route on this interface. This command takes effect only if a default route exists in the routing table. |
| DefaultListen | Enables (true) or disables (false) the switch to accept the default route learned through RIP on this interface. |
| TriggeredUpdate | Enables (true) or disables (false) the switch to send out RIP updates on this interface. |
| AutoAggregate | Enables (true) or disables (false) automatic route aggregation on this interface. When enabled, the switch automatically aggregates routes to their natural mask when they are advertised on an interface. This configuration aggregates only the routes with a mask length longer than natural mask. |
| InPolicy | This policy determines whether to learn a route on this interface. It also specifies the parameters of the route when it is added to the routing table. |
| OutPolicy | This policy determines whether to advertise a route from the routing table on this interface. This policy also specifies the parameters of the advertisement. |
| Cost | Indicates the RIP cost for this interface. Enter a value between 1 and 15. |

## Viewing RIP status

Perform the following procedure view the RIP protocol statistics.

### Procedure steps

In the COM navigation pane, expand managers, click on Routing Manager and select a node under **IPv4 Networks, RIP, Status**.

The RIP Status table appears in the contents pane.

## Job aid

The following table describes the fields in the RIP Status table.

| Field | Description |
|---|---|
| Address | The IP address of the router interface. |
| RcvBadPackets | The number of RIP response packets received by the RIP process that were subsequently discarded for any reason (for example, a version 0 packet or an unknown command type). |
| RcvBadRoutes | The number of routes, in valid RIP packets, that were ignored for any reason (for example, unknown address family or invalid metric). |
| SentUpdates | The number of triggered RIP updates actually sent on this interface. This field explicitly does not include full updates sent containing new information. |
| HolddownTime | The hold down time. |
| TimeoutInterval | The time interval between two rip packets. |
| ProxyAnnounce Flag | |

# Configuring VRRP

This section contains information about the following topics:

- Configuring VRRP Globals on page 200
- Configuring VRRP Interfaces on page 200

For a list of devices that support VRRP, see Supported devices for Routing Manager on page 179.

## Configuring VRRP Globals

Perform the following procedure configure VRRP global properties.

### Procedure steps

1. In the COM navigation pane, expand managers, click on Routing Manager and select **IPv4 Networks, VRRP, Globals**.

   The VRRP – Globals table appears in the contents pane.
2. To modify any of the configurable VRRP global properties, modify the fields directly in the contents pane and click **Apply Changes**.

## Job aid

The following table describes the fields in the VRRP – Globals table.

| Field | Description |
|---|---|
| Devices | Identifies the device. |
| NotificationCntl | Indicates whether the VRRP-enabled router generates Simple Network Management Protocol (SNMP) traps for events defined in this management information base (MIB):<br>• Enabled—SNMP traps are sent<br>• Disabled—no traps are sent |
| VirtualAddr Enable | Used to configure whether this device must respond to pings directed to a virtual router IP address. |

## Configuring VRRP Interfaces

Perform the following procedure configure VRRP interface properties.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select a node under **IPv4 Networks, VRRP, Interfaces**.

   The VRRP – Interfaces table appears in the contents pane.
2. To modify any of the configurable VRRP interface properties, modify the fields directly in the contents pane and click **Apply Changes**.

## Job aid

The following table describes the fields in the VRRP – Interfaces table.

| Field | Description |
|---|---|
| IfIndex | Interface of the VRRP router. |
| VrId | A number that uniquely identifies a virtual router on a given VRRP router. The virtual router acts as the default router for one or more assigned addresses (1 to 255). |
| IpAddr | The assigned IP addresses that a virtual router is responsible for backing up. |
| VirtualMacAddr | The MAC address of the virtual router interface. |
| State | The state of the virtual router interface:<br>• initialize—waiting for a startup event<br>• backup—monitoring availability and state of the master router<br>• master—functioning as the forwarding router for the virtual router IP addresses |
| Control | Whether VRRP is enabled or disabled for the port (or VLAN). |
| Priority | Priority value to be used by this VRRP router. Set a value from 1 to 255, where 255 is reserved for the router that owns the IP addresses associated with the virtual router. The default is 100. |
| MasterIpAddr | The IP address of the physical interface of the master virtual router that is responsible for forwarding packets sent to the virtual IP addresses associated with the virtual router. |
| FasterAdv IntervalEnabled | Enables or disables the fast advertisement interval. When disabled, the regular advertisement interval is used. The default is disabled. |
| Advertisement Interval | The time interval (in seconds) between sending advertisement messages. Set from 1 to 255 seconds with a default of 1 second. Only the master router sends advertisements. |
| FasterAdv Interval | Sets the fast advertisement interval, which is the time interval between sending VRRP advertisement messages. The interval is between 200 and 1000 milliseconds, and you must enter the same value on all participating routers. The default is 200. You must enter the values in multiples of 200 milliseconds. |
| VirtualRouter UpTime | The time interval, in hundredths of a second, since this virtual router was initialized. |
| Action | Using the following action list to manually override the delay timer and force preemption: |

| Field | Description |
|---|---|
| | • preemption—preempt the timer<br>• none—allow the timer to keep working |
| HoldDown Timer | The time interval (in seconds) a router is delayed for the following conditions:<br>• The VRRP holddown timer is executed during the switch transitions from Init to backup and then to master. It occurs only during a switch bootup.<br>• The VRRP holddown timer is not executed during a non-bootup condition. If the master VR goes down, the backup switch becomes the master after the master downtime interval. (3 * hello interval).<br>• The VRRP holddown timer applies to the VRRP BackupMaster feature. |
| HoldDown State | When Hold Down Timer is counting down status is active and preemption occurs. The text box displays dormant when preemption is not pending. |
| HoldDownTime Remaining | The remaining time (in seconds) before preemption. |
| CriticalIpAddr Enable | Sets the IP interface on the local router to enable or disable the backup. |
| CriticalIpAddr | An IP interface on the local router configured so that a change in its state causes a role switch in the virtual router (for example, from master to backup) in case the interface stops responding. |
| BackUpMaster Enable | Indicates if the VRRP backup master is enabled or disabled. This option is not recommended for non Split-MLT ports. |
| BackUpMaster State | Displays the BackupMaster operational state. The BackUpMaster state is down if VRRP is enabled on a switch during the master state . The BackUpMaster state is up if VRRP is enabled on a switch during the backup state.<br>• up: during BackupMaster state<br>• down: during the original state |

# Viewing and configuring IPv6 routing

In the Routing Manager navigation pane, the navigation tree shows the IP addresses of discovered devices. Icons associated with IP addresses on the branches indicate the following types of routes:

- IPv6 Routing
- IPv6 OSPF

This section contains information about configuring routes for IPv6 routes and protocols. This section includes information about the following topics:

- Configuring IPv6 routing on page 203
- Configuring IPv6 OSPF on page 205

For a list of devices that support IPv6 routing, see Supported devices for Routing Manager on page 179.

# Configuring IPv6 routing

This section contains information about the following topics:

- Configuring IPv6 routing Globals on page 203
- Configuring IPv6 routing Interfaces on page 204

## Configuring IPv6 routing Globals

Perform the following procedure view the IPv6 routing global properties.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select a node under **IPv6 Networks, IPV6 ROUTING, Globals**.

   The Globals table appears in the contents pane.
2. To modify any of the configurable global routing properties, modify the fields directly in the contents pane and click **Apply Changes**.

### Job aid

The following table describes the fields in the IPv6 routing – Globals table.

| Field | Description |
|---|---|
| Devices | Identifies the device. |

| Field | Description |
|---|---|
| Forwarding | Indicates whether this entity is acting as an IPv6 router in respect to the forwarding of datagrams received by, but not addressed to, this entity. IPv6 routers forward datagrams. IPv6 hosts do not (except those source-routed through the host). |
| DefaultHopLimit | The default value inserted into the Hop Limit field of the IPv6 header of datagrams originated at this entity whenever a Hop Limit value is not supplied by the transport layer protocol. |
| Interfaces | The number of IPv6 interfaces (regardless of their current state) present on this system. |
| IfTableLastChange | The value of sysUpTime at the time of the last insertion or removal of an entry in the ipv6IfTable. If the number of entries is unchanged since the last reinitialization of the local network management subsystem, then this object contains a zero value. |
| IcmpNetUnreach | Enables or disables ICMP net unreach feature. |
| IcmpRedirectMsg | Enables or disables ICMP redirect feature. |
| IcmpErrorInterval | The rate (in milliseconds) at which ICMP error messages can be sent out. A value of zero indicates that no ICMP error messages are sent. |
| MulticastAdminStatus | This indicates the global admin status for multicast. |
| FasterAdvIntervalEnable | |
| FasterAdvInterval | |

## Configuring IPv6 routing Interfaces

Perform the following procedure configure IPv6 routing properties for interfaces.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select a node under **IPv6 Networks, IPV6 ROUTING, Interfaces**.

   The Interfaces table appears in the contents pane.
2. To add an interface entry, from the menu bar, click **Add Entry**.

   The IPv6 Routing - Insert Interface dialog box appears.
3. Complete the fields as required.
4. Click **Save**.
5. Click **Ok** or **Details** if there are errors or warnings.

   The new entry appears in the contents pane.

### Job aid

The following table describes the fields in the IPv6 Routing – Interfaces table.

| Field | Description |
|---|---|
| Interface | A unique value to identify a physical interface or a logical interface (VLAN). For the brouter port, this is the ifindex of the port. For the VLAN, this is the ifindex of the VLAN. |
| Identifier | IPv6 address interface identifiers. This is a binary string of up to 8 octets in network byte-order. |
| IdentifierLength | The length of the interface identifier in bits. |
| Descr | A textual string containing information about the interface. This string can be set by a network management system. |
| VlanId | A value that uniquely identifies the VLAN associated with this entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag. |
| Type | The interface type. |
| ResmMaxSize | MTU for this IPv6 interface. This value should be the same for all the IP addresses defined on this interface. |
| PhysAddress | The media-dependent physical address. For Ethernet media, this is the MAC address. |
| AdminStatus | The indication of whether IPv6 is enabled (up) or disabled (down) on this interface. This object does not affect the state of the interface itself, only its connection to an IPv6 stack. |
| OperStatus | Operating status of the interface. |
| ReachableTime | The time (in milliseconds) a neighbor is considered reachable after receiving a reachability confirmation. Reference RFC2461, Section 6.3.2 |
| RetransmitTime | The time (in milliseconds) between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Reference RFC2461, Section 6.3. |
| MulticastAdminStatus | The admin status for multicast for this interface. |

## Configuring IPv6 OSPF

This section contains information about the following topics:


- Configuring IPv6 OSPF General on page 206
- Configuring IPv6 OSPF Interfaces on page 208

- Configuring IPv6 OSPF Area on page 210
- Configuring IPv6 OSPF Neighbors on page 212

For a list of devices that support IPv6 OSPF, see Supported devices for Routing Manager on page 179.

## Configuring IPv6 OSPF General

Perform the following procedure configure IPv6 OSPF general properties.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select a node under **IPv6 Networks, IPv6 OSPF, General**.

   The IPv6 OSPF—General table appears in the contents pane.

2. To modify any of the configurable IPv6 OSPF general routing properties, modify the fields directly in the contents pane and click **Apply Changes**.

### Job aid

The following table describes the fields in the IPv6 OSPF – Globals table.

| Field | Description |
|---|---|
| Devices | Identifies the device. |
| RouterId | Identifies the router independent of other routers in the OSPF domain. The router ID has the same format as an IPv6 address. |
| AdminStat | The administrative status of OSPF in the router. Enabled indicates that you can activate OSPF interfaces. Disabled deactivates OSPF on all interfaces. |
| VersionNumber | Current version number of OSPF. |
| AreaBdrRtr Status | A read-only flag identifying this router as an area border router (ABR).<br>**Important:**<br>The AreaBdrRtrStatus value must be true to create a virtual router interface. |
| ASBdrRtrStatus | When you select the ASBdrRtrStatus option, the router is configured as an autonomous system boundary router (ASBR). |
| AsScopeLsa Count | A read-only field displaying the number of external (LS type 5) LSAs in the link-state database. |
| AsScopeLsa CksumSum | A read-only field displaying the 32-bit unsigned sum of the LS checksums of the external LSAs in the link-state database. This sum determines changes and compares the linkstate databases of two routers. |
| Originate NewLsas | A read-only field displaying the number of new LSAs. The number is incremented each time the router originates a new LSA. |

| Field | Description |
|---|---|
| RxNewLsas | A read-only field displaying the number of new LSAs received. This number does not include new instantiations of self-originated LSAs. |
| ExtLsaCount | A read-only field displaying the number of external (LS type 0x4005) LSAs in the link-state database. |
| ExtArea LsdbLimit | The maximum number of nondefault AS-external LSA entries stored in the link-state database. If the value is —1, then there is no limit. The default is -1. You must set the LSDB limit to the same value for all routers attached to the OSPFv3 backbone or any regular OSPFv3 area (that is, OSPFv3 stub areas and NSSAs are excluded). |
| Multicast Extensions | A bit mask indicating whether the router is forwarding IPv6 multicast datagrams based on the algorithms defined in the multicast extensions to OSPF. Possible forwarding includes:<br>• intraAreaMulticast—forwards to directly attached areas (called intra-area multicast routing)<br>• interAreaMulticast—forwards between OSPFv3 areas (called inter-area multicast routing)<br>• interAsMulticast—forwards between Autonomous Systems (called inter-AS multicast routing) |
| ExitOverflow Interval | The number of seconds that, after entering the overflow state, a router attempts to leave the overflow state. This allows the router resend nondefault AS-external LSAs. When the value is set to 0, the router does not leave the overflow state until the router is restarted. |
| Demand Extensions | The router support for demand routing. |
| Traffic Engineering Support | The router support for traffic engineering extensions. |
| Reference Bandwidth | The reference bandwidth in kilobits per second for calculating default interface metrics. The default value is 100 000 Kb/s (100 Mb/s). |
| RestartSupport | The router support for OSPF hitless restart. Options include no restart support, only planned restarts, or both planned and unplanned restarts. Options include:<br>• none (default)<br>• plannedOnly<br>• plannedAndUnplanned |
| RestartStatus | A read-only field indicating the current status of OSPF hitless restart. Options include: |

| Field | Description |
|---|---|
| | • notRestarting (default)<br>• plannedRestart<br>• unplannedRestart |
| RestartInterval | The configured OSPF hitless restart timeout interval in the range 1 through 1800 seconds. |
| RestartAge | A read-only field indicating the remaining time in the current OSPF hitless restart interval in seconds. The range is 1 to 1800. |
| RestartExit Reason | A read-only field indicating the outcome of the last attempt at a hitless restart. Options include:<br>• none: indicates no restart was attempted<br>• inProgress: indicates a restart attempt is currently underway<br>• completed: indicates a completed restart<br>• timedout: indicates a timed out restart<br>• topologyChanged: indicates a cancelled restart due to topology change |

## Configuring IPv6 OSPF Interfaces

Perform the following procedure configure IPv6 OSPF interfaces.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager, and select a node under **IPv6 Networks, IPv6 OSPF, Interfaces**.
2. To modify any of the configurable IPv6 OSPF interface properties, modify the fields directly in the contents pane, and click **Apply Changes**.

### Job aid

The following table describes the fields in the IPv6 OSPF – Interfaces table.

| Field | Description |
|---|---|
| Index | The interface index of this OSPFv3 interface. The index corresponds to the interface index of the IPv6 interface where OSPFv3 is configured. |
| AreaId | Dotted decimal value to designate the OSPF area name. VLANs that maintain the default area setting on the interface cause the LSDB to be inconsistent. |

| Field | Description |
|---|---|
| | **Important:**<br>The area name is not related to an IPv6 address. You can use any value for the OSPF area name (for example, 1.1.1.1 or 200.200.200.200). |
| Type | Type of OSPF interface (broadcast, nbma, point-to-point, or point-to-multipoint). |
| AdminStat | Current administrative state of the OSPF interface (enabled or disabled). |
| RtrPriority | OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become the designated router or the backup. The priority is used only during election of the designated router and backup designated router. The range is 0 to 255. The default is 1. |
| TransitDelay | Length of time, in seconds (1 through 1800), required to transmit an LSA update packet over the interface. |
| RetransInterval | Length of time, in seconds (1 through 1800), required between LSA retransmissions. |
| HelloInterval | Length of time, in seconds, between Hello packets. This value must be the same for all routers attached to a common network.<br>**Important:**<br>When you change the Hello interval values, you must save the configuration file and reboot the switch for the values to be restored and checked for consistency. |
| RtrDeadInterval | Adjacent routers use this interval to determine if the router has been removed from the network. The interval must be identical on all routers on the subnet and a minimum of four times the Hello interval. To avoid interpretability issues, the RtrDeadInterval value for the OSPF interface must match the RtrDeadInterval value for the OSPF virtual interface. |
| PollInterval | Length of time, in seconds, between Hello packets sent to an inactive OSPF router. |
| State | A read-only field indicating the OSPFv3 interface state. Options include:<br>• down<br>• loopback<br>• waiting<br>• pointToPoint<br>• designatedRouter |

| Field | Description |
|---|---|
| | • backupDesignatedRouter<br>• otherDesignatedRouter |
| Designated Router | A read-only field indicating the router ID of the designated router. |
| BackupDesignated Router | A read-only field indicating the router ID of the backup designated router. |
| Events | A read-only field indicating the number of times this OSPF interface changed state or an error occurred. |
| MetricValue | The metric assigned to this interface. The default value of the metric is the Reference Bandwidth or ifSpeed. The value of the reference bandwidth is configured by the rcOspfv3ReferenceBandwidth object. |
| LinkScope LsaCount | A read-only field indicating the number of Link-Scope LSAs in the link-state database. |
| LinkLsaCksum Sum | A read-only field indicating the 32-bit unsigned sum of the Link-Scope link-state advertisement LS checksums in the link-state database. The sum determines a change in the router link-state database and compares the link-state database of two routers. |
| InstId | Enables multiple instances of OSPFv3 over a single link. The switch assigns each protocol instance a separate ID. This ID has local link significance only. |
| DemandNbr Probe | Indicates whether neighbor probing is enabled. Neighbor probing determines whether the neighbor is inactive. |
| DemandNbr ProbeRetxLimit | The number of consecutive LSA retransmissions before the neighbor is deemed inactive and the neighbor adjacency is deactivated. |
| DemandNbr ProbeInterval | Defines how often, in seconds, the neighbor is probed. |

## Configuring IPv6 OSPF Area

Perform the following procedure configure IPv6 OSPF areas.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select a node under **IPv6 Networks, IPv6 OSPF, Area**.

   The IPv6 OSPF – Area table appears in the contents pane.

2. To add an area, from the menu bar, click **Add Entry**.

   The Insert Areas dialog box appears.

3. Complete the fields as required.

4. Click **Save**.
5. Click **Ok** or **Details** if there are errors or warnings.

   The new entry appears in the contents pane.

## Job aid

The following table describes the Configuration of IPv6 OSPF area.

| Field | Description |
|---|---|
| Id | A 32-bit integer uniquely identifying an area. Area ID 0.0.0.0 is used for the OSPF backbone. VLANs that maintain the default area setting on the interface cause the LSDB to be inconsistent. |
| ImportAsExtern | The support for importing AS-external LSAs. Options include importExternal (default), importNotExternal, or importNssa (not so stubby area). |
| SpfRuns | Indicates the number of SPF calculations OSPF performs. |
| BdrRtrCount | The number of area border routers reachable within this area. The switch calculates the value, initially zero, in each SPF pass. |
| AsBdrRtrCount | The total number of autonomous system border routers reachable within this area. The switch calculates the value, initially zero, in each SPF pass. |
| ScopeLsaCount | The number of LSAs in the area link-state database, excluding AS External LSAs. |
| ScopLsaCksum Sum | The 32-bit unsigned sum of the LSAs. This sum excludes external (LS type 5) LSAs. The sum determines changes in a router link-state database and compares the link-state databases of two routers. |
| Summary | The area support for summary advertisements in a stub area. |
| StubMetric | The number of active interfaces in this area. |
| NssaTranslator Role | Indicates an NSSA border router ability to translate NSSA type-7 LSAs into type-5 LSAs. Options include:<br>• always<br>• candidate (default) |
| NssaTranslator State | Indicates if and how an NSSA border router translates NSSA type-7 LSAs into type-5 LSAs. Options include: |

| Field | Description |
|---|---|
| | • enabled indicates the NSSA border router translator role is set to always.<br>• elected indicates a candidate NSSA border router is translating type-7 LSAs into type-5.<br>• disabled indicates a candidate NSSA border router is not translating type-7 LSAs into type-5. |
| NssaTranslator StabilityInterval | The number of seconds after an elected translator determines translation is not required that it resumes translation duties. |
| NssaTranslator Events | A read-only field indicating the number of Translator State changes that occurred since the last bootup. |
| StubMetricType | Sets the type of metric advertised as a default route:<br>• rcOspfv3Metric indicates the OSPF metric<br>• comparableCost indicates an external type 1<br>• nonComparable indicates an external type 2 |

## Configuring IPv6 OSPF Neighbors

Perform the following procedure configure IPv6 OSPF neighbors.

### Procedure steps

1. In the COM navigation pane, expand the managers, click on the Routing Manager and select a node under **IPv6 Networks, IPv6 OSPF, Neigbors**.

   The IPv6 OSPF – Neighbors table appears in the contents pane.
2. Select and modify any of the fields in the table.
3. Click **Apply Changes**.

## Job aid

The following table describes the fields in the IPv6 OSPF – Neighbors table.

| Field | Description |
|---|---|
| Interface | A read-only field indicating the local link ID of the link over which the neighbor is reached. |
| RtrId | A read-only field indicating the router ID of the neighboring router, which in OSPF has the same format as an IPv6 address but identifies the router independent of IPv6 address. |

| Field | Description |
|---|---|
| AddressType | A read-only field indicating the address type of rcOspfv3NbrAddress. Only IPv6 addresses without zone index are expected. Options include:<br>• unknown<br>• ipv6<br>• ipv6z<br>• dns |
| Address | A read-only field indicating the IPv6 address for the neighbor associated with the local link. |
| Options | A read-only field indicating the bit mask corresponding to the options field on the neighbor. |
| Priority | A read-only field indicating the preferential treatment assignment, which places the transmitted packets into queues. The priority field also indicates the possible selection of the priority field in the data link header when the switch forwards the packet. |
| State | A read-only field indicating the OSPF interface state:<br>• down<br>• attempt<br>• init<br>• twoWay<br>• exchangeStart<br>• exchange<br>• loading<br>• full |
| Events | A read-only field indicating the number of state changes or error events occurring between the OSPF router and the neighbor router. |
| LsRetransQLen | A read-only field indicating the number of elapsed seconds between advertising retransmissions of the same packet to a neighbor. |
| Hello Suppressed | A read-only field indicating whether Hellos are suppressed at a neighbor. |
| IfId | A read-only field indicating the interface ID that the neighbor advertises in Hello packets on this link, that is, the neighbor local interface index. |
| RestartHelper Status | A read-only field indicating that the router acts as a hitless restart helper for the neighbor. Options include:<br>• notHelping<br>• helping |

| Field | Description |
|---|---|
| RestartHelper Age | A read-only field indicating the time remaining in the current OSPF hitless restart interval, if the router acts as a restart helper for the neighbor. The range is 1 through 1800 seconds. |
| RestartHelper ExtReason | A read-only field indicating the outcome of the last attempt to act as a hitless restart helper for the neighbor. Options include:<br>• none: indicates no restart was attempted (default)<br>• inProgress: indicates a restart attempt is currently underway<br>• completed: indicates a completed restart<br>• timedout: indicates a timed-out restart<br>• topologyChanged: indicates a cancelled restart due to the topology change |

# Chapter 8: Configuration of Trap/Log Manager

The Trap/Log Manager is a Configuration and Orchestration Manager (COM) manager that allows you to configure and view the traps/notifications and the system log. This manager combines the functionality of the original Trap Receiver and Log Manager, and adds trap/notification configuration and syslog configuration.

You can configure the network manager to which the traps are sent using this manager. You can also configure the severity of the log, the host, and the port to which the log is sent. The trap receiver shows the traps received from the configured devices.

Similarly, the syslog receiver shows the system log for the configured devices.

**Note:**

Avaya Virtual Services Platform (VSP) and Avaya Wireless Controller (WC) devices are supported, and appear in the interface with the ERS family in the tree.

For WC 8xxx devices, the Trap/Log Manager functions the same way as the mERS 5600 family of devices. The WC family of devices appears in the UI with the mERS5600 family in the tree.

### Navigation



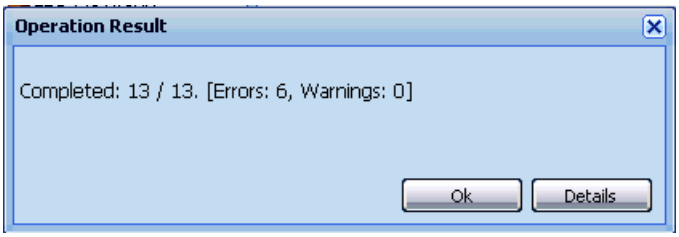
## Starting Trap/Log Manager

Perform the following procedure to start Trap/Log Manager.

### Procedure steps

1. In the **Configuration and Orchestration Manager Navigation** tree, expand **Managers**.
2. Click **Trap/Log Manager** icon.

COM automatically launches the device discovery, and displays the operation result (errors and warnings), as shown in the following figure.




3. Click **Ok** to view Trap/Log Manager tab.

   **OR**

   Click **Details** to view errors or warnings, if any.

   The following figure shows the Trap/Log Manager window.

# Trap/Log Manager window

The following figure shows the Trap/Log Manager window.

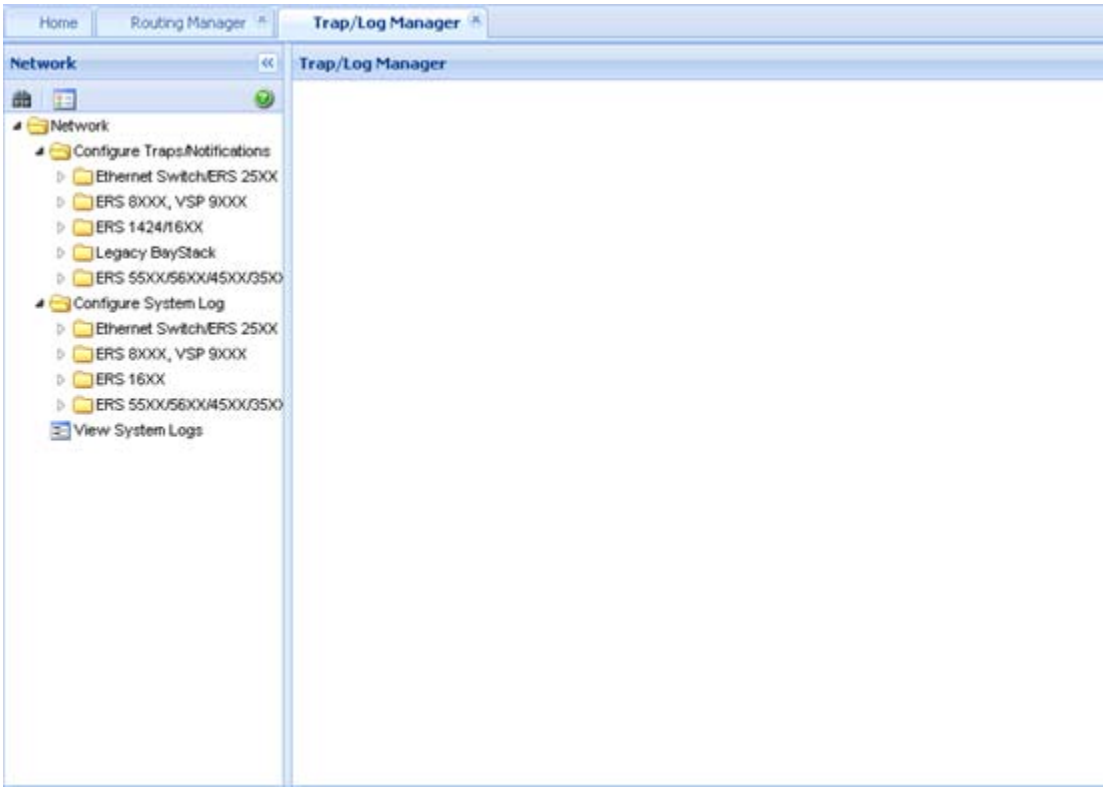



**Figure 24: Trap/Log Manager window**

The following table describes the parts of the Trap/Log Manager window.

**Table 47: Parts of the Trap/Log Manager window**

| Part | Description |
|---|---|
| Tool bar | Provides quick access to commonly used Trap/Log Manager commands. For more information, see Tool bar buttons on page 217. |
| Navigation pane | Allows you to navigate to the settings for the current network devices. For more information, see Navigation pane on page 218. |
| Contents pane | Displays details of the folder selected on the navigation pane. For more information, see Contents pane on page 218. |

# Tool bar buttons

The following table describes the Trap/Log Manager tool bar buttons.

**Table 48: Tool bar buttons**

| Button | Description |
|---|---|
| Discover Trap/Log | Discovers the devices for the Trap/Log Manager. |
| Preferences | Allows you to set the preferences for working with the Trap/ Log Manager. |

## Navigation pane

The Trap/Log Manager navigation pane displays a hierarchical folder tree that you can use to navigate to the groups.

The following figure shows the navigation pane of the Trap/Log Manager window.

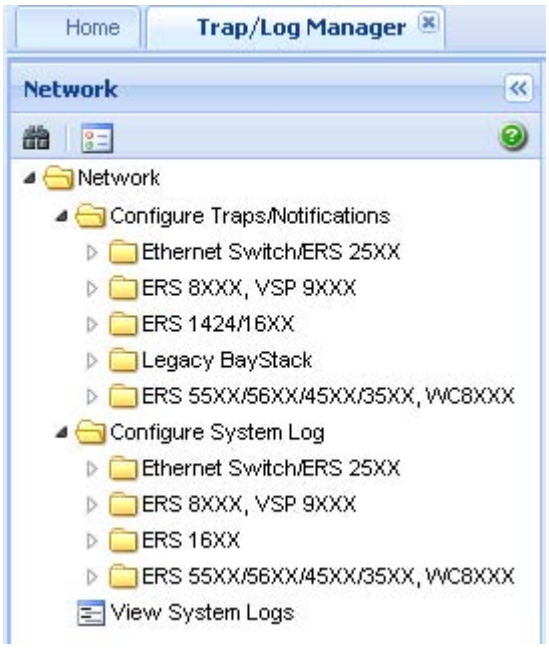



**Figure 25: Navigation pane**

## Contents pane

The contents pane displays detailed information for the element selected in the navigation pane.

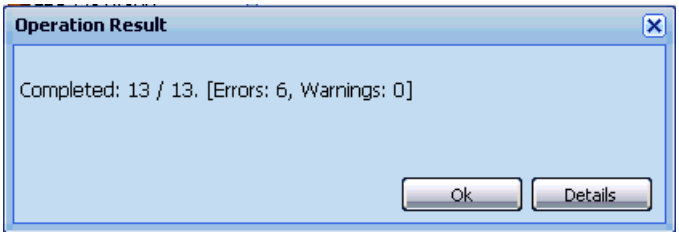
# Discovering devices

You can discover the information in the Trap/Log Manager window with trap/log information polled from the network devices. You can use this feature to load any updated information that took effect since you opened Trap/Log Manager. Perform the following procedure to discover traps/logs.

### Procedure steps

Click on the **Discover Trap/Log** button in the tool bar.

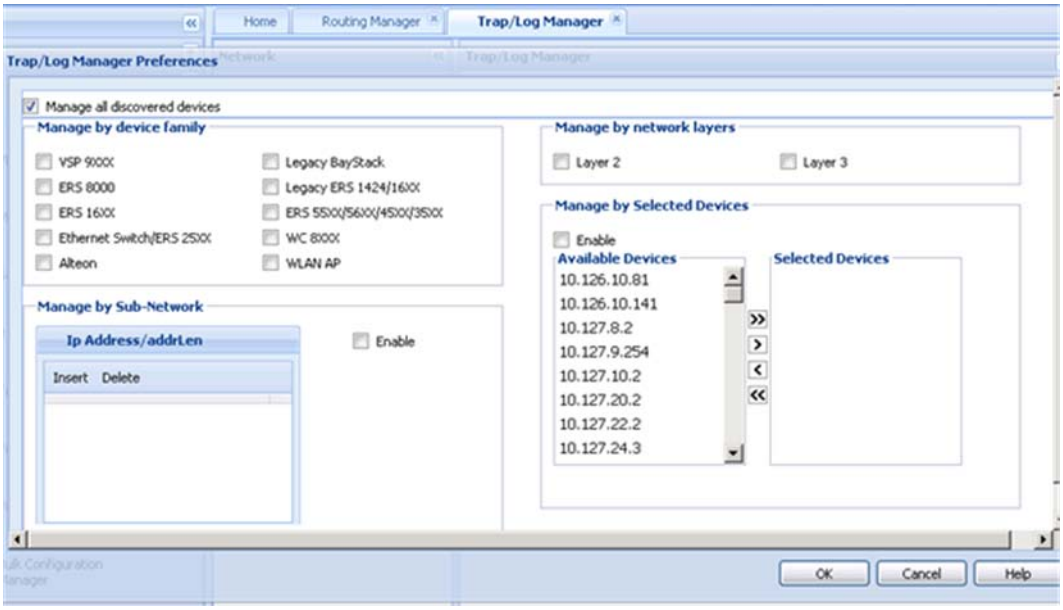
COM initiates the device discovery, and displays the operation result (errors and warnings), as shown in the following figure.




# Displaying Preferences

You can select the specific set of assigned devices to be used in the Trap/Log Manager discovery process in the Trap/Log Manager Preferences dialog box, based on several criteria.

Click **Preferences** button in the tool bar. The Trap/Log Manager preferences dialog box appears.




For more information on editing the Preferences, see Setting File Inventory Manager preferences on page 265.

# Configuring Traps

For instructions on configuring traps for ERS, VSP, and WC devices, see the following sections.

- Configuring Trap Receivers for ERS and WC devices on page 220
- Configuring Target Address Table for ERS, VSP and WC devices on page 222
- Configuring Target Params Table for ERS, VSP, and WC devices on page 224
- Configuring Notify Table for ERS, VSP, and WC devices on page 226

## Configuring Trap Receivers for ERS and WC devices

Perform the following procedure to configure trap/logs for the following devices:

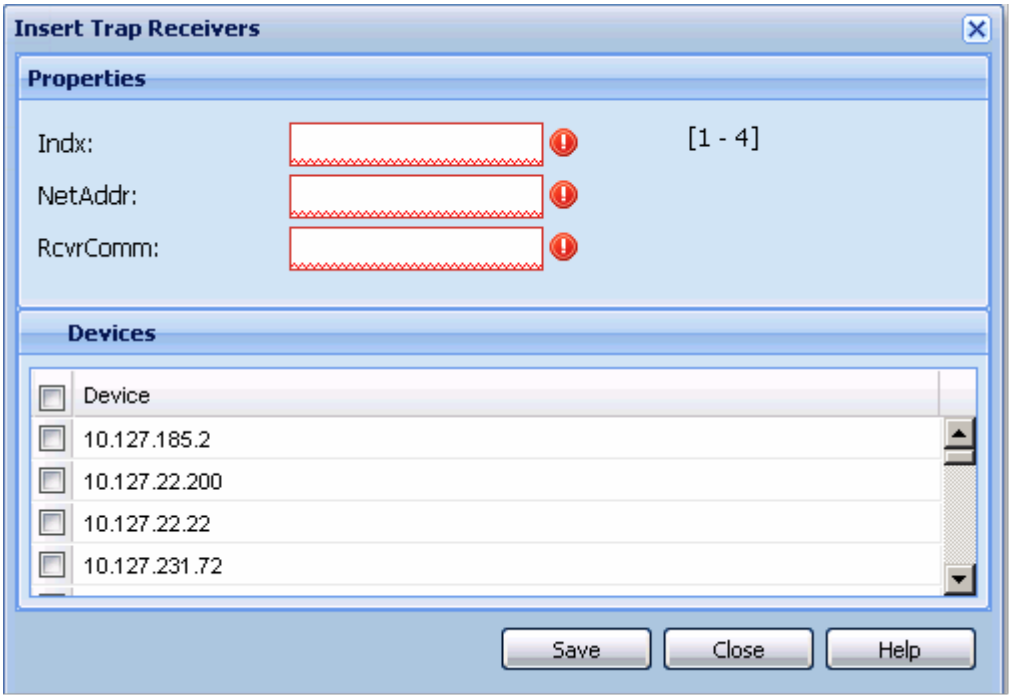
- ERS 25XX
- ERS 55XX/56XX/45XX/35XX, WC 8XXX

### Procedure steps

1. In the **Trap/Log Manager** navigation tree, click **Configure Traps/Notifications**.
2. Choose the switch for which you want to configure trap receivers.

3. In the contents pane, click the **Trap Receivers** tab.
4. To add a trap receiver entry for a device, click the **Add** button in the tool bar.

   The Insert Trap Receiver dialog box appears.




5. Populate the fields as required.
6. Click **Save**.

   A row corresponding to the newly created trap receiver is added to the table in the contents pane.

You can also edit the existing trap receiver by editing the corresponding cells.

## Job aid

The following table describes the Insert Trap Receiver dialog box fields:

| Part | Definition |
|---|---|
| Indx | Specifies the index value. Ranges from 1 to 4. |
| NetAddr | Specifies the network address. |
| RcvrComm | Specifies the receiver address. |
| Devices | Allows you to set these values for other similar devices. |

# Configuring Target Address Table for ERS, VSP and WC devices

Perform the following procedure to configure Target Address Table for the following devices:

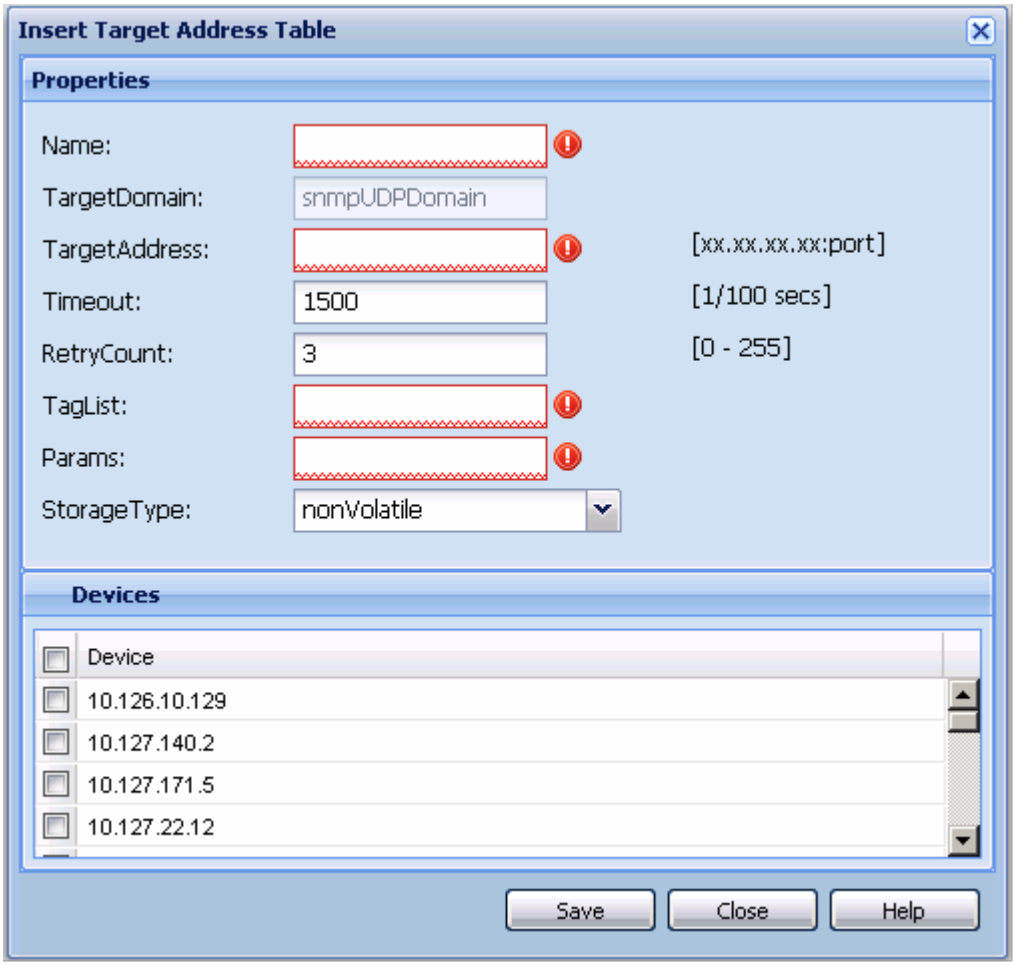
- ERS 25XX
- ERS 55XX/56XX/45XX/35XX, WC 8XXX
- ERS 8000, VSP 9XXX
- ERS 1424/16XX

### Procedure steps

1. In the Trap/Log Manager navigation tree, click Configure Traps/Notifications.
2. Choose the switch for which you want to configure target addresses.
3. In the contents pane, click the Target Address Table tab.

   By default, the Target Address Table tab opens.
4. To add a target address entry for a device, click the Add button in the tool bar

   The Insert Target Address Table dialog box appears.




5. Enter the values in the fields as required.
6. Click Save.

   A row corresponding to the newly created Target Address is added to the table in the Contents pane.

You can edit the existing Target Address entries by editing the corresponding cells.

You can modify any of the configurable global routing properties directly in the Contents pane and save the changes by clicking Apply changes.

## Job aid

The following table describes the Insert Target Address Table dialog box fields.

| Part | Definition |
|---|---|
| Name | Specifies the name of the target table. |
| TDomain | Specifies the TDomain for the target table. |

| Part | Definition |
|---|---|
| TAddress | The IP address and the host of the target and the UDP port number.<br>**Important:**<br>Port 162 is reserved for SNMP traps. |
| Timeout | The maximum round trip time required for communicating with the transport address defined by this row. |
| RetryCount | The number of retries to be attempted when a response is not received for a generated message. |
| TagList | Specifies a list of tag values. A tag value refers to a class of targets to which the messages may be sent. |
| Params | The string value that identifies snmpTargetParamsTable entries. |
| StorageType | Specifies the storage type. Default value is nonVolatile. |

# Configuring Target Params Table for ERS, VSP, and WC devices

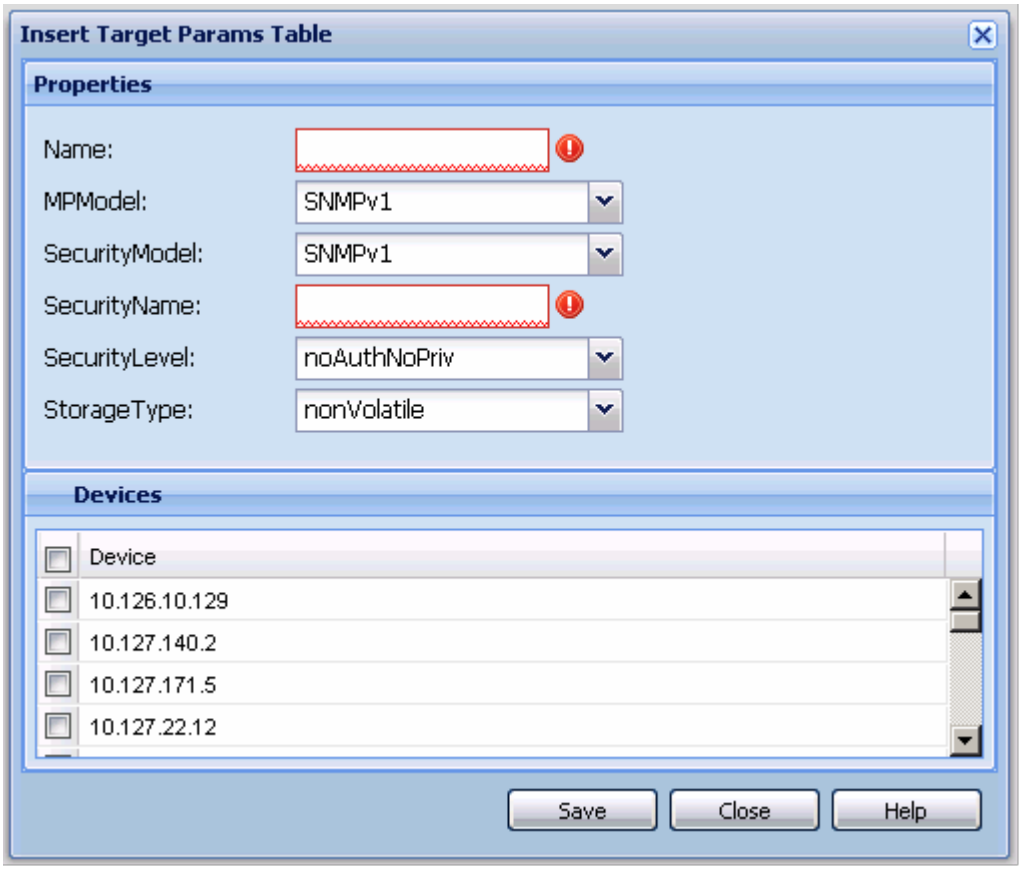
Perform the following procedure to configure Target Params Table for the following devices:

- ERS 25XX
- ERS 55XX/56XX/45XX/35XX, WC 8XXX
- ERS 8000, VSP 9XXX
- ERS 1424/16XX

### Procedure steps

1. In the **Trap/Log Manager** navigation tree, click **Configure Traps/Notifications**.
2. Choose the switch for which you want to configure target parameters.
3. In the contents pane, click the **Target Params Table** tab.
4. To add a target parameter entry for a device, click the **Add** icon in the tool bar menu.

   The Insert Target Params dialog box appears.




5. Enter the values in the fields as required.
6. Click **Save**.

   A row corresponding to the newly created Target Params entry is added to the table in the contents pane.

   You can edit the existing values by editing the corresponding cells and clicking **Apply Changes**.

## Job aid

The following table describes he Insert Target Params dialog box fields.

| Part | definition |
|---|---|
| Name | Specifies the unique name of the target parameters table. |
| MPModel | Specifies the Message Processing model, SNMPv1, SNMPv2c, or SNMPv3/USM. Default value is SNMPv1. |
| SecurityModel | Specifies the security model, SNMPv1, SNMPv2c, or SNMPv3/USM. Default value is SNMPv1. |

| Part | definition |
|---|---|
| SecurityName | Specifies a new security name, which identifies the principal to generate SNMP messages. |
| SecurityLevel | The security level. The valid options are noAuthNoPriv, authNoPriv, and authPriv. Default value is noAuthNoPriv. |
| StorageType | Specifies the storage type. Default value is non-volatile. |
| Multiple Devices Insertion | Allows you to set these values for other similar devices. |

# Configuring Notify Table for ERS, VSP, and WC devices

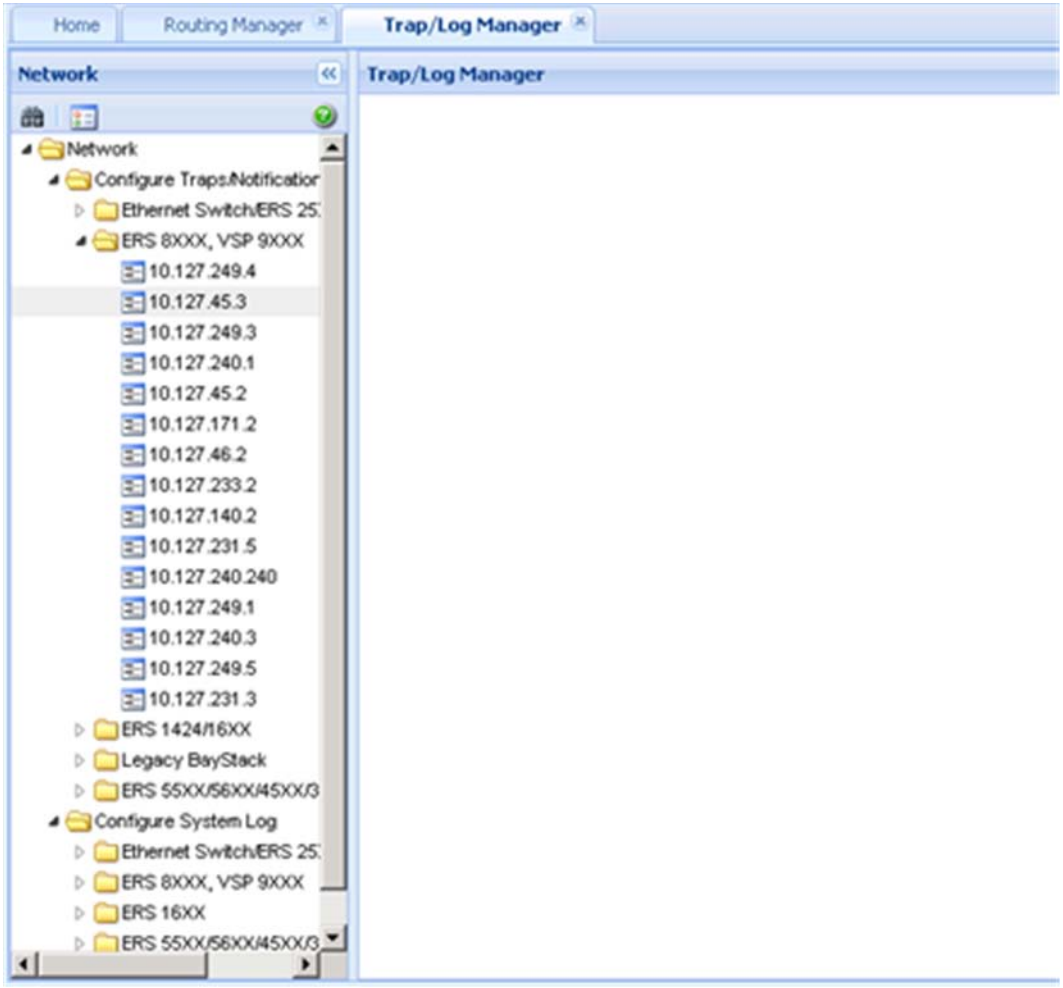
Perform the following procedure to configure Notify Table for the following devices:

- ERS 25XX
- ERS 55XX/56XX/45XX/35XX, WC 8XXX
- ERS 8000, VSP 9XXX
- ERS 1424/16XX

## Procedure steps

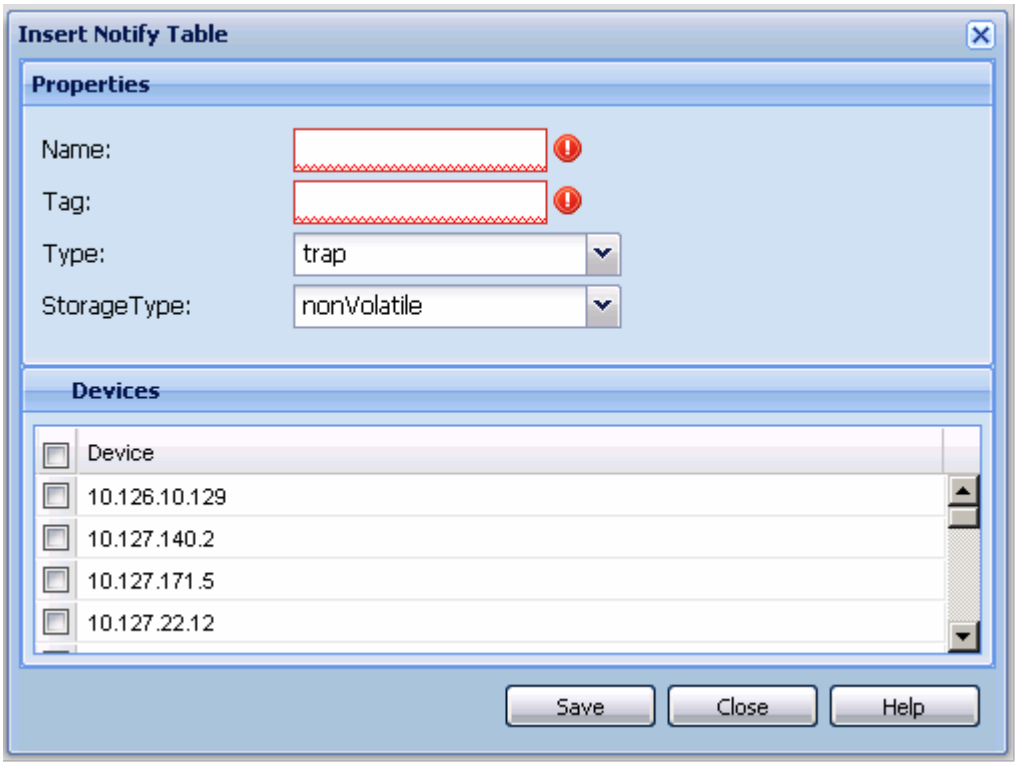
1. In the **Trap/Log Manager** navigation tree, click **Configure Traps/Notifications**.
2. Choose the switch for which you want to configure notifications.
3. In the contents pane, click the **Notify Table** tab.

   The Notify Table window appears.




4. To add a notification entry for a device, click the **Add** icon in the tool bar.

   The Insert Notify Table dialog box appears.




5. Enter the values in the fields as required.
6. Click **Save**.

   A row corresponding to the newly created notification is added to the table in the contents pane.

   You can modify any of the existing notifications by modifying the fields directly in the Contents pane and clicking **Apply Changes**.

## Job aid

The following table describes the Insert Trap Receiver dialog box fields.

| Part | definition |
|---|---|
| Name | Specifies the unique identifier associated for the notify table. |
| Tag | A single tag value used to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable that contains a tag value equal to the value of an instance of this object is selected. If this object contains a value of zero length, no entries are selected. |
| Type | This object determines the type of notification generated for entries in the snmpTargetAddrTable that are selected by the corresponding instance of snmpNotifyTag. If the value of this object is trap, then any messages generated for selected rows contain SNMPv2-Trap PDUs. |

| Part | definition |
|---|---|
| | If the value of this object is inform, then any messages generated for selected rows contain Inform PDUs.<br>**Important:**<br>If an SNMP entity only supports generation of traps (and not informs), then this object is read-only. |
| StorageType | Specifies the storage type. Default value is other. |

# Configuring System Log

The Trap/Log Manager lists the devices that support System Log configuration that are discovered using the Topology Manager. In each of the configuration nodes, the devices are grouped by family of device. Each device can be selected to see the configuration.

To display the devices, expand the **Configure System Log navigation** tree.

**Important:**
The Add icon on the tool bar is enabled only on clicking a device.

### Navigation

- Configuring System Log for ERS and VSP devices on page 229
- Enabling System Log for ERS, VSP, and WC devices on page 231

# Configuring System Log for ERS and VSP devices

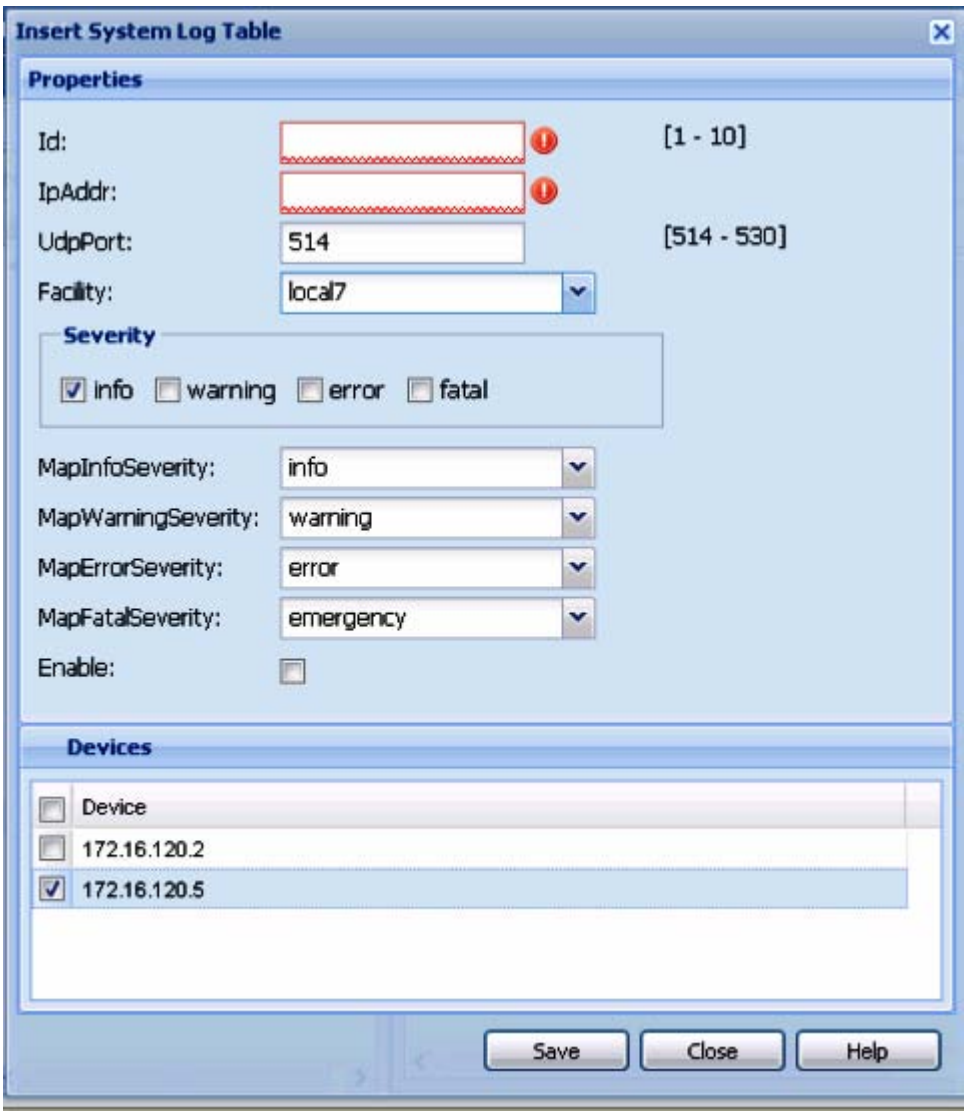
Perform the following procedure to create a system log for the following devices:

- ERS 8000, VSP 9XXX
- ERS 1424/16XX

### Procedure steps

1. In the **Configure System Log** folder, choose a device to create a system log.
2. Click **System Log Table** tab.
3. Click **Add** button on the tool bar.

   The Insert Syslog Log Table dialog box appears.




4. Enter values in the fields as required.
5. Click **Save**.

   To modify any of the configurable SyslogHost interface properties, modify the fields directly in the contents pane and click **Apply Changes** on the tool bar.

## Job aid

The following table describes the Insert Syslog dialog box fields.

| Part | Definition |
|---|---|
| Id | ID for the syslog host being created. |
| IPAddr | IP address of the syslog host. |

| Part | Definition |
|---|---|
| UdpPort | The UDP port to use to send messages to the syslog host (514 to 530). Default value is 514. |
| Facility | The syslog host facility used to identify messages (LOCAL0 to LOCAL7). |
| Severity | The Ethernet Routing Switch 8000 Series message severity for which syslog messages will be sent. Default value has all values enabled: info, fatal, warning and error. |
| MapInfo Severity | The fields that map the Ethernet Routing Switch 8000 Series severity levels to syslog severity. Default value is info. |
| MapWarning Severity | The fields that map Ethernet Routing Switch 8000 Series warning severity levels to syslog severity. Default value is warning. |
| MapError Severity | The fields that map Ethernet Routing Switch 8000 error severity levels to syslog severity. Default value is error. |
| MapFatal Severity | The fields that map Ethernet Routing Switch 8000 fatal severity levels to syslog severity. Default value is emergency. |
| Enable | Enables or disables sending messages to the syslog host. Default value is false (not selected). |

## Enabling System Log for ERS, VSP, and WC devices

Perform the following procedure to enable the system log for the following devices:

- ERS 25XX
- ERS 55XX/56XX/45XX/35XX, WC 8XXX
- ERS 8000, VSP 9XXX
- ERS 1424/16XX

### Procedure steps

1. In the **Configure System Log** folder, choose a device for which to enable the system log.
2. In the **System Log** window, click in the **Enable** field.
3. Select the check box in the field.
4. To apply the changes, click the **Apply Changes** in the tool bar.

   The value in the **Enable** field is updated to **true**.

## Job aid

The following table describes the System Log tab fields.

| Part | Definition |
|---|---|
| Enable | Used to enable/disable the syslog feature. |
| MaxHosts | The maximum number of remote hosts considered active and able to receive messages from the syslog service. |
| OperState | The operational state of the syslog service. |

# Chapter 9: Using File Inventory Manager

The File Inventory Manager allows you to manage the hardware and software configurations for different devices. File Inventory Manager allows you to

- view hardware configurations
- view software configurations
- edit Preferences
- download files from a device
- upload files to a device
- backup configuration files
- restore configuration files
- archive configuration files
- synchronize configuration files
- upgrade devices
- compare runtime configuration with existing configurations

**Note:**

The File Inventory Manager workflow for VSP devices is the same as for the ERS 8600 device types. The only exception is that the image of the Virtual Serviced Platform (VSP) device has an altered screen which does not contain the TFTP server address. The File Inventory Manager workflow for the Wireless Controller (WC) devices is the same as the mERS5600 device type.

This section describes using File Inventory Manager. It includes the following information:

# About File Inventory Manager

File Inventory Manager has two primary functions—file management and inventory management. This section describes the capabilities provided by those functions.

This section contains information on the following topics:



## File management features

The file management features of File Inventory Manager allows you to upload and download files to and from network devices. For all devices that support multiple devices, you can also use File Inventory Manager to do bulk uploads or downloads to or from multiple devices. This feature makes it easier to deploy updated image or configuration files across your network.

The following table summarizes the file management capabilities of File Inventory Manager.

**Table 49: File Inventory Manager file management capabilities**

| Device family | Operation | Multiple devices | File types |
|---|---|---|---|
| ERS 8000<br>VSP 9xxx | Download | Yes | Any (for example image, WSM image, and configuration.) |
| | Upload | Yes | Any (image, configuration, syslog, etc.) |
| | Backup | Yes | Configuration or boot configuration |
| | Restore | Yes | Configuration or boot configuration |
| | Archive | Yes | Configuration or boot configuration |
| | Synchronize | Yes | Configuration or boot configuration |
| | Device upgrade wizard | Yes | Image |
| | Compare runtime | Yes | Configuration |
| Passport 1000 (legacy) | Not supported | | |
| Legacy ERS 1424/16xx | Download | Yes | Image or configuration |

| Device family | Operation | Multiple devices | File types |
|---|---|---|---|
| | Upload | Yes | Configuration or history log |
| | Backup | Yes | Configuration |
| | Restore | Yes | Configuration |
| | Archive | Yes | Configuration |
| | Synchronize | Yes | Configuration |
| | Device upgrade | Yes | Image |
| | Compare runtime | Yes | Configuration |
| Legacy ERS 1424/16xx | Download | Yes | Image or configuration |
| | Upload | Yes | Configuration or history log |
| | Backup | Yes | Configuration |
| | Restore | Yes | Configuration |
| | Archive | Yes | Configuration |
| | Synchronize | Yes | Configuration |
| | Device upgrade | Yes | Image |
| | Device upgrade wizard (ERS 16xx only) | Yes | Image |
| | Compare runtime | Yes | Configuration |
| Ethernet Routing Switch 55xx/35xx/ 45xx/25xx | Download | Yes | Image, configuration, firmware image, or ASCII configuration file |
| | Upload | Yes | Configuration only |
| | Backup | Yes | Configuration |
| | Restore | Yes | Configuration |
| | Archive | Yes | Configuration |
| | Synchronize | Yes | Configuration |
| | Device upgrade | Yes | Image |
| | Compare runtime | Yes | Configuration |
| Ethernet Switch | Upload | Yes | Image, configuration, firmware image*, or ASCII configuration file* |

| Device family | Operation | Multiple devices | File types |
|---|---|---|---|
| | | | * Ethernet Switch 460/470, Ethernet Switch 425 3.0 |
| | Download | Yes | Configuration only |
| | Backup | Yes | Configuration |
| | Restore | Yes | Configuration |
| | Archive | Yes | Configuration |
| | Synchronize | Yes | Configuration |
| | Device upgrade | Yes | Image |
| | Compare runtime | Yes | Configuration |
| Legacy BayStack | Download | Yes | Image, configuration, firmware image*, or ASCII configuration file* * BPS 2000 2.0.5 and up, BayStack 380 3.0, BayStack 420 3.0 |
| | Upload | Yes | Configuration only |
| | Backup | Yes | Configuration |
| | Restore | Yes | Configuration |
| | Archive | Yes | Configuration |
| | Synchronize | Yes | Configuration |
| | Device upgrade | Yes | Image |
| Alteon | Download | Yes | Image or configuration |
| | Upload | Yes | Configuration or dump file |
| | Backup | Yes | Configuration |
| | Restore | Yes | Configuration |
| | Archive | Yes | Configuration |
| | Synchronize | Yes | Configuration |
| | Device upgrade | Yes | Image |
| OM 1000 | Download | Yes | Image, configuration, firmware image, or ASCII configuration file |
| | Upload | Yes | Configuration only |
| | Backup | Yes | Configuration |
| | Restore | Yes | Configuration |
| | Archive | Yes | Configuration |

| Device family | Operation | Multiple devices | File types |
|---|---|---|---|
| | Synchronize | Yes | Configuration |
| | Device upgrade | Yes | Image |
| WLAN AP devices | Download | Yes | ApplicationImage or Configuration or NN Data file |
| | Upload | Yes | Configuration only |
| | Backup | Yes | Configuration |
| | Restore | Yes | Configuration |
| | Archive | Yes | Configuration |
| | Synchronize | Yes | Configuration |
| | Device upgrade | Yes | Image |

**Important:**

The actual file upload and download operations are performed by a Trivial File Transfer Protocol (TFTP) server. You can use either TFTP server software running on the COM management station, or you can designate a separate machine as the TFTP server.

## Inventory management features

The inventory management features of File Inventory Manager show you current information about the hardware and software discovered on your network.

- Device and chassis types
- Installed blades
- Serial and revision numbers
- Image and configuration file names and versions
- GBIC data

# Starting File Inventory Manager

Perform the following procedure to start File Inventory Manager.

The administrator must assign the File Inventory Manager in the MultiElementManager Assignment tab.

### Procedure steps

1. Select **Managers** from **Configuration and Orchestration Manager**, and then click the **File Inventory Manager** Icon.

   The Confirmation dialog box appears.

2. Click **Yes** to query the discovered devices for inventory information, or click **No** to get inventory information from a previously saved inventory file. If you click **No**, File Inventory Manager prompts you for the location of the inventory file. Browse the file and then click **Open Inventory**.

3. Select the device from the **Available Devices** list, click **>** or **>>** to move the highlighted devices in the **Selected Devices** list, and then click **Query Now**.

   The **File Inventory Manager** dialog box appears.

   **Important:**
   Discovery process does not include devices without proper credentials assigned to them.

# Using the File Inventory Manager window

The following figure shows the File Inventory Manager window.

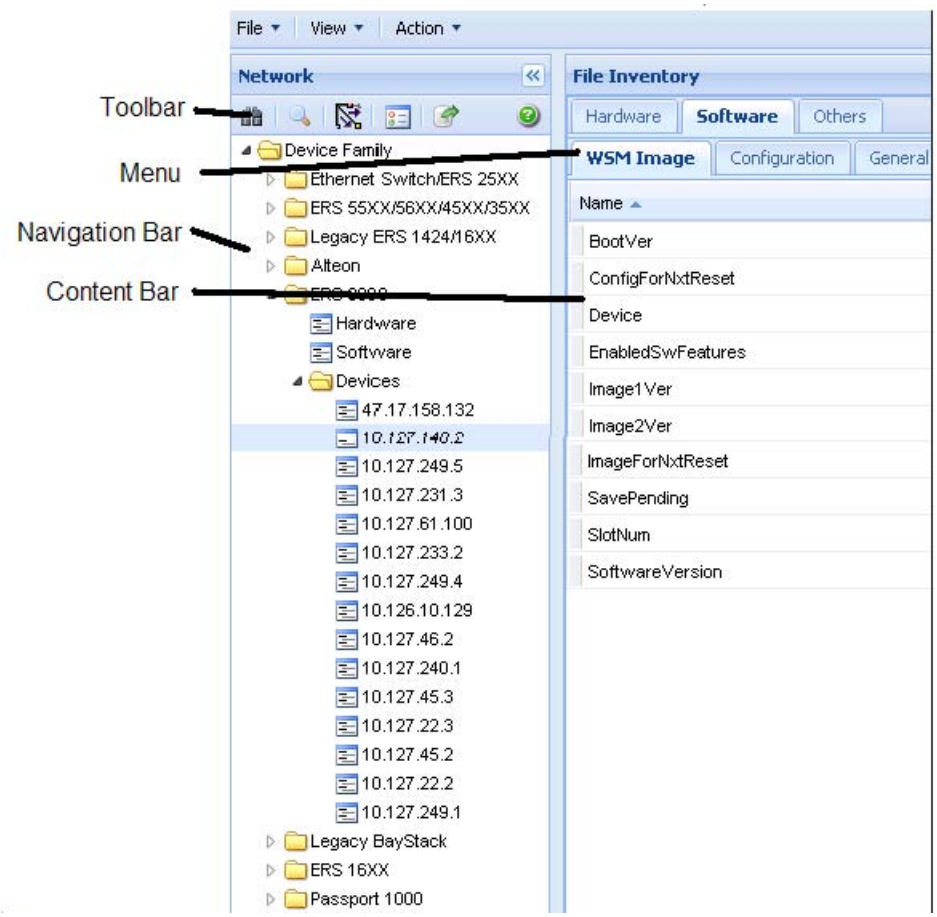



**Figure 26: File Inventory Manager window**

The following table describes the parts of the File Inventory Manager window.

**Table 50: Parts of the File Inventory Manager window**

| Part | Description |
|---|---|
| Menu bar | Provides access to all File Inventory commands. For more information, see Tool bar commands on page 240. |
| Tool bar | Provides quick access to commonly used File Inventory commands. For more information, see Tool bar commands on page 240. |
| Navigation pane | Allows you to navigate File Inventory elements for devices discovered on the network. For more information, see Navigation pane on page 241. |
| Contents pane | Displays file and inventory information for the element selected on the Navigation pane. For more information, see Contents pane on page 243. |

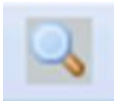
### Navigation



## Tool bar commands

The following table describes the File Inventory Manager tool bar commands.

**Table 51: Tool bar commands**

| Command | Toolbar Button | Description |
|---|---|---|
| Discover |  | Rediscovers the inventory information and reloads File Inventory Manager with the latest information. |
| Set Preferences |  | Filters devices based on Family or Capabilities. |
| Find |  | Finds matching text strings in the navigation or contents panes. |
| Highlight Topology |  | Highlights devices of the selected family on the Configuration and Orchestration Manager topology map. |
| Help |  | Opens online Help for the current folder or tab. |
| Export |  | Exports inventory information displayed in content panel grid in to a text file. |

## Menu bar commands

The following table describes the File Inventory Manager menu bar commands.

**Table 52: Menu bar commands**

| Command | Description |
|---|---|
| Save Inventory information | Allows you to save inventory files that you can load again later. |
| Open Inventory file | Allows you to load saved inventory files. |
| Save Inventory in Tab delimited text file | Allows you to save network inventory information in a tab-delimited text file. |
| Set View Preferences | Allows you to select the information to be displayed. |
| Download file to device | Allows you to download configuration or image files or both to devices. |
| Upload file from device | Allows you to upload configuration or image files or both from devices. |
| Backup Config | Allows you to create backup files that can be restored to devices in the event of a network failure. |
| Restore Config | Allows you to restore the configuration for the target device(s). |
| Archive Config | Allows you to archive the configuration for the target device(s). |
| Synchronize Config | Allows you to synchronize the configuration for the target device(s). |
| Upgrade device | Allows you to update the software for the specified device(s). |
| Upgrade device wizard | Displays the Auto Upgrade form. |
| Edit File | Allows you to edit configuration files with a text editor. |
| Compare Config | Compares the runtime configuration for the specified device(s) with the external configuration file. |

## Navigation pane

The File Inventory Manager Navigation pane allows you to navigate File/Inventory elements for devices discovered on the network. Devices are grouped in folders according to the device family. They are identified by their IP address.

Double-click the folder to view its elements, and then click an element to examine detailed information in the Contents panel.

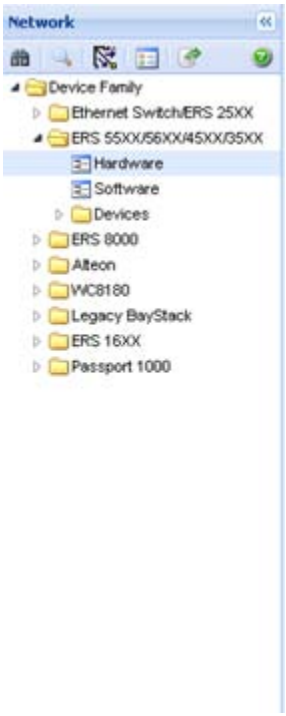



**Figure 27: Parts of the File/Inventory Navigation pane**

The following table describes the Navigation pane.

**Table 53: Parts of Navigation pane**

| Part | Description |
|---|---|
| Device Family folder | Specifies the root folder; contains all of the icons and folders in the Tree Panel. |
| ERS 8000, VSP 9XXX folder | Displays the information specific to ERS 8xxx devices, and VSP 9xxx devices. |
| ERS 55XX/45XX/35XX folder | Displays the information specific to ERS 55xx, 45xx, and 35xx devices. |
| Legacy ERS 1424/16xx | Displays the information specific to ERS 1424 and 16xx devices. |
| ERS 55xx/35xx/45xx/25xx folder | Displays the information specific to ERS 55xx, 35xx, 45xx and 25xx devices. |
| Legacy BayStack | Displays the information specific to legacy baystack. |
| Alteon | Displays the information specific to Alteon devices. |
| OM 1000 | Displays the information specific to OM 1000 devices. |
| WLAN AP devices | Displays the information specific to WLAN AP devices. |
| Hardware | Displays all hardware information for the discovered devices. |

| Part | Description |
|---|---|
| Software | Displays all software information for the discovered devices. |
| Devices | Displays hardware and software information for the selected device. |

## Contents pane

The contents pane displays file and inventory information for the element selected on the Navigation pane. The information is provided in tabular format. Each tab at the top of the contents pane is a table. Click the tab to view the table contents. Use the horizontal scroll bar at the bottom of the contents pane when a table is wider than the contents pane.

## Understanding the File Inventory navigation tree

The following figure shows the File Inventory Manager navigation tree. Depending on the devices that were discovered, your File Inventory Manager window may show folders that are not listed here, and may not show folders that are listed.

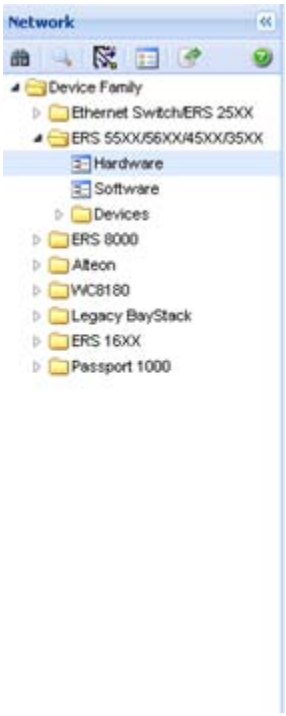



**Figure 28: Understanding the File Inventory Manager navigation tree**

The following sections describe the tab contents of Device Family folders:

- ERS 55xx/45xx/35xx folder on page 244
- ERS 8000, VSP 9XXX folder on page 251

## ERS 55xx/45xx/35xx folder

Use the ERS 55xx/45xx/35xx folder to view information about Ethernet Routing Switch 5510, 5520, 5530, 4548GT, 4548GT_PWR, 4550T, 4550T_PWR, 4526FX, and 3510 hardware, software, and devices in the network inventory.

The following table describes the parts of the ERS 55xx/45xx/35xx folder.

**Table 54: Parts of the ERS 55xx/45xx/35xx folder**

| Part | Description |
|---|---|
| ERS 55xx/45xx/35xx Hardware table on page 245 | Shows information about Ethernet Routing Switch 55xx, 45xx, and 35xx device hardware in the network inventory. |
| ERS 55xx/45xx/35xx Software table on page 247 | Shows information about software running on Ethernet Routing Switch 55xx, 45xx, and 35xx devices in the network inventory. |

| Part | Description |
|---|---|
| ERS 55xx/45xx/35xx Devices folder on page 248 | Shows information about each of the Ethernet Routing Switch 55xx, 45xx, and 35xx devices discovered on the network. |

## ERS 55xx/45xx/35xx Hardware table

Use the ERS 55xx/45xx/35xx Hardware table to view information about Ethernet Routing Switch 55xx. 45xx, and 35xx device hardware in the network inventory.

The following table describes the parts of the ERS 55xx/45xx/35xx Hardware table.

**Table 55: Parts of the ERS 55xx/45xx/35xx Hardware table**

| Part | Description |
|---|---|
| Stack tab on page 245 | Shows information about Ethernet Routing Switch 55xx, 45xx, and 35xx stack. |
| Gbic tab on page 246 | Shows information about the system that Ethernet Routing Switch 55xx, 45xx, and 35xx use to determine the device capabilities. |

## Stack tab

Use the Stack of the ERS 55xx/45xx/35xx folder to view information about Ethernet Routing Switch 55xx, 45xx, and 35xx stack.


The following table describes the parts of the Stack tab.

**Table 56: Parts of the stack tab of the ERS 55xx/45xx/35xx Hardware table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |
| Indx | Shows the index number of the device. |

| Part | Description |
|---|---|
| Descr | Shows the description for the device |
| Ver | Shows the version number of the device. |
| SerNum | Shows the serial number of the device. |
| Location | Show the location of the device. |

## Gbic tab

Use the Gbic tab of the ERS 55xx/45xx/35xx folder to view information about the system that Ethernet Routing Switch 55xx, 45xx, and 35xx use to determine the device capabilities.

The following table describes the parts of the Gbic tab

**Table 57: Parts of the Gbic tab of the ERS 55xx/45xx/35xx Hardware table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |
| Port Number | Shows the port number of the device. |
| GBIC Type | Shows the gbic type. It follows the port number. |
| Vendor Name | Shows the gbic vendor name. |
| Vendor OUI | Shows the company ID of the gbic vendor IEEE. |
| Vendor Part # | Shows the part number provided by gbic vendor. |
| Vendor Revision | Shows the revision level for part number provided by vendor. |
| Vendor Serial | Shows the serial number provided by the vendor. |
| HW Options | Shows the hardware options for the gbic. |
| Date Code | Shows the manufacturing date code of the vendor. |
| Vendor Data | Shows the vendor specific data for gbic. |

## Chassis tab

Use the Chassis tab of the ERS 55xx/45xx/35xx folder to view information about Ethernet Routing Switch 55xx, 45xx, and 35xx chassis.

The following table describes the parts of the Chassis tab.

**Table 58: Parts of the Chassis tab of the ERS 55xx/45xx/35xx Hardware table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |

| Part | Description |
|---|---|
| ModuleType | Shows the Ethernet Routing Switch module type. |
| HwRevision | Shows the current hardware revision of the device chassis. |
| DeviceSerial Number | Shows the serial number of the device. |

## ERS 55xx/45xx/35xx Software table

Use the ERS 55xx/45xx/35xx Software table to view information about software running on Ethernet Routing Switch 55xx, 45xx, and 35xx devices in the network inventory.

The following table describes the parts of the ERS 55xx/45xx/35xx Software table.

**Table 59: Parts of the ERS 55xx/45xx/35xx Software table**

| Part | Description |
|---|---|
| General tab on page 247 | Shows general information about software running on Ethernet Routing Switch (legacy) 55xx, 45xx, and 35xx devices in the network inventory. |
| Image Config tab on page 248 | Shows information about software configuration settings. |

## General tab

Use the General tab of the ERS 55xx/45xx/35xx Software table on page 247to view general information about the software running on Ethernet Routing Switch 55xx, 45xx, and 35xx devices.

The following table describes the parts of the General tab.

**Table 60: Parts of the General tab of the ERS 55xx/45xx/35xx Software table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name of the device. |
| Type | Shows the type of the device. |
| SysName | Shows the system name of the device. |
| Description | Shows a description of the device. |
| Location | Shows the location of the device. |
| Contact | Shows the administrative contact for the device. |
| UpTime | Shows the elapsed time since the last restart of the device. |

### Image Config tab

Use the Image/Config tab of the ERS 55xx/45xx/35xx Software table on page 247 to view information about image and configuration files loaded on the Ethernet Routing Switch 55xx, 45xx, and 35xx devices.

The following table describes the parts of the Image/Config tab.

**Table 61: Parts of the Image/Config tab of the ERS 55xx/45xx/35xx software table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name of the device. |
| ImgFname | Shows the filename of the last image file downloaded to the device. |
| CfgFname | Shows the filename of the last configuration file downloaded to or uploaded from the device. |

## ERS 55xx/45xx/35xx Devices folder

Use the ERS 55xx/45xx/35xx Devices folder to view information about each of the Ethernet Routing Switch 55xx, 45xx, and 35xx devices discovered on the network.

For each device in the Devices folder, File Inventory Manager displays the following tabs in the contents pane

**Table 62: Parts of the ERS 55xx/45xx/35xx Devices folder**

| Part | Description |
|---|---|
| Stack tab on page 249 | Shows information about Ethernet Routing Switch 55xx, 45xx, and 35xx stack. |
| Gbic tab on page 249 | Shows information about the system that Ethernet Routing Switch 55xx, 45xx, and 35xx use to determine the device capabilities. |
| General tab on page 250 | Shows general information about software running on Ethernet Routing Switch 55xx, 45xx, and 35xx devices in the network inventory. |
| Image Config tab on page 250 | Shows information about software configuration settings. |

**Important:**

The contents pane displays the tabs described in the previous table, only when you select a device from the device folder.

### Chassis tab

Use the Chassis tab of the ERS 55xx/45xx/35xx Devices folder on page 248 to view information about Ethernet Routing Switch 55xx, 45xx, and 35xx chassis.

The following table describes the parts of the Chassis tab.

**Table 63: Parts of the Chassis tab of the ERS 55xx/45xx/35xx Devices folder**

| Part | Description |
|---|---|
| ModuleType | Specifies the Ethernet Routing Switch module type. |
| HwRevision | Specifies the current hardware revision of the device chassis. |
| DeviceSerialNumber | Specifies the serial number for the device. |

## Stack tab

Use the Stack tab of the ERS 55xx/45xx/35xx Devices folder on page 248 to view information about Ethernet Routing Switch 55xx, 45xx, and 35xx Stack.

The following table describes the parts of the Stack tab.

**Table 64: Parts of the stack tab of the ERS 55xx/45xx/35xx Devices folder**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |
| Indx | Shows the index number of the device. |
| Descr | Shows the description for the device |
| Ver | Shows the version number of the device. |
| SerNum | Shows the serial number of the device. |
| Location | Show the location of the device. |

## Gbic tab

Use the Gbic tab of the ERS 55xx/45xx/35xx Devices folder on page 248 to view information about the system that Ethernet Routing Switch 55xx, 45xx, and 35xx use to determine the device capabilities.

The following table describes the parts of the Gbic tab.

**Table 65: Parts of the Gbic tab of the ERS 55xx/45xx/35xx Devices folder**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |
| Port Number | Shows the port number of the device. |
| GBIC Type | Shows the gbic type. It follows the port number. |
| Vendor Name | Shows the gbic vendor name. |

| Part | Description |
|---|---|
| Vendor OUI | Shows the company ID of the gbic vendor IEEE. |
| Vendor Part # | Shows the part number provided by gbic vendor. |
| Vendor Revision | Shows the revision level for part number provided by vendor. |
| Vendor Serial | Shows the serial number provided by the vendor. |
| HW Options | Shows the hardware options for the gbic. |
| Date Code | Shows the manufacturing date code of the vendor. |
| Vendor Data | Shows the vendor specific data for gbic. |

## General tab

Use the General tab of the ERS 55xx/45xx/35xx Devices folder on page 248 to view general information about the selected Ethernet Routing Switch 55xx, 45xx, and 35xx device.

The following table describes the parts of the General tab.

**Table 66: Parts of the General tab of the Devices folder**

| Part | Description |
|---|---|
| Type | Shows the type of the device. |
| SysName | Shows the system name of the device. |
| Description | Shows a description of the device. |
| Location | Shows the location of the device. |
| Contact | Shows the administrative contact for the device. |
| UpTime | Shows the elapsed time since the last restart of the device. |

## Image Config tab

Use the Image/Config tab of the ERS 55xx/45xx/35xx Devices folder on page 248to view information about image and configuration files loaded on the device.

The following table describes the parts of the Image/Config tab.

**Table 67: Parts of the Image/Config tab of the ERS 55xx/45xx/35xx Devices folder**

| Part | Description |
|---|---|
| PromFWVersion | Shows the version number of the agent PROM firmware. |
| RuntimeSW Version | Shows the version number of the runtime software. |
| FirmwareFile | Shows the filename of the last image or firmware file downloaded to the device. |
| ConfigFName | Shows the filename of the last configuration file downloaded to or uploaded from the device. |

# ERS 8000, VSP 9XXX folder

Use the ERS 8000, VSP 9XXX folder to view information about Ethernet Routing Switch 8000 and Virtual Services Platform (VSP) 9XXX hardware, software, and devices in the network inventory.

The following table describes the parts of the ERS 8000, VSP 9XXX folder.

**Table 68: Parts of the ERS 8000, VSP 9XXX folder**

| Part | Description |
|---|---|
| ERS 8000, VSP 9XXX Hardware table on page 251 | Shows information about Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX device hardware in the network inventory. |
| ERS 8000, VSP 9XXX Software table on page 255 | Shows information about software running on Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX devices in the network inventory. |
| ERS 8000, VSP 9XXX Devices folder on page 259 | Shows information about each of the Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX devices discovered on the network. |

## ERS 8000, VSP 9XXX Hardware table

Use the ERS 8000, VSP 9XXX Hardware table to view information about Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX device hardware in the network inventory.


The following table describes the parts of the ERS 8000, VSP 9XXX Hardware table.

**Table 69: Parts of the ERS 8000, VSP 9XXX Hardware table**

| Part | Description |
|---|---|
| Chassis tab on page 252 | Shows information about Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family chassis. |
| Card tab on page 252 | Shows information about cards installed in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family chassis. |

| Part | Description |
|---|---|
| Mda tab on page 254 | Shows information about MDAs installed in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family chassis. |
| Gbic tab on page 254 | Shows information about the system that Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family use to determine the device capabilities. |
| IP Phone on page 255 | Shows information about IP Phone installed in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family chassis. |

## Chassis tab

Use the Chassis tab of the ERS 8000, VSP 9XXX Hardware table on page 251 to view information about Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family chassis.

The following table describes the parts of the Chassis tab.

**Table 70: Parts of the Chassis tab of the ERS 8000, VSP 9XXX Hardware table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |
| Type | Shows the module type. |
| SerialNumber | Shows the serial number for the device. |
| Hardware Revision | Shows the current hardware revision of the device chassis. |
| NumSlots | Shows the number of slots (or cards) this device can contain. |
| NumPorts | Shows the number of ports currently on this device. |
| BaseMacAddr | Shows the starting point of the block of MAC addresses used by the switch for logical and physical interfaces. |
| HaCpu | Shows you the L2 redundancy on the master CPU is enabled or disabled. |
| StandbyCpu | Shows you whether the L2 Redundancy is enabled on the standby CPU. The possible states are<br>• hotStandbyCPU<br>• warmStandbyCPU<br>• standbyCPUNotPresent |

## Card tab

Use the Card tab of the ERS 8000, VSP 9XXX Hardware table on page 251to view information about cards installed in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX series chassis.

The following table describes the parts of the Card tab.

**Table 71: Parts of the Card tab of the ERS 8000, VSP 9XXX Hardware table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name of the device. |
| SlotNum | Shows the slot numbers of cards installed in the chassis. |
| FrontType | Indicates the card types in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX Series devices. Front refers to the I/O portion of the module, the I/O card. |
| FrontDescription | Shows the model number of the module (for example, 8608GT). |
| FrontSerialNum | Shows the serial number of the I/O card. |
| FrontHwVersion | Shows the hardware version of the I/O card. |
| FrontPartNumber | Shows the part number of the I/O card. |
| FrontDateCode | Shows the manufacturing date code for the I/O card. |
| FrontDeviations | Shows front deviations for the card. |
| BackType | Shows the back type of the card. Possible values are<br>• rc2kBackplane<br>• rc2kSFM<br>• rc2kBFM0<br>• rc2kBFM2<br>• rc2kBFM3<br>• rc2kBFM6<br>• rc2kBFM8<br>• rc2kMGSFM<br>• other |
| BackDescription | Shows the back description for the card. |
| BackSerialNum | Shows the back serial number for the card. |
| BackHwVersion | Shows the back hardware version for the card. |
| BackPartNumber | Shows the back part number for the card. |
| BackDateCode | Shows the back date code for the card. |
| BackDeviations | Shows the back deviations for the card. |

### Mda tab

Use the Mda tab of the ERS 8000, VSP 9XXX Hardware table on page 251 to view information about MDA installed in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices in the network inventory.

The following table describes the parts of the Mda tab.

**Table 72: Parts of the Mda tab of the ERS 8000, VSP 9XXX Hardware table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name of the device in which the MDA is installed. |
| SlotNum | Shows the identity of the slot in which the MDA is installed. |
| MdaNum | Shows the number of the MDA. |
| Type | Shows the type of the MDA. |
| Description | Shows the MDA description. Possible values include<br>• OC-3c SMF MDA—Dual port OC-3c SMF<br>• OC-3c MMF MDA—Dual port OC-3c MMF<br>• OC-12c SMF MDA—Single Port OC-12c SMF<br>• OC-12c MMF MDA—Single Port OC-12c MMF |
| NumPorts | Shows the number of ports on the MDA. |

### Gbic tab

Use the Gbic tab of the ERS 8000, VSP 9XXX Hardware table on page 251 to view information about the system that Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family use to determine the device capabilities.

The following table describes the parts of the Gbic tab.

**Table 73: Parts of the Gbic tab of the ERS 8000, VSP 9XXX Hardware table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |
| Slot/Port | Shows the slot number and the port number of Gbic in the device. |
| Type | Shows the gbic type. It follows the port number. |
| Vendor | Shows the gbic vendor name. |
| Part | Shows the part number provided by gbic vendor. |

## IP Phone

Use the IP Phone tab of the ERS 8000, VSP 9XXX Hardware table on page 251 to view information about the IP Phone that are installed on the Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family.

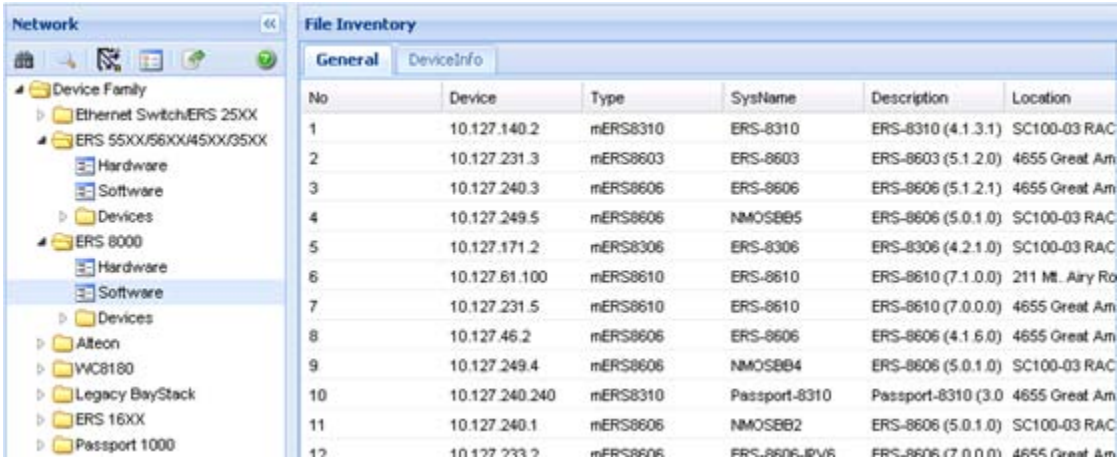
The following table describes the parts of the IP Phone tab.

**Table 74: Parts of the IP Phone tab of the ERS 8000, VSP 9XXX Hardware table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |
| TimeMark | Shows the time. |
| PortNum | Shows the port number. |
| Index | Shows the port index. |
| Type | Shows the port type. |
| ConnectedIPPhone | Shows the IP phone connected to the device. |
| SysName | Shows the system name. |
| Description | Shows the description. |

## ERS 8000, VSP 9XXX Software table

Use the ERS 8000, VSP 9XXX Software table to view information about software running on Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX devices in the network inventory.




The following table describes the parts of the ERS 8000, VSP 9XXX Software table.

**Table 75: Parts of the ERS 8000, VSP 9XXX Software table**

| Part | Description |
|---|---|
| General tab on page 256 | Shows general information about software running on Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices in the network inventory. |
| Device Info tab on page 256 | Shows information about the device. |
| Software tab on page 257 | Shows information about software versions and sources. |
| Configuration tab on page 257 | Shows information about software configuration settings. |
| WSM Image tab on page 258 | Shows information about WSM images. |

## General tab

Use the General tab of the ERS 8000, VSP 9XXX Software table on page 255 to view general information about software running on Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices on the network.

The following table describes the parts of the General tab.

**Table 76: Parts of the General tab of the ERS 8000, VSP 9XXX Software table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name of the device. |
| Type | Shows the type of the device. |
| SysName | Shows the system name of the device. |
| Description | Shows a description of the device. |
| Location | Shows the location of the device. |
| Contact | Shows the administrative contact for the device. |

## Device Info tab

Use the Device Info tab of the ERS 8000, VSP 9XXX Software table on page 255 to view information about the device in the Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family chassis.

The following table describes the parts of the device info tab.

**Table 77: Parts of the Device Info tab of the ERS 8000, VSP 9XXX Software table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |
| Slot | Shows the slot number for the pcmcia card in the device. |
| FlashBytesUsed | Shows the number of bytes used in the system configuration flash device. |
| Flash BytesFree | Shows the number of bytes available in the system configuration flash device. |
| Flash NumFiles | Shows the number of files available in the system configuration flash device. |
| Pcmcia BytesUsed | Shows the number of bytes used by pcmcia device in the system. |
| Pcmcia BytesFree | Shows the number of bytes available in the system pcmcia device. |
| Pcmcia NumFiles | Shows the number of files available in the system pcmcia device. |

## Software tab

Use the Software tab of the ERS 8000, VSP 9XXX Software table on page 255 to view information about the software running on cards installed in the Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family chassis. The table on the tab has one row for each CPU card in the chassis.

The following table describes the parts of the Software tab.

**Table 78: Parts of the Software tab of the ERS 8000, VSP 9XXX Software table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name of the device. |
| Slot | Shows the slot number of the card on which the software is running. |
| SwVersion | Shows the version number of the software. |
| LastRuntime ImageSource | Shows the name of the file from which the runtime image was loaded. |
| PrimaryImage Source | Shows the name of the file from which the primary image was loaded. |

## Configuration tab

Use the Configuration tab of the ERS 8000, VSP 9XXX Software table on page 255 to view information about configuration files loaded on the device. The table on the tab has one row for each CPU card in the chassis.

The following table describes the parts of the Configuration tab.

**Table 79: Parts of the Configuration tab of the ERS 8000, VSP 9XXX Software table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name of the device. |
| Slot | Shows the slot number of the card on which the software is running. |
| LastBootConfig Source | Shows the name and location of the file from which the last boot configuration was loaded. |
| LastRuntime ConfigSource | Shows the name and location of the file from which the last runtime configuration was loaded. |
| PrimaryConfig Source | Shows the name and location of the file from which the last primary configuration was loaded. |

## WSM Image tab

Use the WSM Image tab of the ERS 8000, VSP 9XXX Software table on page 255 to view information about WSM image software running on Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices.

The following table describes the parts of the WSM Image tab.

**Table 80: Parts of the WSM Image tab of the ERS 8000, VSP 9XXX Software table**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name of the device. |
| Software Version | Shows the software version of the WSM image. |
| Enabled SwFeatures | Shows the enabled features of the WSM image. |
| BootVer | Shows the boot version of the WSM image. |
| Image1Ver | Shows the version number of WSM image 1. |
| Image2Ver | Shows the version number of WSM image 2. |
| ImageForNxt Reset | Shows the image file that loads the next time the WSM card resets. |
| ConfigForNxt Reset | Shows the configuration file that loads the next time the WSM card resets. |
| SavePending | Indicates that a save action is required because the configuration has been applied but has not been saved to the flash. |

## ERS 8000, VSP 9XXX Devices folder

Use the ERS 8000, VSP 9XXX Devices folder to view information about each of the Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX devices discovered on the network.

The following table describes the parts of the ERS 8000, VSP 9XXX Devices folder.

**Table 81: Parts of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| Chassis tab on page 259 | Shows information about Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family chassis. |
| Card tab on page 260 | Shows information about cards installed in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX series chassis. |
| Mda tab on page 261 | Shows information about MDA installed in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices in the network inventory. |
| General tab on page 262 | Shows general information about software running on Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices in the network inventory. |
| Software tab on page 262 | Shows information about software versions and sources. |
| Configuration tab on page 262 | Shows information about software configuration settings. |
| WSM Image tab on page 263 | Shows information about WSM images. |
| FlashFiles tab on page 263 | Shows information about the files in the flash memory of Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices. |
| DeviceInfo tab on page 264 | Shows information about the device. |
| Gbic tab on page 264 | Shows information about the system that Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family use to determine the device capabilities. |
| PcmciaFiles tab on page 265 | Shows information about the PcmciaFiles. |

## Chassis tab

Use the Chassis tab of the ERS 8000, VSP 9XXX Devices folder on page 259 to view information about the Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX device chassis. The following table describes the parts of the Chassis tab.

**Table 82: Parts of the Chassis tab of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| Type | Shows the module type. |
| SerialNumber | Shows the serial number for the device. |
| Hardware Revision | Shows the current hardware revision of the device chassis. |
| NumSlots | Shows the number of slots (or cards) this device can contain. |
| NumPorts | Shows the number of ports currently on this device. |
| BaseMacAddr | Shows the starting point of the block of MAC addresses used by the switch for logical and physical interfaces. |
| HaCpu | Shows you whether the L2 redundancy on the master CPU is enabled or disabled. |
| StandbyCpu | Shows you whether the L2 Redundancy is enabled on the standby CPU. The possible states are<br>• hotStandbyCPU<br>• warmStandbyCPU<br>• standbyCPUNotPresent |

## Card tab

Use the Card tab of the ERS 8000, VSP 9XXX Devices folder on page 259 to view information about cards installed in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX series chassis.

The following table describes the parts of the Card tab.

**Table 83: Parts of the Card tab of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| SlotNum | Shows the slot numbers of cards installed in the chassis. |
| FrontType | Indicates the card types in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX Series devices. Front refers to the I/O portion of the module, the I/O card. |
| FrontDescription | Shows the model number of the module (for example, 8608GT). |
| FrontSerialNum | Shows the serial number of the I/O card. |
| FrontHwVersion | Shows the hardware version of the I/O card. |
| FrontPartNumber | Shows the part number of the I/O card. |
| FrontDateCode | Shows the manufacturing date code for the I/O card. |
| FrontDeviations | Shows front deviations for the card. |
| BackType | Shows the back type of the card. Possible values are |

| Part | Description |
|---|---|
| | • rc2kBackplane<br>• rc2kSFM<br>• rc2kBFM0<br>• rc2kBFM2<br>• rc2kBFM3<br>• rc2kBFM6<br>• rc2kBFM8<br>• rc2kMGSFM<br>• other |
| BackDescription | Shows the back description for the card. |
| BackSerialNum | Shows the back serial number for the card. |
| BackHwVersion | Shows the back hardware version for the card. |
| BackPartNumber | Shows the back part number for the card. |
| BackDateCode | Shows the back date code for the card. |
| BackDeviations | Shows the back deviations for the card. |

## Mda tab

Use the Mda tab of the ERS 8000, VSP 9XXX Devices folder on page 259 to view information about MDA installed in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices in the network inventory.

The following table describes the parts of the Mda tab.

**Table 84: Parts of the Mda tab of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| SlotNum | Shows the identity of the slot in which the MDA is installed. |
| MdaNum | Shows the number of the MDA. |
| Type | Shows the type of the MDA. |
| Description | Shows the MDA description. Possible values include<br>• OC-3c SMF MDA—Dual port OC-3c SMF<br>• OC-3c MMF MDA—Dual port OC-3c MMF<br>• OC-12c SMF MDA—Single Port OC-12c SMF<br>• OC-12c MMF MDA—Single Port OC-12c MMF |
| NumPorts | Shows the number of ports on the MDA. |

### General tab

Use the General tab of the ERS 8000, VSP 9XXX Devices folder on page 259 to view general information about software running on Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices on the network.

The following table describes the parts of the General tab.

**Table 85: Parts of the General tab of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| Type | Shows the type of the device. |
| SysName | Shows the system name of the device. |
| Device | Shows the device. |
| Description | Shows a description of the device. |
| Location | Shows the location of the device. |
| Contact | Shows the administrative contact for the device. |

### Software tab

Use the Software tab of the ERS 8000, VSP 9XXX Devices folder on page 259 to view information about software running on cards installed in Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family chassis. The table on the tab will have one row for each CPU card in the chassis.

The following table describes the parts of the Software tab.

**Table 86: Parts of the Software tab of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| Slot | Shows the slot number of the card on which the software is running. |
| SwVersion | Shows the version number of the software. |
| LastRuntime ImageSource | Shows the name of the file from which the runtime image was loaded. |
| PrimaryImage Source | Shows the name of the file from which the primary image was loaded. |

### Configuration tab

Use the Configuration tab of the ERS 8000, VSP 9XXX Devices folder on page 259 to view information about configuration files loaded on the device. The table on the tab will have one row for each CPU card in the chassis.

The following table describes the parts of the Configuration tab.

**Table 87: Parts of the Configuration tab of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| Slot | Shows the slot number of the card on which the software is running. |
| LastBootConfig Source | Shows the name and location of the file from which the last boot configuration was loaded. |
| LastRuntime ConfigSource | Shows the name and location of the file from which the last runtime configuration was loaded. |
| PrimaryConfig Source | Shows the name and location of the file from which the last primary configuration was loaded. |

## WSM Image tab

Use the WSM Image tab of the ERS 8000, VSP 9XXX Devices folder on page 259 to view information about WSM image software running on Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices.

The following table describes the parts of the WSM Image tab.

**Table 88: Parts of the WSM Image tab of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name of the device. |
| Software Version | Shows the software version of the WSM image. |
| Enabled SwFeatures | Shows the enabled features of the WSM image. |
| BootVer | Shows the boot version of the WSM image. |
| Image1Ver | Shows the version number of WSM image 1. |
| Image2Ver | Shows the version number of WSM image 2. |
| ImageForNxt Reset | Shows the image file that will be loaded the next time the WSM card resets. |
| ConfigForNxt Reset | Shows the configuration file that will be loaded the next time the WSM card resets. |
| SavePending | Indicates that a save action is required because the configuration has been applied but has not been saved to the flash. |

## FlashFiles tab

Use the Flash Files tab of the ERS 8000, VSP 9XXX Devices folder on page 259 to view information about the files in the flash memory of the selected Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX device.

The following table describes the parts of the Flash Files tab.

**Table 89: Parts of the Flash Files tab of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name of the device. |
| Slot | Displays slot number of the card that contains the Flash files. |
| Name | Displays the name of the file |
| Date | Displays the date the file was written to the flash memory |
| Size | Displays the file size in bytes |

## DeviceInfo tab

Use the Device Info tab of the ERS 8000, VSP 9XXX Devices folder on page 259 to view information about the device selected Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX device.

The following table describes the parts of the DeviceInfo tab.

**Table 90: Parts of the DeviceInfo tab of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |
| Slot | Shows the slot number for the pcmcia card in the device. |
| FlashBytes Used | Shows the number of bytes used in the system configuration flash device. |
| FlashBytes Free | Shows the number of bytes available in the system configuration flash device. |
| FlashNum Files | Shows the number of files available in the system configuration flash device. |
| Pcmcia BytesUsed | Shows the number of bytes used by pcmcia device in the system. |
| PcmciaBytes Free | Shows the number of bytes available in the system pcmcia device. |
| PcmciaNum Files | Shows the number of files available in the system pcmcia device. |

## Gbic tab

Use the Gbic tab of the ERS 8000, VSP 9XXX Devices folder on page 259 to view information about the system that Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family use to determine the device capabilities.

The following table describes the parts of the Gbic tab.

**Table 91: Parts of the Gbic tab of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |
| Slot/Port | Shows the slot number and the port number of gbic in the device. |
| Type | Shows the gbic type. It follows the port number. |
| Vendor | Shows the gbic vendor name. |
| Part | Shows the part number provided by gbic vendor. |

### PcmciaFiles tab

Use the PmciaFiles tab of the ERS 8000, VSP 9XXX Devices folder on page 259 to view pcmcia file information of the selected Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX device.

The following table describes the parts of the PcmciaFiles tab.

**Table 92: Parts of the PcmciaFiles tab of the ERS 8000, VSP 9XXX Devices folder**

| Part | Description |
|---|---|
| No. | Shows the row number of the table entry. |
| Device | Shows the IP address or host name for the device. |
| Slot | Shows the slot number for the pcmcia card in the device. |
| Name | Shows the name of the files in pcmcia card. |
| Date | Shows the file creation date. |
| Size | Shows the size of the file. |

# Setting File Inventory Manager preferences

You can set preferences for displaying and managing devices on the File Inventory Manager. This section contains information about setting the following preferences:

Setting device management preferences on page 265

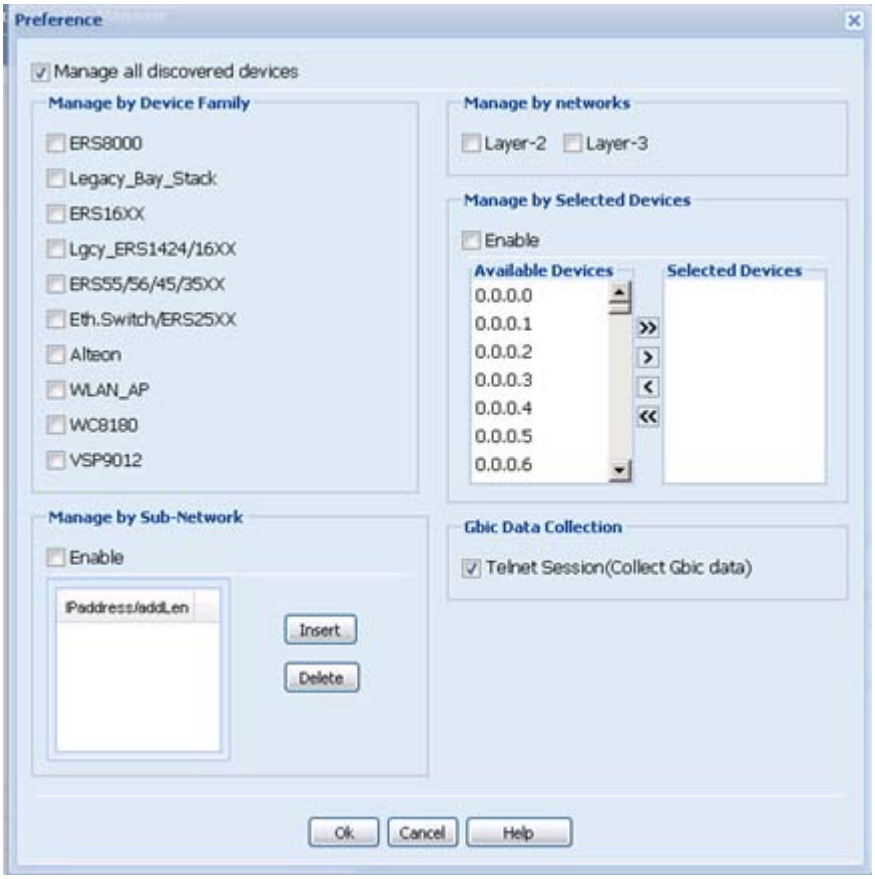
## Setting device management preferences

Perform the following procedure to set the preferences for managing devices using the File Inventory Manager.

### Procedure steps

1. Open the File Inventory Manager.
2. Select **Preferences** tab from the menu bar.

   The Preference dialog box appears.




3. Select or clear the check boxes to enable or disable the associated filters for managing devices. The available options are:

   - **Manage by device family**—allows you to choose the supported device families: ERS 8000, ERS 16XX, Ethernet Switch/ERS 25XX, Alteon, Legacy BayStack, Legacy ERS 1424/16XX, ERS 55XX/45XX/35XX, WLAN AP, WC 8180, VSP 9012, and IP Phone.
   - **Manage by sub-network**—allows you to insert or delete subnetworks. If you select this option, only the assigned devices in the selected subnetworks are used in the next discovery process.
   - **Manage by network layers**—allows you to manage devices based on the network layers: Layer 2 or Layer 3.
   - **Manage by selected devices**—allows you to manage a particular group of devices; you can select devices from the Available Devices. If you select this

option, The File inventory manager uses only the selected devices in the next discovery process.

- **GBIC Data Collection**—allows you to collect the GBIC data.

4. Click **OK** to add the changes.

# Managing files

The following sections describe how to use File Inventory Manager:



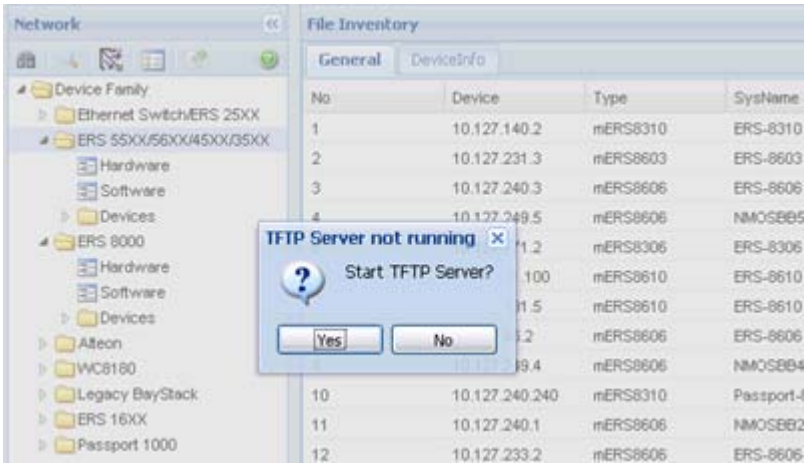
## Downloading a file to the device

Perform the following procedure to download configuration files and image files to devices.

### Procedure steps

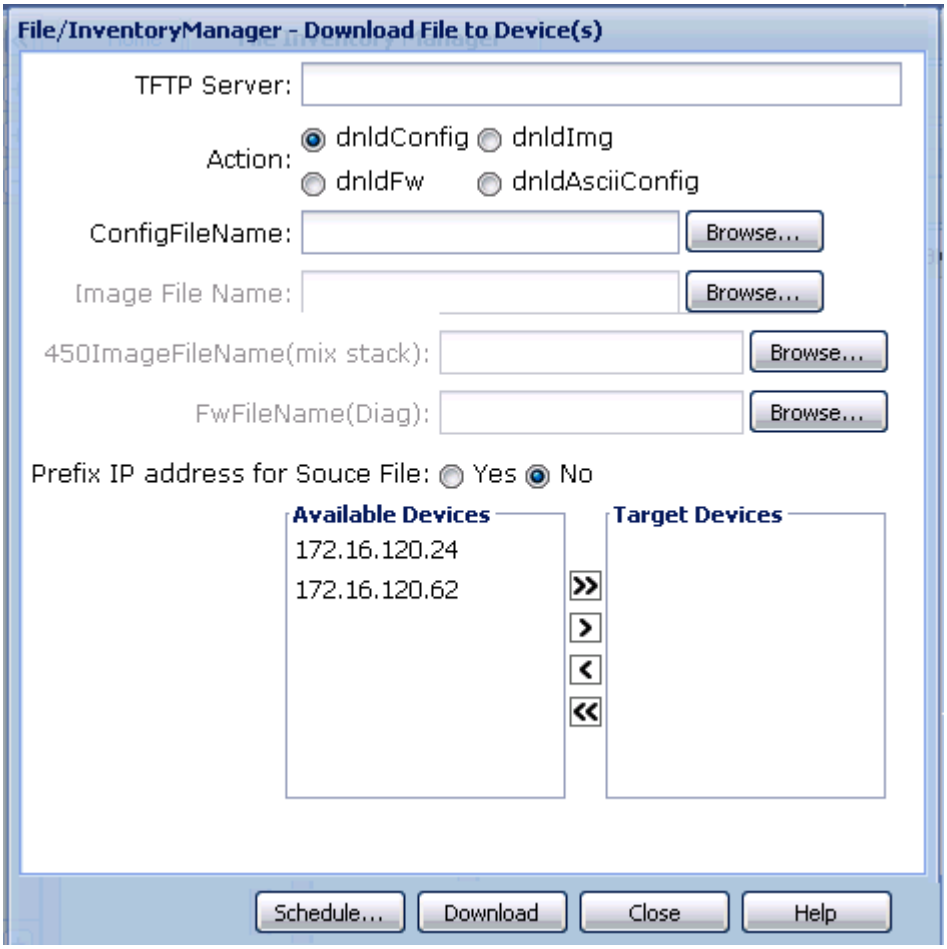
1. Open **File Inventory manager**.
2. Select **Action**, **Download File to Device(s)** from the menu bar.

   The TFTP Server Not Running dialog box appears.




3. Click **Yes** to start TFTP server.

   The File/Inventory Manager - Download File to Device(s) dialog box appears.




4. In the **TFTP Server** field, enter the host name or IP address of the TFTP server for the download operation.

5. In the **ConfigFileName** field, enter the name of the base file you are downloading.
6. In the **Image File Name**, **450ImageFileName(mix stack)**, and **FwdFileName(Diag)** fields, enter the appropriate file names.
7. Use the **Prefix IP address for Source File** option to set how the filename is interpreted:
   - When you choose **No**, File Inventory Manager downloads the file with the selected filename.
   - When you choose **Yes**, File Inventory Manager downloads files to the selected device according to the IP address appended to the filename. For example, suppose the file name is config.cfg , and the selected device is 10.160.41.204, then the File Inventory Manager downloads the file 10_160_41_204_config.cfg to the device. The source directory for the download operation is determined by the settings of the TFTP server. Review the configuration settings of the TFTP server to determine the source directory.
8. In the **Available Devices** list, select one or more devices to which you want to download the selected file.
9. Click **>** to move the selected device(s) to the **Target Devices** list. **OR** Click **>>** to move all the available devices to the **Target Devices** list. Click **<** or **<<** to move devices back to the **Available Devices** list.
10. Click **Download** to download the file.
11. A message that shows the results of the operation appears at the bottom of the dialog box.

**Table 93: Parts of the Download File to Device(s) dialog box**

| Part | Description |
|---|---|
| TFTP Server | Allows you to enter the IP address of the TFTP server for the operation. The default setting is the TFTP server (if any) specified on the Preferences dialog box. |
| Source File Name | Allows you to choose a file to download to Ethernet Routing Switch 8000 devices. You can use the **Browse** button to browse the file. The source directory for the download operation is determined by the settings of the TFTP server. Review the configuration settings of the TFTP server to determine the source directory. |
| Destination File Name | Allows you to enter a destination filename for a Ethernet Routing Switch 8000 download operation. |
| Prefix IP address for Source File | Use the Prefix IP address for Source File options to set whether or not you are downloading files according to the IP address appended to the filename: |

| Part | Description |
|---|---|
| | • When you choose No, File Inventory Manager downloads the selected file to all selected devices.<br>• When you choose Yes, File Inventory Manager downloads files to the selected devices according to the IP address appended to filename.<br>For example, suppose the file name is config.cfg and the selected the device is 10.160.41.204. File Inventory Manager will download the file 10_160_41_204_config.cfg to 10.160.41.204.<br>The source directory for the download operation is determined by the settings of the TFTP server. Review the configuration settings of the TFTP server to determine the source directory. |
| Available Devices list | Allows you to choose from all the available devices. |
| Target Devices list | Allows you to arrange multiple devices in the order in which you want to download the file. |
| >> | Allows you to move all the devices from the Available Devices list into the Target Devices list. |
| > | Allows you to move the selected device from the Available Devices list into the Target Devices list. |
| < | Allows you to move the selected device from the Target Devices list to the Available Devices list. |
| << | Allows you to move all the devices in the Target Devices list to the Available Devices list. |
| Download | Downloads the files to the devices shown on the Target Devices list. |
| Stop | Terminates the ongoing operation. |
| Close | Discards your settings and closes the dialog box. |
| Help | Opens Online Help for the Download File to Device(s) dialog box. |

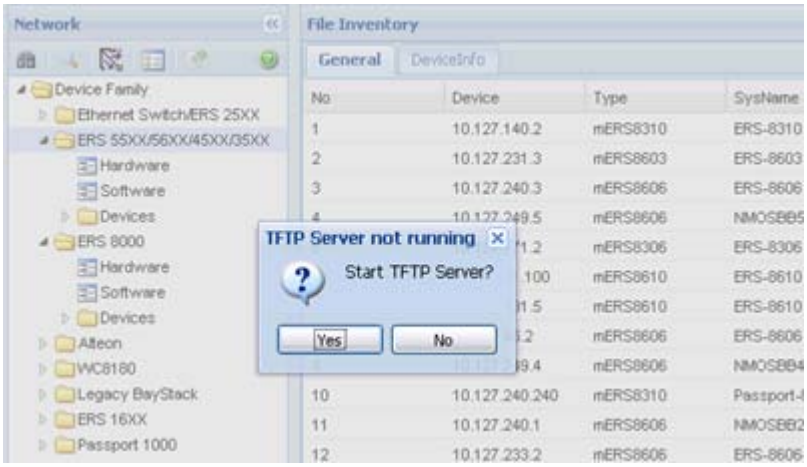
# Uploading a file from a device

Perform the following procedure to upload files from one or more devices.

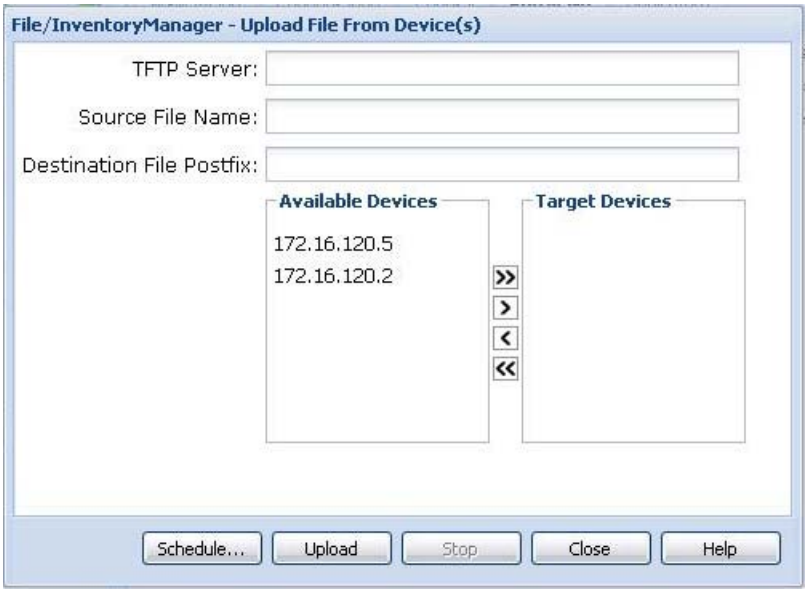
### Procedure steps

1. Open the File Inventory manager.
2. Select **Action**, **Upload File from Device(s)** from the menu bar.

   The TFTP Server Not Running dialog box appears.




3. Click **Yes** to start TFTP server. The File/Inventory Manager - Upload File to Device(s) dialog box appears.




4. In the **TFTP Server** field, enter the host name or IP address of the TFTP server for the upload operation.
5. In the **Action** field, select one of the option **uplodConfig** or **upldAsciiConfig** based on the requirement for upload operation.
6. Use the **Dest File Name** option to set how the filename is interpreted:
    - When you choose **No**, File Inventory Manager uploads the file with the selected filename.
    - When you choose **Yes**, File Inventory Manager uploads files from the selected device according to the IP address appended to the filename. For example, suppose the file name is config.cfg , and the selected device is 10.160.41.204, then the File Inventory Manager uploads the file 10_160_41_204_config.cfg from the device. The source directory for the upload operation is determined

by the settings of the TFTP server. Review the configuration settings of the TFTP server to determine the source directory.

7. In the **Available Devices** list, select one or more devices from which you want to upload the selected file.
8. Click **>** to move the selected device(s) to the **Target Devices** list. OR Click **>>** to move all the available devices to the **Target Devices** list. Use the **<** and **<<** buttons to move devices back to the **Available Devices** list.
9. Click **Upload** to transfer the file.

   File Inventory Manager opens an alert box to prompt you to confirm the upload operation.
10. Click **Yes** to continue. A message that shows the results of the operation appears at the bottom of the dialog box.

**Table 94: Parts of the Upload File from Device(s) dialog box**

| Part | Description |
|---|---|
| TFTP Server | Allows you to enter the IP address for the TFTP server for the operation. The default setting is the TFTP server (if any) specified on the Preferences dialog box. |
| Source File Name | Allows you to choose a file to upload. |
| Destination File Postfix | Allows you to enter a base filename for the destination file. Observe the following points regarding the destination filename:<br>• During the upload operation, the IP address of the device or devices will be appended to the base filename. This feature helps you upload configuration files from multiple devices without overwriting the destination files. For example, if you enter config.cfg as the filename, and selected two devices, 10.160.41.204 and 10.160.41.229. The actual destination files will be named 10_160_41_204_config.cfg and 10_160_41_229_config.cfg.<br>• The destination directory for the upload is determined by the settings of the TFTP server. Review the configuration settings of the TFTP server to determine the destination directory.<br>• For Ethernet Switch, ERS 55xx/35xx, and Legacy BayStack devices, the actual destination filename is limited to a maximum of 29 characters, including the appended IP address. |
| Available Devices list | Allows you to choose from all the available devices. |
| Target Devices list | Allows you to arrange multiple devices in the order in which you want to upload the files from them. |
| >> | Allows you to move all the devices from the Available Devices list into the Target Devices list. |

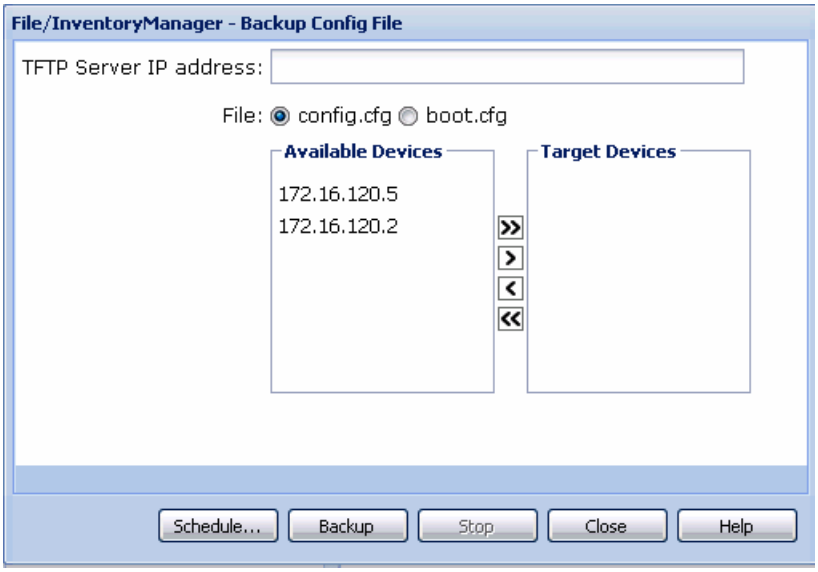
| Part | Description |
|---|---|
| > | Allows you to move the selected device from the Available Devices list into the Target Devices list. |
| < | Allows you to move the selected device from the Target Devices list to the Available Devices list. |
| << | Allows you to move all the devices in the Target Devices list to the Available Devices list. |
| Upload | Uploads the file from the devices shown in the Target Devices list and closes the dialog box. |
| Stop | Terminates the ongoing operation. |
| Close | Discards your settings and closes the dialog box. |
| Help | Opens online Help for the Upload File from Device(s) dialog box. |

## Backing up a configuration file

Perform the following procedure to back up configuration files from devices.

### Procedure steps

1. Open File Inventory Manager.
2. From the menu bar, choose **Actions, Backup Config File**. The File/Inventory Manager - Backup Config File dialog box appears.




3. In the **TFTP Server IP Address** field, enter the IP address of the TFTP server for the backup operation.

4. In the **File** field, select the type of file to back up (config.cfg or boot.cfg).
5. In the **Available Devices** list, select one or more devices whose configuration file you want to back up.
6. Click **>** to move the selected device to the **Target Devices** list. OR Click **>>** to move all the available devices to the **Target Devices** list. Use the **<** or **<<** buttons to move devices back to the **Available Devices** list.
7. Click **Backup** to back up the configuration file(s) immediately.

   File Inventory Manager opens an alert box to prompt you to confirm the upload operation.
8. Click **Yes** to continue. Configuration and Orchestration Manager backs up the selected configuration file to the \backup subdirectory of the TFTP root directory.

**Table 95: Parts of the Backup Config File dialog box**

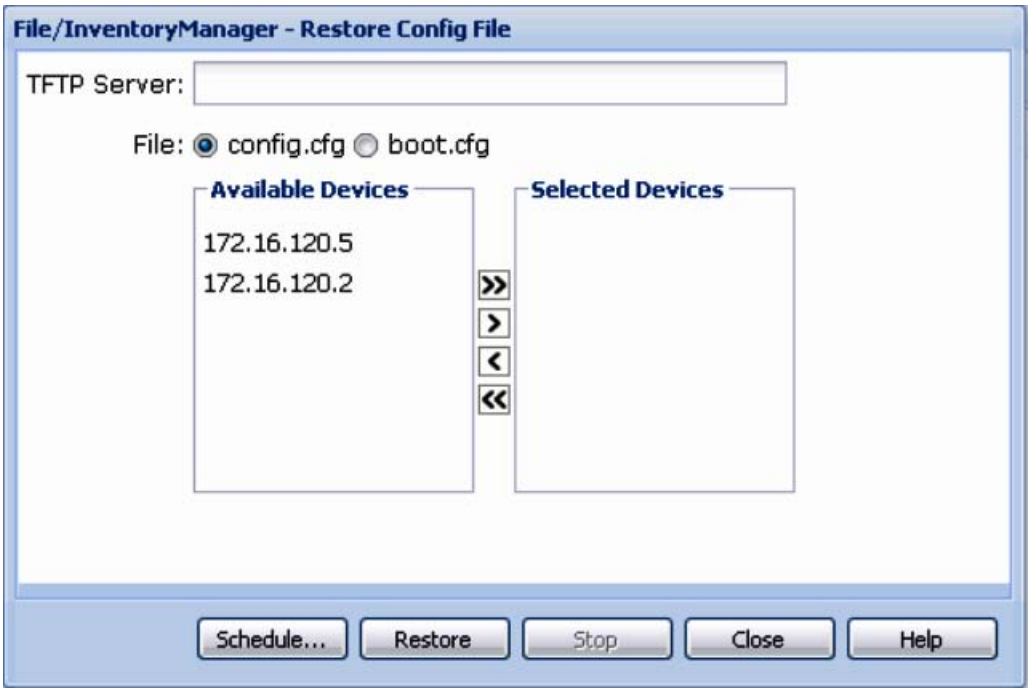
| Part | Description |
|---|---|
| TFTP Server IP Address | Allows you to enter the IP address for the TFTP server for the operation. The default setting is the TFTP server (if any) specified on the Preferences dialog box. |
| File | Allows you choose whether to back up the config.cfg or boot.cfg file. |
| Available Devices list | Allows you to choose from all the available devices. |
| Target Devices list | Allows you to arrange multiple devices in the order in which you want to back up the configuration files. |
| >> | Allows you to move all the devices from the Available Devices list into the Target Devices list. |
| > | Allows you to move the selected device from the Available Devices list into the Target Devices list. |
| < | Allows you to move the selected device from the Target Devices list to the Available Devices list. |
| << | Allows you to move all the devices in the Target Devices list to the Available Devices list. |
| Backup | Backs up the configuration file(s) for the devices shown in the Target Devices list and closes the dialog box. |
| Stop | Terminates the ongoing operation. |
| Close | Discards your settings and closes the dialog box. |
| Help | Opens Online Help for the Backup Config File dialog box. |

# Restoring a configuration File

Perform the following procedure to restore a configuration file to a device.

### Procedure steps

1. Open **File Inventory Manager**.
2. From the menu bar, choose **Actions, Restore Config File**. The File/Inventory Manager - Restore Config File dialog box appears.




3. In the **TFTP Server** box, enter the host name or IP address of the TFTP server for the restore operation.
4. In the **File** field, select the type of file to restore (config.cfg or boot.cfg).
5. Click **>** to move the selected device(s) to the **Target Devices** list. OR Click **>>** to move all the available devices to the **Target Devices** list. Use the **<** and **<<** buttons to move devices back to the **Available Devices** list.
6. Click **Restore** to restore the configuration files.

   File Inventory Manager opens an alert box to prompt you to confirm the upload operation.
7. Click **Yes** to continue. Configuration and Orchestration Manager restores the selected configuration file to the devices. It also logs the results of the restore operation to the selected backup log file

**Table 96: Parts of the Restore Config File dialog box**

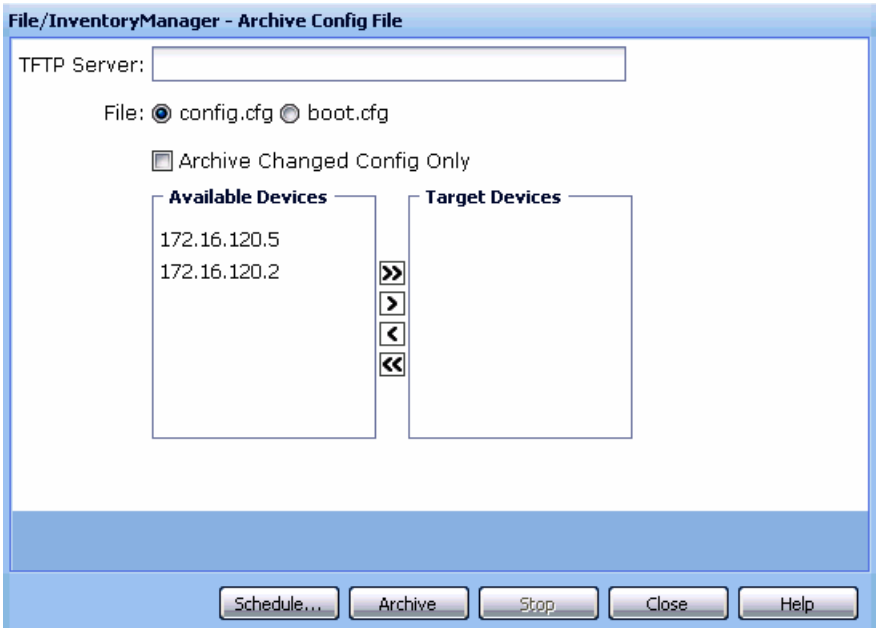
| Part | Description |
|---|---|
| TFTP Server | Allows you to enter the IP address for the TFTP server for the operation. The default setting is the TFTP server (if any) specified on the Preferences dialog box. |
| File | Allows you to choose whether to restore the config.cfg or boot.cfg file. |
| Available Devices list | Allows you to choose from all the available devices. |
| Target Devices list | Allows you to arrange multiple devices in the order in which you want to restore configuration files. |
| >> | Allows you to move all the devices from the Available Devices list into the Target Devices list. |
| > | Allows you to move the selected device from the Available Devices list into the Target Devices list. |
| < | Allows you to move the selected device from the Target Devices list to the Available Devices list. |
| << | Allows you to move all the devices in the Target Devices list to the Available Devices list. |
| Restore | Restores the configuration files for the devices shown in the Target Devices list and closes the dialog box. |
| Stop | Terminates the ongoing operation. |
| Close | Discards your settings and closes the dialog box. |
| Help | Opens Online Help for the Restore Config File dialog box. |

# Archiving a configuration file

Perform the following procedure to archive a device configuration file.

### Procedure steps

1. Open **File Inventory Manager**.
2. From the menu bar, choose **Actions, Archive Config File**. The File/Inventory Manager - Archive Config File dialog box appears.




3. In the **TFTP Server** field, enter the host name or IP address of the TFTP server for the archive operation.
4. Use the **File** option to select the type of file to archive (config.cfg or boot.cfg).
5. Select **Archive Changed Config Only** option to archive the configuration file only if it differs from the last saved file.
6. In the **Available Devices** list, select one or more devices whose configuration file you want to archive.
7. Click **>** to move the selected device(s) to the **Target Devices** list. OR Click **>>** to move all the available devices to the **Target Devices** list. Use the **<** and **<<** buttons to move devices back to the **Available Devices** list.
8. Click **Archive** to archive the configuration files.

   File Inventory Manager opens an alert box to prompt you to confirm the upload operation.
9. Click **Yes** to continue. Configuration and Orchestration Manager archives the selected configuration file(s). It also logs the results of the archive operation to the selected archive log file.

**Table 97: Parts of the Archive Config File dialog box**

| Part | Description |
|---|---|
| TFTP Server | Allows you to enter the IP address for the TFTP server for the operation. The default setting is the TFTP server (if any) specified on the Preferences dialog box. |
| File | Allows you to choose whether to archive the config.cfg or boot.cfg file. |

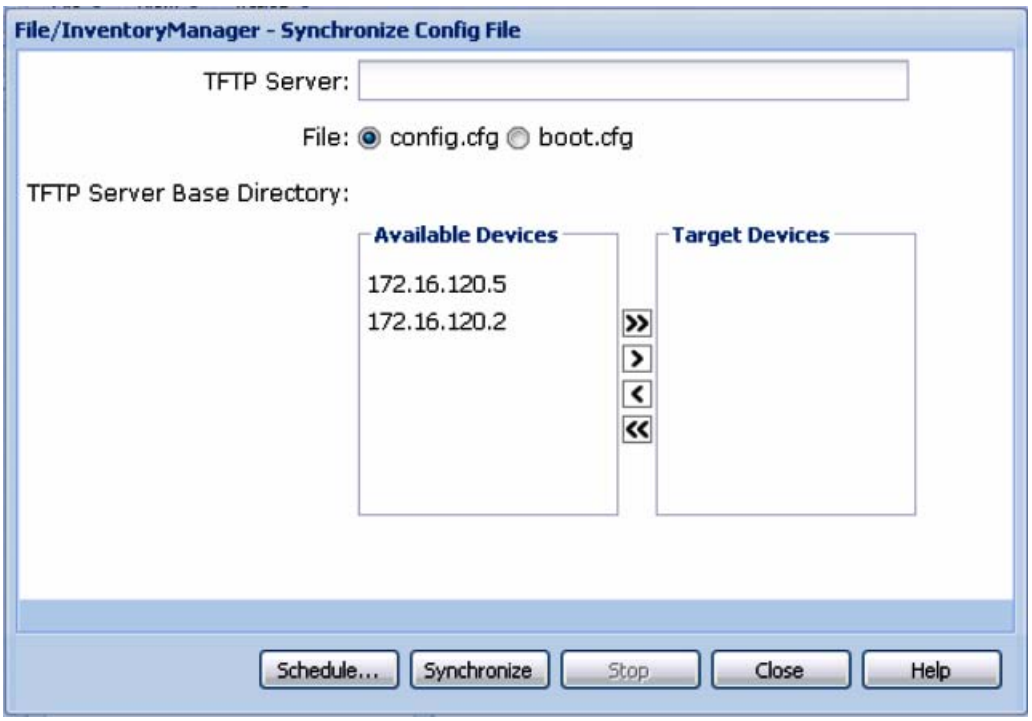
| Part | Description |
|---|---|
| Archive Changed Config Only | Specifies to archive the configuration only if it has changed. COM compares the latest archived file with the current configuration and saves a new file only if the current configuration is different from the archived file. |
| TFTP Server Base Directory | Specifies the base directory of the TFTP server. Click the **Browse** button to browse. |
| Available Devices list | Allows you to choose from all the available devices. |
| Target Devices list | Allows you to arrange multiple devices in the order in which you want to archive their configuration files. |
| >> | Allows you to move all the devices from the Available Devices list into the Target Devices list. |
| > | Allows you to move the selected device from the Available Devices list into the Target Devices list. |
| < | Allows you to move the selected device from the Target Devices list to the Available Devices list. |
| << | Allows you to move all the devices in the Target Devices list to the Available Devices list. |
| Archive | Archives the configuration files for the devices shown in the Target Devices list and closes the dialog box. |
| Stop | Terminates the ongoing operation. |
| Close | Discards your settings and closes the dialog box. |
| Help | Opens online Help for the Archive Config File dialog box. |

## Synchronizing the configuration files on devices

Perform the following procedure to synchronize the configuration files on devices in your network. You can use this procedure to upload a current configuration or boot.cfg file of the device to the currently deployed subdirectory of the TFTP root directory.

### Procedure steps

1. Open **File Inventory Manager**.
2. From the menu bar, choose **Actions, Synchronize Config File**. The File/Inventory Manager - Synchronize Config File dialog box appears.




3. In the **TFTP Server** field, enter the host name or IP address of the TFTP server for the synchronize operation.
4. Use the **File** option to select the type of file to synchronize (config.cfg or boot.cfg).
5. In the **Available Devices** list, select one or more devices whose configuration file you want to synchronize.
6. Click **>** to move the selected device(s) to the **Target Devices** list. OR Click **>>** to move all the available devices to the **Target Devices** list.
7. Use the **<** and **<<** buttons to move devices back to the **Available Devices** list.
8. Click **Synchronize** to upload the configuration files.

   File Inventory Manager opens an alert box to prompt you to confirm the upload operation.
9. Click **Yes** to continue.

**Table 98: Parts of the Synchronize Config File dialog box**

| Part | Description |
|---|---|
| TFTP Server | Allows you to enter the IP address for the TFTP server for the operation. The default setting is the TFTP server (if any) specified on the Preferences dialog box. |
| File | Allows you choose whether to synchronize the config.cfg or boot.cfg file. |

| Part | Description |
|---|---|
| TFTP Server Base Directory | Specifies the base directory of the TFTP server. |
| Available Devices list | Allows you to choose from all the available devices. |
| Target Devices list | Allows you to arrange multiple devices in the order in which you want to synchronize their configuration files. |
| >> | Allows you to move all the devices from the Available Devices list into the Target Devices list. |
| > | Allows you to move the selected device from the Available Devices list into the Target Devices list. |
| < | Allows you to move the selected device from the Target Devices list to the Available Devices list. |
| << | Allows you to move all the devices in the Target Devices list to the Available Devices list. |
| Synchronize | Uploads the configuration files for the device(s) shown in the Target Devices list to the currently deployed subdirectory of the TFTP root directory and closes the dialog box. |
| Stop | Terminates the ongoing operation. |
| Close | Discards your settings and closes the dialog box. |
| Help | Opens Online Help for Synchronize Config File dialog box. |

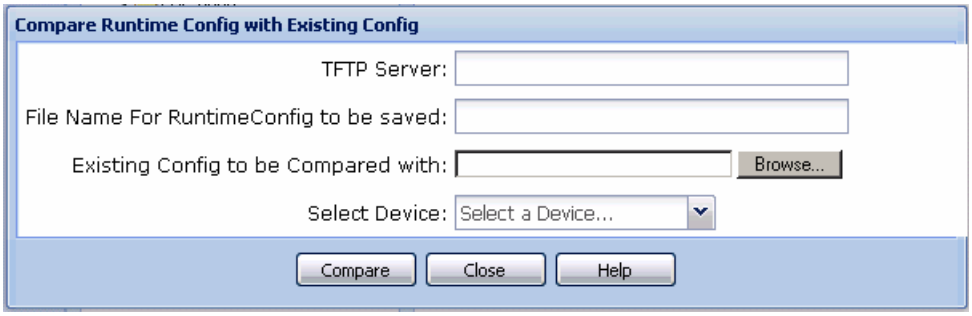
# Comparing runtime configuration with existing configuration

Perform the following procedure to compare the runtime configuration with an existing configuration.

### Procedure steps

1. Open the **File Inventory manager**.
2. From the menu bar, choose **Action**, **Compare Runtime Config with Existing Config**.

   The Compare Runtime Config With Existing Config dialog box appears.




3. Complete the fields as described in the following table

| Field | Description |
|---|---|
| TFTP Server | Specifies the host name or IP address of the TFTP server for the compare operation. |
| File Name For RuntimeConfig to be saved | Specifies the name of the runtime configuration file that is saved for the compare operation. |
| Existing Config to be Compared with | Specifies the existing configuration file to compare against the runtime configuration. Click the **Browse** button to browse the file. |
| Select Device | Specifies the selected device. |

4. Click **Compare** to perform the operation.

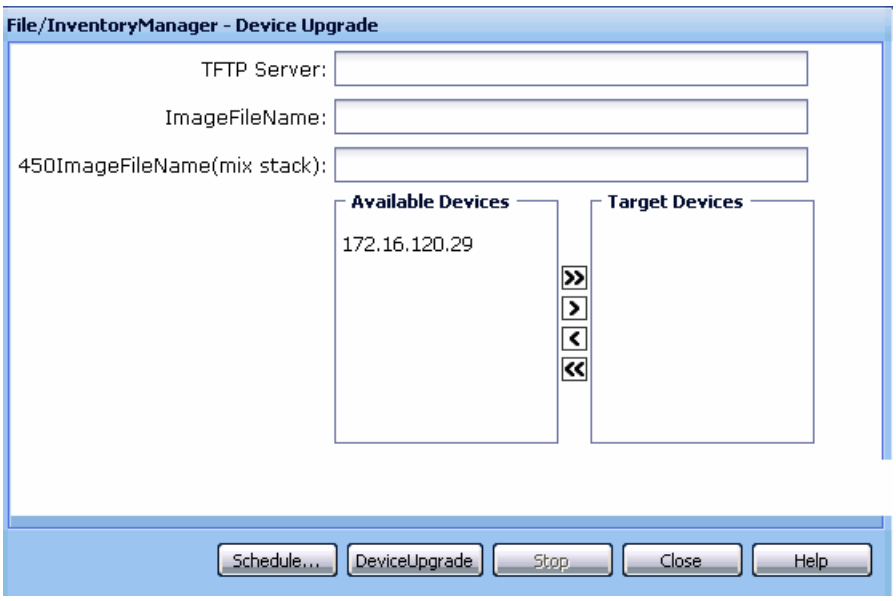
## Upgrading a device

Perform the following procedure to upgrade the image file on a device.

### Procedure steps

1. Open **File Inventory Manager**.
2. From the menu bar, choose **Actions**, **Device Upgrade**.

   The File/Inventory Manager - Device Upgrade dialog box appears.




3. In the **TFTP Server** field, enter the host name or IP address of the TFTP server for the upgrade operation.
4. In the **ImageFileName** field, enter the name of the image file to download.
5. In the **450ImageFileName(mix stack)**field, enter the name of the 450image (mix stack).
6. In the **Available Devices** list, select one or more devices to upgrade.
7. Click **>** to move the selected device(s) to the **Target Devices** list. OR Click **>>** to move all the available devices to the **Target Devices** list. Use the **<** and **<<** buttons to move devices back to the **Available Devices** list.
8. Click **DeviceUpgrade** to upgrade the devices immediately.

   File Inventory Manager opens an alert box to prompt you to confirm the upload operation.
9. Click **Yes** to continue.

**Table 99: Parts of the Device Upgrade dialog box**

| Part | Description |
|---|---|
| TFTP Server | Allows you to enter the IP address for the TFTP server for the operation. The default setting is the TFTP server (if any) specified on the Preferences dialog box. |
| ImageFileName | Allows you to enter the name of the file to download. |
| Available Devices list | Allows you to choose from all the available devices. |
| Target Devices list | Allows you to arrange multiple devices in the order in which you want to upgrade them. |
| >> | Allows you to move all the devices from the Available Devices list into the Target Devices list. |

| Part | Description |
|---|---|
| > | Allows you to move the selected device from the Available Devices list into the Target Devices list. |
| < | Allows you to move the selected device from the Target Devices list to the Available Devices list. |
| << | Allows you to move all the devices in the Target Devices list to the Available Devices list. |
| DeviceUpgrade | Downloads the selected image file to the device(s) shown in the Target Devices list and closes the dialog box. |
| Stop | Terminates the ongoing operation. |
| Close | Discards your settings and closes the dialog box. |
| Help | Opens Online Help for Device Upgrade dialog box. |

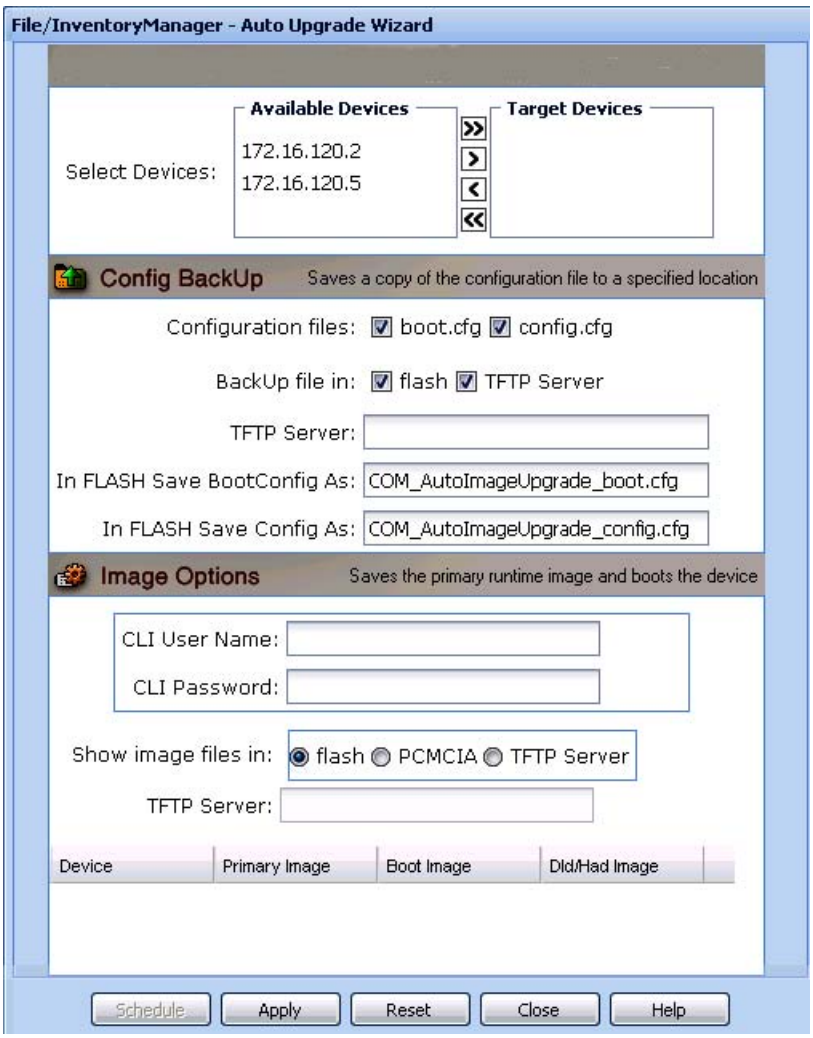
## Upgrading devices using Device Upgrade wizard

For ERS 8000 device family, you can update a device using the Device Upgrade Wizard.

### Procedure steps

1. Open **File Inventory manager**.
2. From the menu bar, select **Action >> Device Upgrade Wizard**.

   The File/Inventory Manager - Auto Upgrade Wizard appears.




3. Click **>** to move the selected device(s) to the **Target Devices** list. OR Click **>>** to move all the available devices to the **Target Devices** list. Use the **<** and **<<** buttons to move devices back to the **Available Devices** list.
4. In the **Config Backup** pane, specify the following parameters for the backup operation:
    - In the **Configuration files** field, select the file types to back up; you can choose config.cfg or boot.cfg, or both.
    - In the **BackUp files in** field, select the destination for the backup files; you can choose flash or TFTP Server or both.
    - If you are uploading to TFTP, enter the host name or IP address of the TFTP server for the upload operation in the **TFTP Server** field.
    - If you are backing up the boot.cfg file to flash, enter a filename for the backup boot.cfg file (by default, COM_AutoImageUpgrade_boot.cfg) in the **In FLASH Save Bootconfig As** field.

- If you are backing up the config.cfg file to flash, enter a filename for the backup config.cfg file (by default, COM_AutoImageUpgrade_config.cfg) in the **In FLASH Save Config As** field.

**Important:**

If you do not specify a location in the BackUp files in field and you click Apply, COM automatically instructs the device to save a backup of the boot.cfg file in flash as COM_AutoImageUpgrade_boot.cfg. This is because a workable boot.cfg file is required in case of malfunction during the booting process.

5. In the **Image Options** pane, enter a valid CLI user name and password in the **CLI User Name** and **CLI Password** fields.

**Important:**

This CLI user name and password applies to all devices in the Image Options table. To update all listed devices at the same time, they must all have the same CLI user name and password.

6. In the **Show Image Files in** field, choose the source location for the image file. If you choose TFTP Server as the image location, enter the host name or IP address of the **TFTP server** in the provided field.
7. For each device listed in the **Image Options** table, you must specify both the desired primary runtime image and the desired boot image as follows:
   - In a device row, double-click the Boot Image, Primary Image, or Dld/Had Image field. A dialog box appears displaying the available images from the specified location. (If TFTP Server is selected, a Find File dialog box appears allowing you to browse to and select a file.) To display the available images from a different source location, close the dialog box and choose a different location from the Show images files in field, then double-click the Boot Image, Primary Image, or Dld/Had Image field again.
   - Select the desired image from the list.
   - Click **Add**. The selected image file is inserted into its respective column. Repeat these steps for the boot image, primary image, and dld/had image of each device in the list. If you make any mistakes when choosing the desired images, you can click Reset to set the Upgrade Wizard to the default view.
8. After you have specified all desired primary runtime images, boot images, loadable images, and backup parameters, click **Apply**.

**Important:**

If there is a version difference between the primary runtime image and the boot image, a warning message dialog box appears before you can proceed. To properly upgrade images on a device, Avaya recommends that a device have the same version of boot and runtime images.

COM performs the following, one device at a time, according to the listed order of devices:

- backs up the configuration files on the device

- validates and sets the new primary runtime image and boot image
- validates and sets the new loadable image
- resets the device

This operation takes time to complete (approximately 3 minutes to complete for one switch). The logs for the image upgrades are generated in the file AutoImageUpgrade.log under the COM home folder.

# Managing inventory

File Inventory Manager allows you to work with inventory files and view inventory information. The following sections contain information about how to work with and view inventory information.


- Working with inventory files on page 286
- Viewing inventory information on page 289


## Working with inventory files

You can save network inventory information to inventory files. Later, you can reload the inventory information back into File Inventory Manager, or into third-party spreadsheet or database applications.

You can create two different types of files with File Inventory Manager. The following table describes the file types.

**Table 100: Files types supported by File Inventory Manager**

| File type | Description |
|---|---|
| Inventory file (.inv) | Allows you to save inventory information that you can later reload back into File Inventory Manager. |
| Tab-delimited text file | Allows you to save inventory information in tab-delimited text file format that you can later load into third-party spreadsheet and database applications. |

The following sections describe the various operations that you can perform with inventory files.


- Saving inventory information to a file on page 287
- Saving inventory information in a tab delimited text file on page 287
- Loading inventory information from a file on page 288

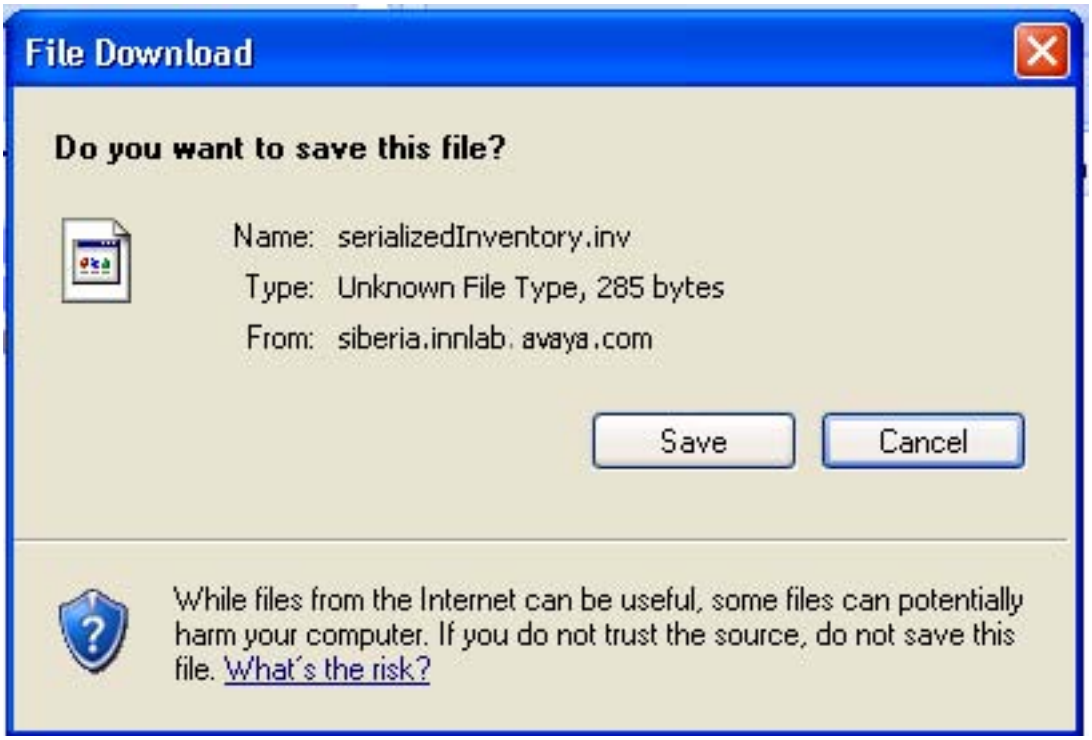
## Saving inventory information to a file

File Inventory Manager allows you to save inventory information to a file. You can use this feature to create inventory files that you can load again later. Perform the following procedure to save the network inventory to a file.

### Procedure steps

1. From the **File Inventory Manager** menu bar, choose **File, Save Inventory Info**.

   The File Download dialog box appears.




2. Click **Save**.
3. Browse the folder where you want to save the inventory information.
4. In the **File name** box, enter a name for the file. The default file name extension is .inv. You can change the extension if you prefer.
5. Click **Save**. File Inventory Manager saves the inventory information in the specified folder and file.

## Saving inventory information in a tab delimited text file

File Inventory Manager allows you to save network inventory information in a tab-delimited text file. You can use this feature to export network inventory information to spreadsheet or database software applications.

Perform the following procedure to save the network inventory to a tab-delimited text file.

### Procedure steps

1. From the **File Inventory Manager** menu bar, choose **File, Save Inventory in Tab delimited text file**.

   A Save dialog box appears.
2. Click **Save** to save the file. OR Click **Open** to view the file.
3. Browse the folder where you want to save the inventory information.
4. In the **File Name** field, enter a name for the file. The default filename extension is .txt. You can use a different extension also.
5. Click **Save**. File Inventory Manager saves the inventory information in the specified folder and file.

## Loading inventory information from a file

File Inventory Manager allows you to load inventory information from inventory files that you previously created. You can use this feature to quickly load inventory information without having to poll it from the network devices. You can also use it to load inventory information for previous network configurations, or for devices that no longer appear on the network.

Perform the following procedure to load inventory information from a file.

### Procedure steps

1. From the File Inventory Manager menu bar, choose **File, Open Inventory File**.

   The File/Inventory Manager - Open Inventory File dialog box appears.


2. Click the + (plus sign) to browse the folder that contains the inventory file you want to open.

   **Important:**

   By default, the Open File dialog box filters for files with the filename extension .inv. If you have saved your inventory files using a different extension, replace .inv in the File name box with the actual filename extension.

3. Click **Open Inventory**.
4. If there is any inventory information already loaded in File Inventory Manager, an alert box prompts you whether you want to keep the current inventory data or not.
5. Do one of the following:
   - Click **Yes** to add the data in the file to the currently loaded inventory data. However, any data in the file about devices in the current inventory is discarded, and does not overwrite data in the current inventory.
   - Click **No** to discard all of the currently loaded inventory data and then load the inventory data from the file.

   File Inventory Manager loads the inventory information from the file.

# Viewing inventory information

This section provides information about how to view inventory information using File Inventory Manager. Use the information in this section to perform the following tasks:


- Viewing hardware configuration information on page 289
- Viewing software configuration information on page 290
- Updating the inventory on page 291
- Highlighting inventory on the topology map on page 292

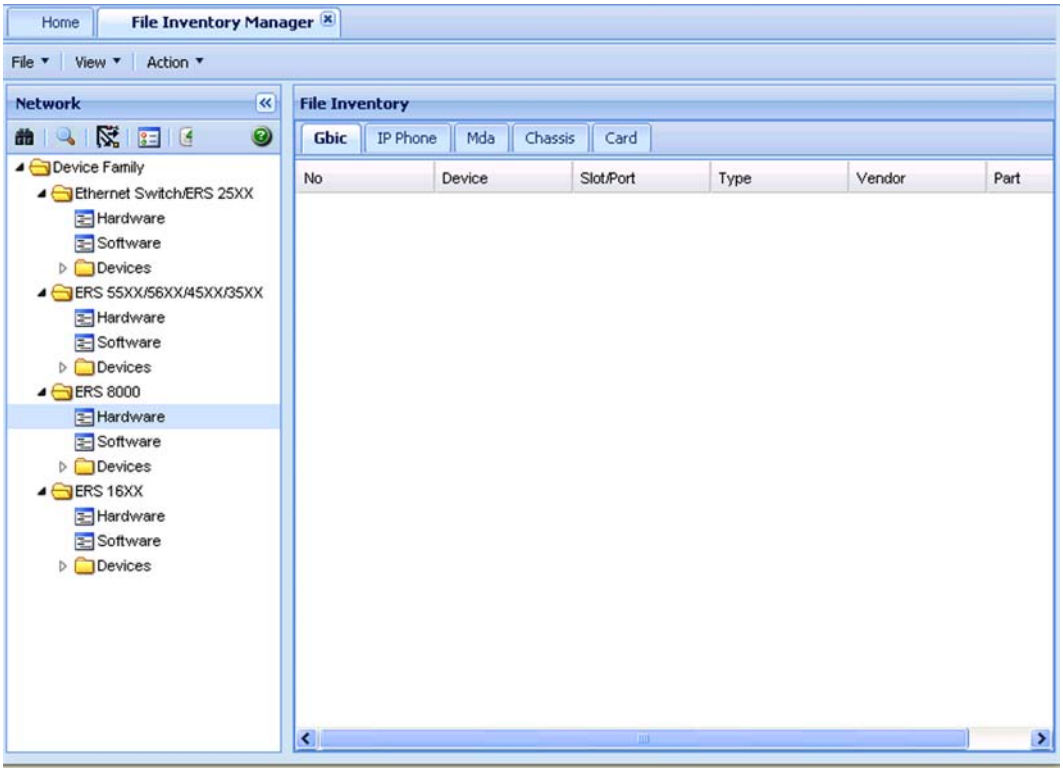

## Viewing hardware configuration information

Perform the following procedure to view hardware configuration.

### Procedure steps

1. Open the **File Inventory Manager**.
2. Select **Hardware** from any device family folder on the Navigation pane. The hardware information appears in the Contents panel.

   The following figure shows the hardware information of ERS 8000.




Content pane displays Gbic, IP Phone, Mda, Card, and Chassis information in different tabs.

### Viewing hardware configuration of a specific device

Perform the following procedure to view the hardware configuration of a specific device.

### Procedure steps

1. Open **File Inventory Manager**.
2. On the Navigation pane, select the target device from any **Device family** folder.
3. Click the **Hardware** tab.

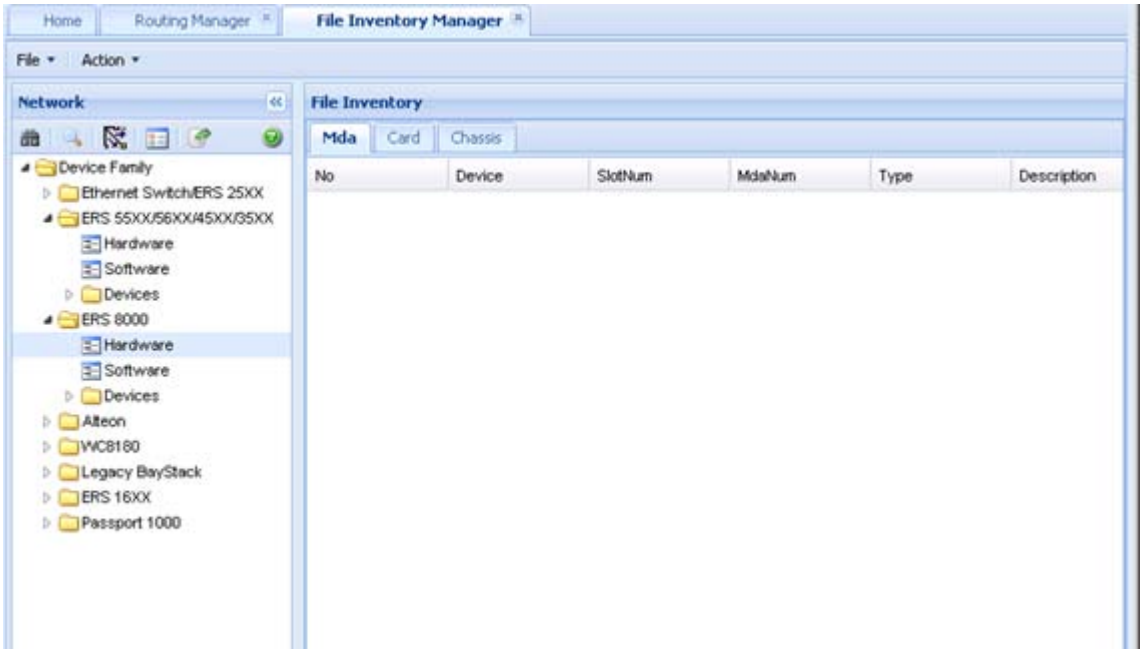
## Viewing software configuration information

Perform the following procedure to view software configuration.

### Procedure steps

1. Open **File Inventory Manager**.
2. Select **Software** from any**Device family** folder on the Navigation pane. The software information appears in the Contents pane.

   The following figure shows the software information of ERS 8000.




Content pane shows WSM Image, Configuration, General, Software, and DeviceInfo information in different tabs.

Content pane shows General and Image/Config information in different tabs.

### Viewing software information of a specific device

Perform the following procedure to view the software formation of a specific device.

### Procedure steps

1. Open File Inventory manager.
2. In Navigation pane, select the target device from any **Device family** folder.
3. Click the **Software** tab.

## Updating the inventory

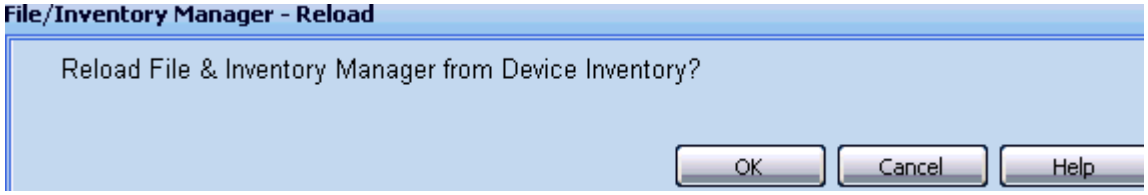
File Inventory Manager allows you to refresh the information in the window with inventory information polled from the network devices. You can use this feature to load any updated information that took effect since you opened File Inventory Manager.

Perform the following procedure to reload the inventory.

### Procedure steps

1. On the File Inventory Manager toolbar, click the **Reload/Discover** icon Or, choose **File, Reload**.

   A File/Inventory Manager - Reload confirmation dialog box appears.




2. Click **OK**.
3. In the **Available Devices** list, select one or more devices to which you want to download the selected file.
4. Click **>** to move the selected device(s) to the **Target Devices** list. OR Click **>>** to move all the available devices to the **Target Devices** list. Click **<** or **<<** to move devices back to the **Available Devices** list.
5. Click **Query Now**.

   COM reloads topology information from the network devices, and refreshes the File Inventory Manager window with it.

## Highlighting inventory on the topology map

As with Trunking Manager and VLAN Manager, the File Inventory Manager supports device highlighting on the Topology map.

Perform the following procedure to highlight file inventory devices on the Topology Map.

### Procedure steps

1. Select a device or device parent node from the File Inventory Manager Navigation pane.
2. Click **Highlight on Topology** icon from the toolbar. Click the Highlight on Topology icon automatically navigate you to the COM Dashboard tab, and displays the selected devices in green highlighting.

**Important:**

Both the Dashboard tab and the File Inventory Manager tabs can be undocked from the main COM content panel and aligned side by side. Undocking and aligning the two tabs within view allows you to scroll up and down the navigation tree and see the highlighted devices come into focus.

# Chapter 10: Using Virtual Routing and Forwarding Manager

Virtual Routing and Forwarding (VRF) Manager is a feature that you can use to configure and manage virtual routing and forwarding on Avaya Ethernet Routing Switch 8600 (ERS 8600), Avaya Ethernet Routing Swith 8300 (ERS 8300), and Avaya Virtual Services Platform (VSP) 9xxx devices. You can use VRF Manager to set the VRF configuration for each device, as well as manage VRF configurations across multiple devices.

The following table outlines the supported device list for VRF.

| Supported devices for VRF | Version |
|---|---|
| ERS 8600 | v5.0 and up |
| ERS 8300 | v4.1 and up |
| VSP 9xxx | v3.0 |

The ERS 8600, ERS 8300, and VSP 9xxx devices support different VRF contexts. The contexts determine the level of access that you have to the switch. Configuration and Orchestration Manager (COM) discovers the VRF information using the GlobalRouter (VRF0) context, which allows the COM administrator to access and manage the entire switch. When the COM administrator assigns users the ability to use VLAN Manager, the COM administrator can control access to the ERS 8600, ERS 8300, or VSP 9xxx device and its functionality by assigning the appropriate VRF context:

- VRF0—If the administrator assigns you the GlobalRouter privilege (VRF0), you can create VRF, and update the VRF table.
- Non-zero VRF—If the administrator assigns you non-GlobalRouter privilege (non-Zero VRF), some features can be disabled for you as you do not have sufficient credentials to perform certain operations.
- No VRF—If no VRF is assigned, then you will default to the GlobalRouter privilege.

A user with the GlobalRouter privilege can choose to switch-to a different context for a device, and behave as that context for that particular session. When you switch to a different context, you can manage only those functions and components that are assigned to that specific VRF. The switched-to context is relevant and applies to the other managers, like Routing Manager and EDM plug-ins.

When an administrator configures a context, the context applies to the access that you have in COM, and also determines the level of access that you have in the device manager.

In addition to the privileges, the method of access to the ERS 8600, ERS 8300, or VSP 9xxx device is associated with a context:

- For SNMPv2 access, you need to have GlobalRouter privilege to operate the VRF manager correctly.
- For SNMPv3 access, a specific VRF needs to be assigned to the user for the device.

Virtual Services Platform devices function similarly to the ERS 8000 family of devices, except for the following:

- VSP devices support 512 VRFs and max routes are up to 250000
- Pim is not supported

The dialog for the creation of VRFs validates the ranges for the devices being set.

### Navigation

Virtual Routing and Forwarding on page 294

# Virtual Routing and Forwarding

VRF allows multiple instances of a routing table to coexist within the same router at the same time. The routing instances are independent; the same or overlapping IP addresses are used without conflicting with each other. In VRF-supported devices, you can configure more than one VRF.

### Prerequisites

- You must have the VRF Manager assigned in the **MultiElementManager Assignment** tab by the administrator.
- You must have devices assigned by the administrator.

### Navigation


- Starting VRF in the COM on page 295
- Adding VRF on a device or multiple devices on page 296
- Setting VRF content for devices on page 297
- Viewing all the VRFs and its statistics configured for a specific device on page 298
- Editing a single configuration or multiple VRF configurations on page 298
- Deleting a VRF configuration from a device on page 299
- VRF enhancement—VLAN and routing on page 299

# Starting VRF in the COM

Perform the following procedure to start the VRF.

### Procedure steps

1. In the **Configuration and Orchestration Manager Navigation** tree, expand **Managers**, and then click **Virtual Routing Manager** icon.

   The Virtual Routing and Forwarding discovery is triggered, and result of discovery operation is displayed.

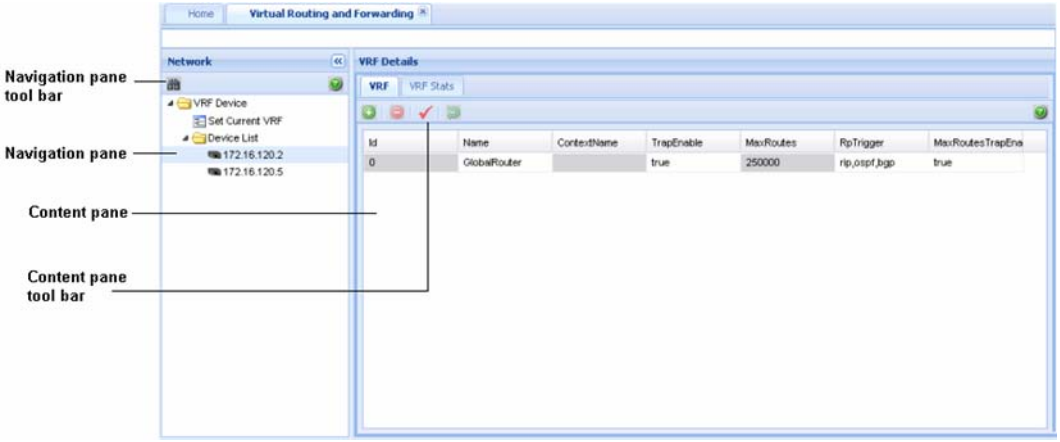
2. Click **Ok** to view the Virtual Routing and Forwarding window.

   **OR**

   Click **Details** to view the errors and warnings, if any.

3. In the VRF navigation pane, expand the **VRF Device** folder and the **Device List** folder.

   The VRF Details dialog box appears.




The following table describes the parts of Virtual Routing and Forwarding window.

**Table 101: Virtual Routing and Forwarding window parts**

| Parts | Description |
|---|---|
| Navigation pane | Lists the navigation tree, and the functions that you can perform on Virtual Routing and Forwarding devices. |
| Navigation pane tool bar | Provides Discover VRF and Help tools. |
| Content pane | Displays information about the Virtual Routing and Forwarding devices. |

| Parts | Description |
|---|---|
| Content pane tool bar | Provides quick access to commonly used Virtual Routing and Forwarding commands. |

# Adding VRF on a device or multiple devices

Perform the following procedure to add the VRF on a device or multiple devices.

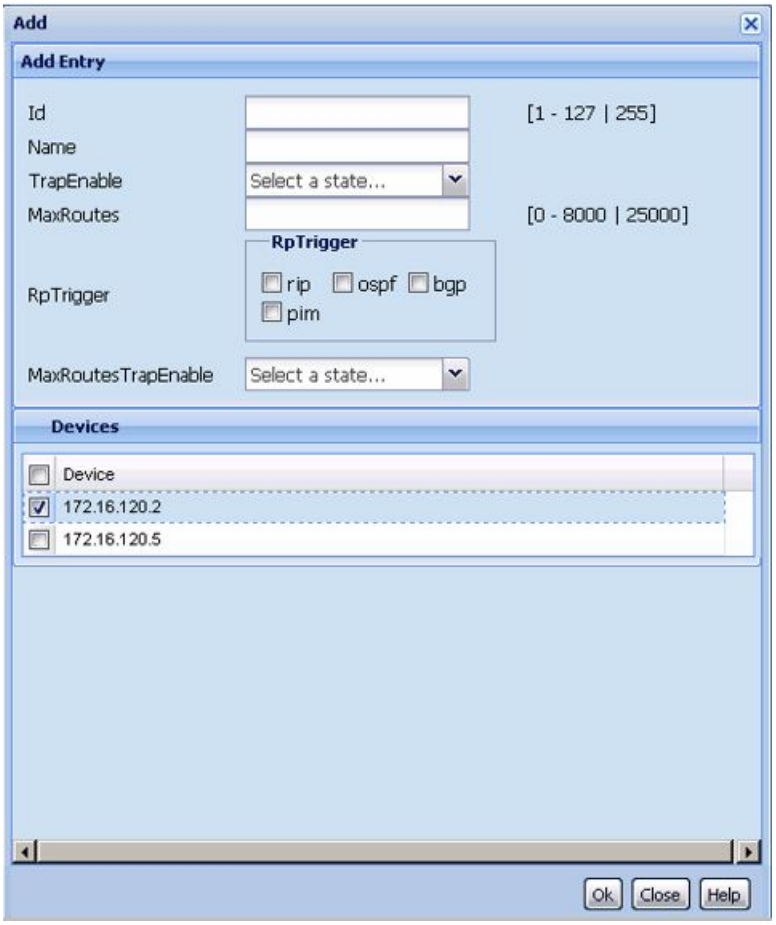
### Procedure steps

1. In the navigation pane of Virtual Routing and Forwarding window, expand the **Device List** folder, and select the target device from the navigation tree.

   The VRF information appears in the contents pane.

2. In the **Contents** toolbar, click **Create Entry**.

   The Add Entry dialog box appears.



3. Set the parameters as appropriate.
4. In the **Devices** table, select the target device or devices.

   If you select multiple devices, then the VRF Manager creates the same VRF configuration on the target devices.

   **Important:**
   VRF functionality applies only to the core router devices, therefore only the relevant 8600/8300 or VSP devices are listed in the Device table.
5. Click **Ok**.

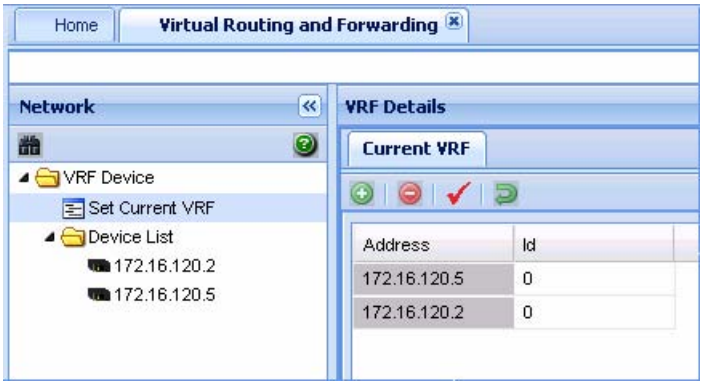
# Setting VRF content for devices

Perform the following procedure to set the VRF content for devices that are used by the COM.

### Procedure steps

1. In the navigation pane of Virtual Routing and Forwarding window, expand the **Device List** folder, click **Set Current VRF** to assign a VRF to the target device.

   The Current VRF table appears in the content pane.




2. For the target devices, change the VRF Id in the **Id** field.
3. Click **Apply Changes**.

   **Important:**
   If you assign a VRF Id as the current VRF for a device, the other managers display only the information specific to that VRF.

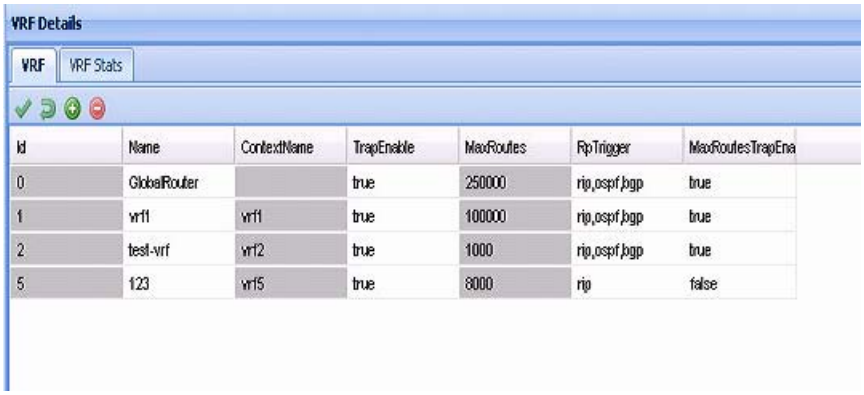
# Viewing all the VRFs and its statistics configured for a specific device

Perform the following procedure to view all the VRFs and its statistics configured for a specific device that is used by the COM.

### Procedure steps

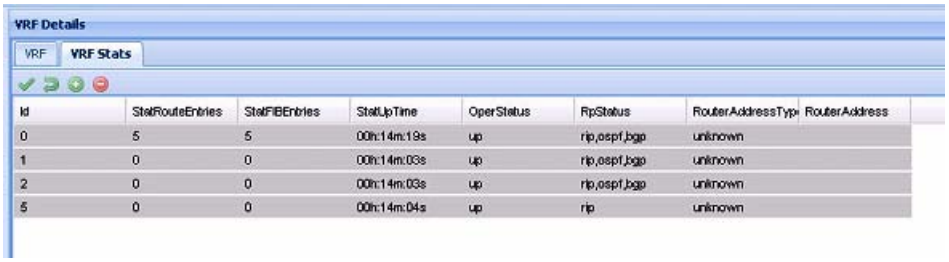
1. In the navigation pane of Virtual Routing and Forwarding window, expand the **Device List** folder, and select a device from the navigation tree.

   The VRF information appears in the contents pane.




2. To see the VRF statistics in the contents pane, click the **VRF Stats** tab.

   The VRF statistics information appears in the contents pane.




# Editing a single configuration or multiple VRF configurations

Perform the following procedure to edit a single VRF configuration or multiple VRF configurations on a specific device.

### Procedure steps

1. In the navigation pane of Virtual Routing and Forwarding window, expand the **Device List** folder, and select the target device from the navigation tree.

   The VRF information appears in the contents pane.
2. In the non-greyed fields, make the changes.
3. Click **Apply Changes** to confirm the changes you made.
4. Click **Revert Changes** to revert all the changes made in the VRF table.

## Deleting a VRF configuration from a device

Perform the following procedure to delete a VRF configuration from a device.

### Procedure steps

1. In the navigation pane of Virtual Routing and Forwarding window, expand the **Device List** folder, and select the target device from the navigation tree.

   The VRF information appears in the contents pane.
2. Select the VRF configuration that you want to delete.
3. Click **Delete Entry**.

   The VRF configuration confirmation dialog box appears.
4. Click **Yes**.

## VRF enhancement—VLAN and routing

Multicast and routing managers use the selected VRF ID from the VRF manager to discover the protocol information. Protocols are virtualized based on the supported devices and enabled protocols for the particular VRF.

#### VRF - based discovery

COM discovers the information using GlobalRouter (VRF0) and not the non-zero VRF of the device. This enhancement provides support to access and configure the non-zero VRF also (along with the GlobalRouter). The discovery occurs based on the VRF you select (vrf-n) where n is the VRF ID. VLAN Manager uses the VRF ID to communicate with the device. The VLAN Manager has a column for the VRF ID (called VrfId). You can change the VLAN to a different VRF. The Routing Manager is aware of the VRF. The Routing Manager displays routing tables and views that show the VRF.

# Chapter 11: Using the Bulk Configuration Manager

The Avaya Bulk Configuration Manager (Avaya BCM) is an application within the Configuration and Orchestration Manager (COM) that consists of a suite of tools that permits you to perform a variety of management tasks across multiple device types using a Web-based interface.

The Avaya BCM requires a separate license to enable the feature set.

**Navigation**



## Node based licensing for BCM

The Avaya Bulk Configuration Manager (BCM) depends on COM. The Avaya BCM resides in COM and follows the same COM rules and restrictions, except that the BCM user gets all supported devices automatically, and skips the device assignment process. To enable the BCM for COM, you must acquire a separate license. The BCM license is node-based, but only counts individual uses of a node. A base license is 100 nodes. If you have a 100 node license, you may have more than 100 devices in inventory. However, after you create tasks that use 100 unique devices, you cannot create tasks for more devices; a license error appears informing you that you have reached the limit and should purchase more increments. If no BCM license is supplied, you can still launch BCM from the COM managers screen to create tasks and import devices, but you cannot run the tasks without a license.

The following list outlines the four types of BCM node based licenses:

- BCM_100_base, (100)
- BCM_Upgrd100_5000_base, (5000)
- BCM_Upgrd100_1200_base, (1200)
- BCM_Upgrd1200_5000_base (5000)

**Note:**
BCM supports device imports from COM or VPFM.

For more information about the configuration of BCM, see *Avaya Bulk Configuration Manager Fundamentals* (NN48021-100).

# Launching BCM main window and navigation

To launch the Bulk Configuration Manager (BCM) main window and navigation, perform the following procedure.

### Procedure steps

1. From the Configuration and Orchestration Manager window Navigation pane, click **Managers**.

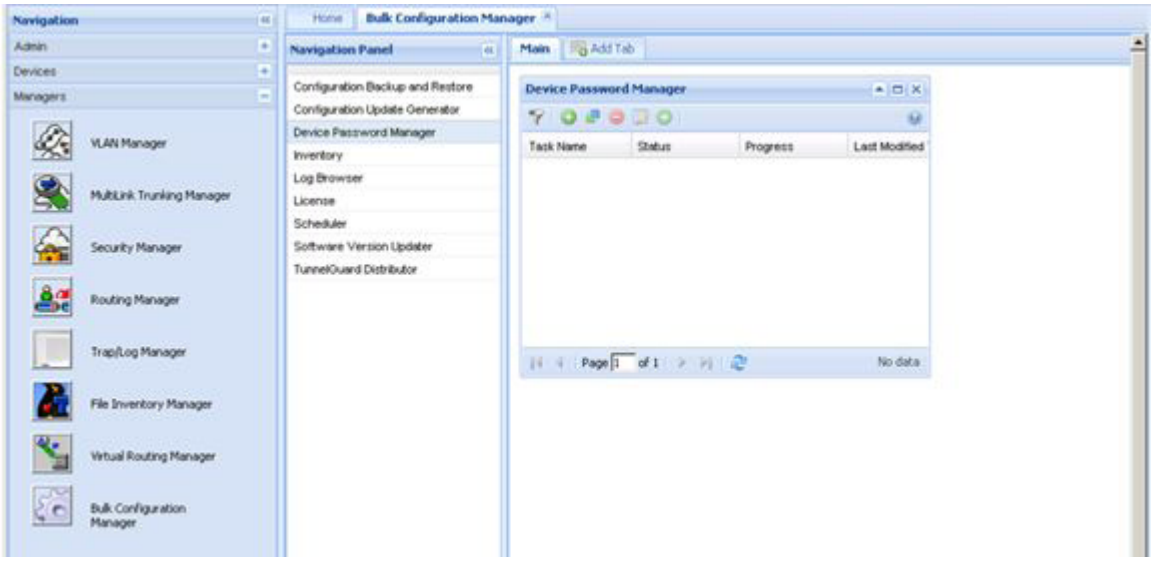
   The list of managers appears on the left side of the window.

2. In the navigation tree, click the **Bulk Configuration Manager** icon.

   The Bulk Configuration Manager is launched and appears in the content pane, under a new tab.

   The ARM is divided into two sections. The panel on the left is the navigation panel. In this panel is a list of tools that you can create. By selecting a tool from this pane, you can create a namable portlet on the content panel on the right. You can create and move portlets around the content panel.

   The following figure is an example of the Bulk Configuration Manager tab.



# BCM tools

The Bulk Configuration Manager (BCM) has nine different tools that can be instantiated more than one time in more than one tab. These tools include the following:

- Configuration Backup and Restore
- Configuration Update Generator
- Device Password Manager
- Inventory
- Log browser
- License
- Scheduler
- Software version Updater
- Tunnel Guard Distributer

For more information about the BCM tools, see *Avaya Bulk Configuration Manager Fundamentals* (NN48021-100).

# Chapter 12: Using the Virtual Services Network Manager

The Virtual Services Network (VSN) Manager permits you to configure and view the L2 Shortest Path Bridging MAC (SPBm) and the L3 SPBm throughout the discovered network. You can use the VSN Manager for adding, deleting, and editing the L2 SPBm and the L3 SPBm across multiple devices. The VSN Manager also provides a device-centric view of the VSNs as well as a VSN-centric view of the networks. Before you launch the VSN Manager, you must install a VSN License.

The following table outlines the supported device list for the VSN Manager:

| Supported device for VSN Manager | Version |
|---|---|
| ERS 8600 | v 7.1 |

### Navigation



## VSN license

Avaya Configuration and Orchestration Manager (COM) 2.3 supports the Virtual Services Network (VSN). To use the VSN Manager and VSN Wizard, you must obtain a VSN license. For more information about obtaining a VSN license, see *Avaya Configuration and Orchestration Installation* (NN47226–300).

# Starting the VSN Manager

Perform the following procedure to start the VSN Manager.

### Procedure steps

1. In the **Configuration and Orchestration Manager** Navigation tree, expand **Managers**.
2. Click **VSN Manager**.

   The COM perfoms a discovery. After the discovery is complete, the Operation Result dialog box appears.
3. In the **Operation Result** dialog box, click **Ok**.

# Virtual Services Network Manager

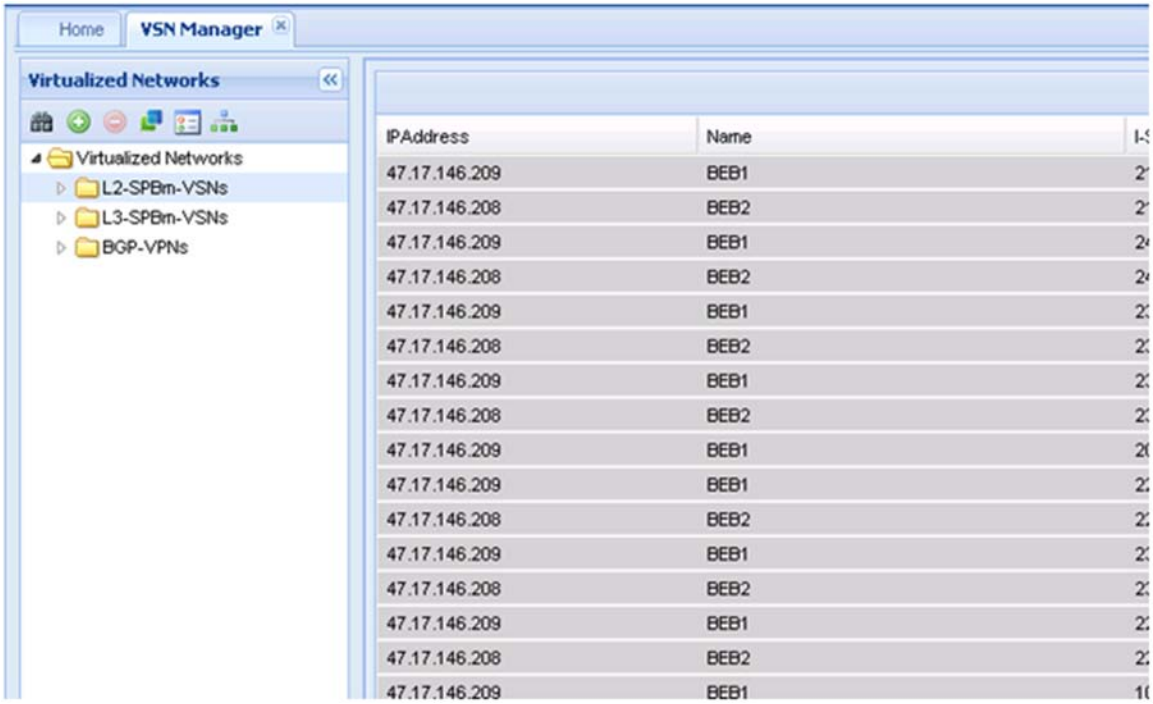
After you launch the Virtual Services Network (VSN) Manager, COM discovers all of the L2 SPBm and L3 SPBm related tables and saves the tables in the VSN Manager. After COM populates the User Interface (UI) with the discovered information, you can view or modify the configuration of the VSN Manager.

There are two VSN Manager views: VSN-centric, and device-centric. The following sections describe each view.

### VSN-centric view

The default view of the VSN Manager is the VSN-centric view of the network. The tree is organized by the VSN types discovered across all devices in the network.

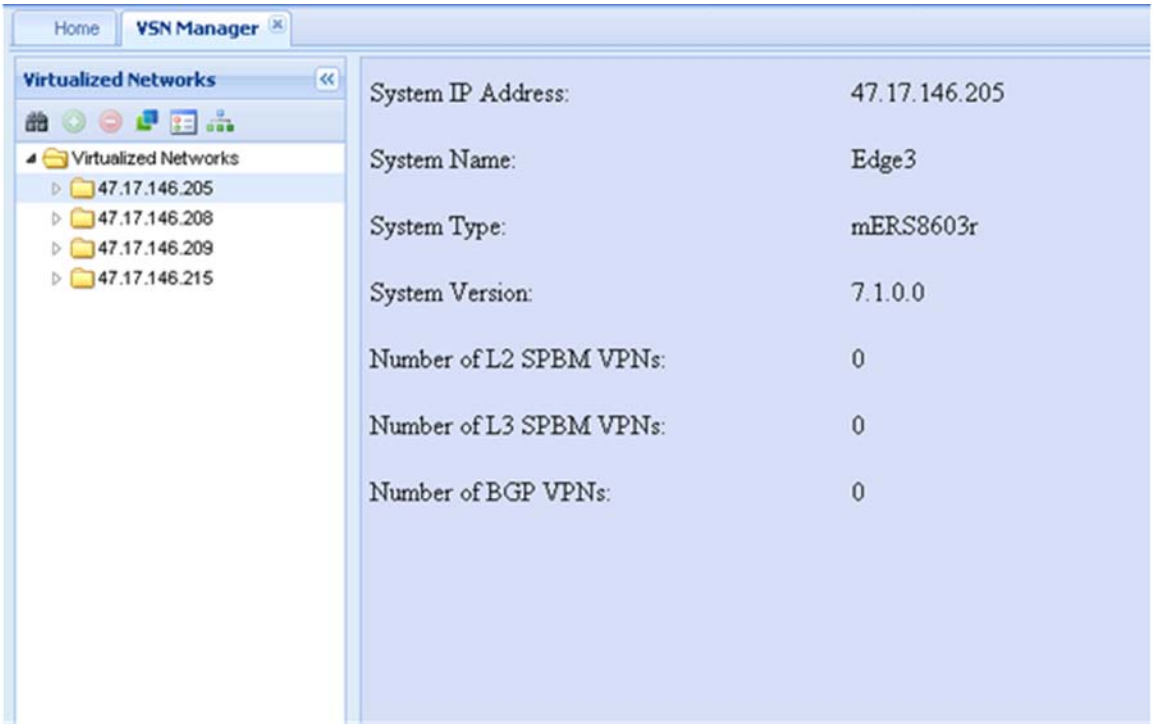
The following figure shows the VSN-centric view.




## Device-centric view

In the device-centric view of the VSN network, the tree is organized by each device in the network. The VSN types appear under each device permitting you to browse the VSNs by type, look inside each device, and browse the VSNs configured in each device.

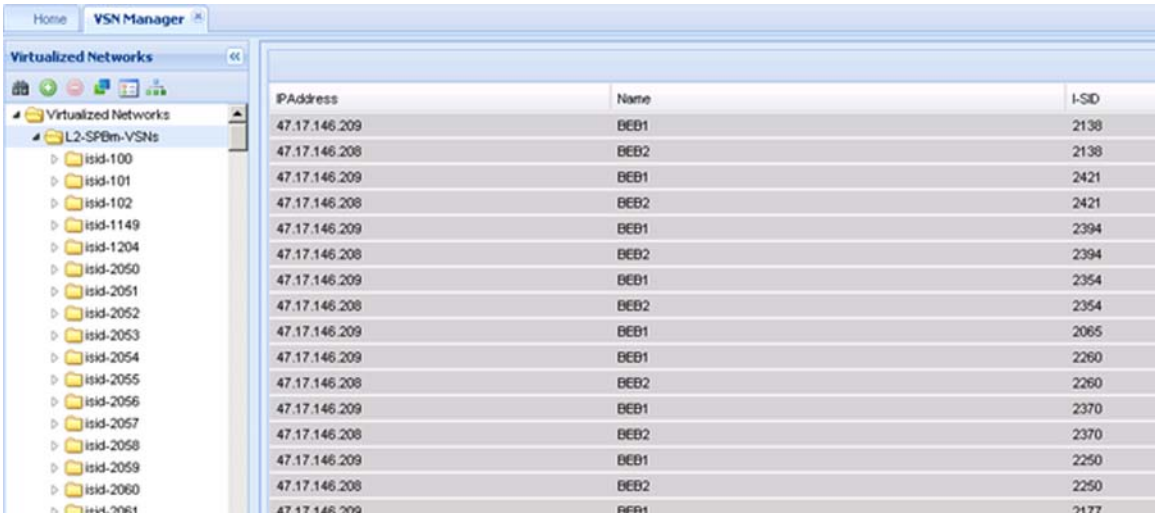
The following figure shows the device-centric view.



# L2 SPBm functionality

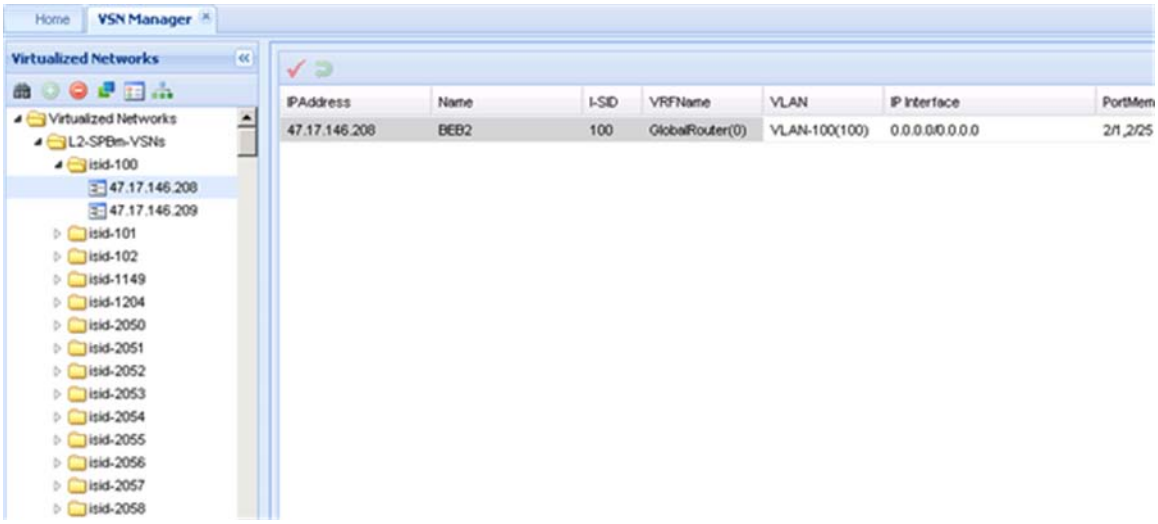
To create L2 Shortest Path Bridging MAC (SPBm) Virtual Services Networks (VSN) on a device, you must configure Intermediate System to Intermediate System (IS-IS), SPBm, and other infrastructure features. The Virtualized Services Manager (VSM) only permits you to configure the service configuration of the L2 SPBm feature, which is the mapping of a customer VLAN to an ISID, an identifier for the L2 SPBm.

The following figure shows the top level L2 SPBm view.




In the L2 SPBm view, all the discovered ISIDs appear in the tree and in the contents pane. The ISID nodes also contain all the devices that belong to a specific ISID.

The following figure is an example of the VSN Manager window showing all the devices that belong to ISID-100.




In the preceding image, a customer VLAN is mapped to the ISID-100. Only one customer VLAN is mapped to a particular ISID.

### Navigation

- Adding an L2 ISID on page 309
- Adding devices to an L2 ISID on page 310
- Deleting an ISID on page 311
- Editing L2 SPBm tables on page 311

## Adding an L2 ISID

Perform the following procedure to add an L2 ISID in the network.

### Prerequisites

You must be in the VSN-centric view.

**Note:**
The add and delete buttons are context-sensitive.

### Procedure steps

1. In the navigation pane of the **VSN Manager** VSN-centric view, select **L2-SPBm-VSNs**.
2. From the **VSN Manager** toolbar, click **Add**.

   The Device Selection page appears.
3. To move a device from the Available Devices panel to the Selected Devices panel, double-click the device name or, click the required device and then click the right-pointing arrow.

**Note:**

To remove a device from the Selected Devices list, click on the required device, and then click the left-pointing arrow.

4. Click **Select**.

   After you have select the required devices, the server discovers all the available customer VLANs (C-VLAN) that are mapped to the ISID. The UI closes the selection panel, and the Configuration page appears.

5. In the Configuration page, **ISID Number** field, type in the ISID number.
6. On top of the table, click on the sync button to sync up all the C-VLANs with the selected row.

   The Select Vlan Per Device table shows modifications for the devices that have a C-VLAN selected. For devices that do not have a selected C-VLAN, no modifications appear.

7. For the devices that remain unmodified, you can either select a different C-VLAN, or leave the devices unmodified.
8. Click **Save**.

COM updates the navigation tree.

# Adding devices to an L2 ISID

Perform the following procedure to add devices to an existing L2 ISID in the network.

### Prerequisites

You must be in the VSN-centric view.

**Note:**

The add and delete buttons are context-sensitive.

### Procedure steps

1. In the navigation pane of the **VSN Manager** VSN-centric view, select **L2-SPBm-VSNs**, and then click on the required ISID.
2. From the **VSN Manager** toolbar, click **Add**.

   The Device Selection page appears.

3. To move a device from the Available Devices panel to the Selected Devices panel, double-click the device name or, click the required device and then click the right-pointing arrow.

**Note:**

To remove a device from the Selected Devices list, click on the required device, and then click the left-pointing arrow.

4. Click **Select**.

   After you have selected the required devices, the Configuration page appears.

5. On top of the table, click on the sync button to sync up all the C-VLANs with the selected row.

   The Select Vlan Per Device table shows modifications for the devices that have a C-VLAN selected. For devices that do not have a selected C-VLAN, no modifications appear. You cannot modify the ISID number.

6. For the devices that remain unmodified, you can either select a different C-VLAN, or leave the devices unmodified.

7. Click **Save**.

COM updates the navigation tree.

## Deleting an ISID

Perform the following procedure to delete an ISID for all devices, or from a selected device.

### Prerequisites

You must be in the VSN-centric view.

**Note:**

The add and delete buttons are context-sensitive.

### Procedure steps

1. To delete the ISID for all the devices, in the navigation pane of the **VSN Manager** VSN-centric view, select a VSN type, and then select an ISID.

   Or,

   To delete the ISID from a device, in the navigation pane of the **VSN Manager** VSN-centric view, select a VSN type, select an ISID, and then select a device.

2. From the VSN Manager toolbar, click on the **Delete** button.

## Editing L2 SPBm tables

You can edit L2 Shortest Path Bridging MAC (SPBm) tables at the following two levels:

- ISID level
- Device level

### Editing L2 SPBm tables at the ISID level

After you select an ISID from the VSN Manager VSN-centric view, information on that ISID appears in a table in the contents pane. In the ISID table, you can modify the following information:

- C-VLAN for a particular ISID
- IP interface/Netmask

The C-VLAN editor is a pull down menu of all available C-VLANs on the selected device. The IP is a text field with a format of IP address/Netmask.

### Editing L2 SPBm tables at the device level

After you select a device from a specific ISID, from the VSN Manager VSN-centric view, information on that device appears in a table in the contents pane. In the table, you can modify the following information:

- C-VLAN
- IP interface/Netmask
- Port members of the particular C-VLAN

You can modify Port members of a C-VLAN.

## L3 SPBm functionality

To create L3 Shortest Path Bridging MAC (SPBm) Virtual Services Networks (VSN) on a device, you must configure Intermediate System to Intermediate System (IS-IS) data, SPBm data, CLIP interfaces, and primary and secondary SPBm BVLANs. The Virtualized Services Manager (VSM) only allows for the service configuration of the L3 SPBm feature which is the mapping of a customer VLAN (C-VLAN) to a VRF which is mapped to a L3 ISID, a number used to identify L3 VSN across a network.

The following list specifies the SPBm and ISIS infrastructure data that you must configure.

- SPBM data
    - SPBm global flag enabled
    - SPBm global state enabled
    - SPBm instance ID created
    - nick names
    - b-vid (spbm – bvlans) defined

- ip shortcuts

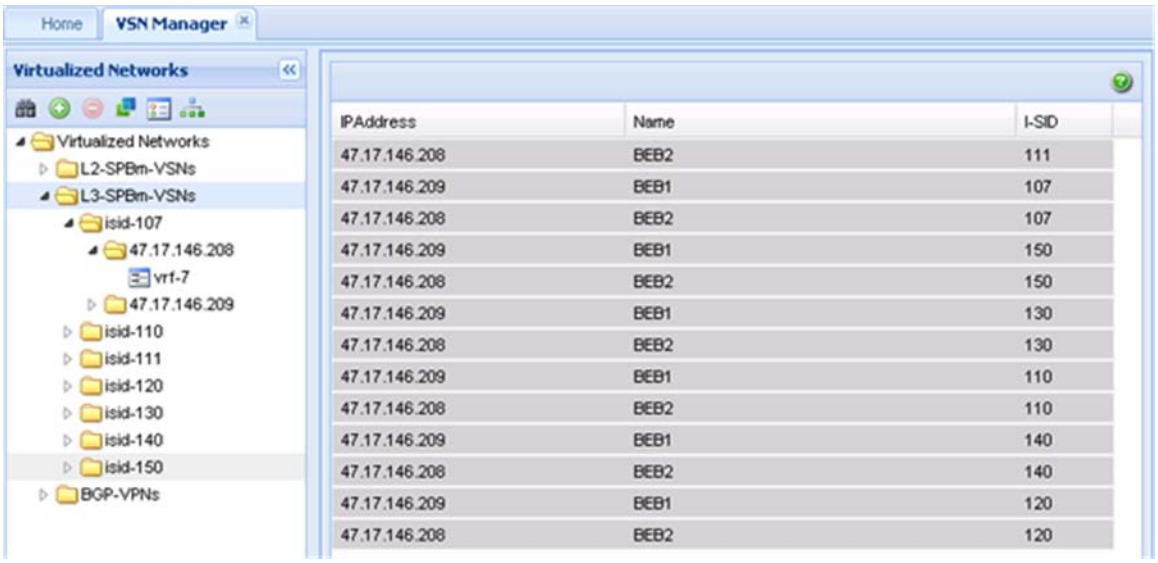
• ISIS data

- system ID
- manual area
- ip source-address
- ISIS state enabled

• CLIP interfaces

• SPBm BVLANs primary and secondary created

The following figure is an example of the L3–SPBm-VSNs screen showing all the discovered L3 SPBms in the COM network.




In the preceding image, each ISID contains a list of devices that belong to the selected ISID; and each device contains VRFs that are mapped to the selected ISID. You can modify the information by adding, deleting or editing L3 SPBms.

### Navigation


• Adding an L3 ISID on page 314

• Adding a successful L3 VPN with the VSN Wizard on page 314

• Adding a device to an L3 ISID on page 316

• Deleting an L3 ISID on page 316

• Deleting a device from an L3 ISID on page 317

• Editing L3 SPBm tables on page 317

## Adding an L3 ISID

Perform the following procedure to add an L3 ISID in the network.

### Procedure steps

1. In the navigation pane of the **VSN Manager**, select **L3–SPBm-VSNs**.
2. From the **VSN Manager** toolbar, click **Add**.

   The Device Selection page appears.
3. To move a device from the Available Devices panel to the Selected Devices panel, double-click the device name or, click the required device and then click the right-pointing arrow.

   **Note:**
   To remove a device from the Selected Devices list, click on the required device, and then click the left-pointing arrow.
4. Click **Select**.

   After you have selected the required devices, the Configuration page appears.
5. In the **ISID Number** field, type in the ISID number.
6. On top of the table, click on the sync button to sync up all the VRFs with the selected row.

   The Select VRF Per Device table shows modifications for the devices that have a VRF selected. For devices that do not have a selected VRF, no modifications appear.
7. For the devices that remain unmodified, you can either select a VRF from the pull-down menu, or leave the devices unmodified.
8. Click **Save**.

## Adding a successful L3 VPN with the VSN Wizard

Perform the following procedure to add a successful L3 VPN using the VSN Wizard.

### Procedure steps

1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizard**, and click **VSN Wizard**.

   The VSN Wizard appears.
2. In the **VSN Wizard** dialog box, select **L3 SPB Service Wizard**.
3. Click **Next**.

The Select Devices screen appears.

4. To move a device from the **Discovered Devices** list to the **Managed Devices** list, from the **Discovered Devices** list, double click on the device or select a device and click on the right pointing arrow.

   Or

   To move all devices from the **Discovered Devices** list to the **Managed Devices** list, click on the double right pointing arrows

   **Note:**
   To unselect a device, from the **Managed Devices** list , select the required item and click the left pointing arrow. To unselect all devices, click the double left pointing arrows.

5. After you select your devices, click **Next**.

   COM performs a VSN discovery, and the Operation Result box appears.

6. Click **Ok**.

   The Select ISID & VRFs screen appears.

7. Only if a new VRF is required, click **Launch VRF Manager**.

   For information about adding a new VRF, see Adding VRF on a device or multiple devices on page 296.

   If configuration of any existing VRFs is changed or new VRFs are added, click on the **VSN Wizard** tab, and click **Refresh**.

8. Only if a new VLAN is required, click **Launch VLAN Wizard**.

   For information about adding a VLAN, see Creating and configuring VLANs for an Avaya STG on page 40.

   If configuration of any existing VLANs is changed or new VLANs are added, click on the **VSN Wizard** tab, and click **Refresh**.

9. In the **ISID** field, enter the ISID number.
10. In the **VRF** column, select the VRF.
11. In the **VLAN** column, select the VLAN.
12. Optionally, in the **VLAN IP Address** and the **VLAN IP Mask** columns, type in the IP Address and Mask for the VLAN.
13. Click **Next**.

    The Confirmation screen appears.

14. Verify the generated script, and click **Finish**.
15. View L3 VPN with the VSN Manager.
    a. The ISID appears under L3 SPBm-L3-VSNs.
    b. Under the ISID, the device IP and VRF appear.

c. Click on the VRF value to view ISID, VRF, IP address, and port members.

## Adding a device to an L3 ISID

Perform the following procedure to add devices to an existing L3 ISID.

### Procedure steps

1. In the navigation pane of the **VSN Manager**, select **L3-SPBm-VSNs**, and then click on an ISID.
2. From the **VSN Manager** toolbar, click **Add**.

   The Device Selection page appears.
3. To move a device from the Available Devices panel to the Selected Devices panel, double-click the device name or, click the required device and then click the right-pointing arrow.

   **Note:**

   To remove a device from the Selected Devices list, click on the required device, and then click the left-pointing arrow.
4. Click **Select**.

   After you have selected the required devices, the Configuration page appears.
5. On top of the table, click on the sync button to sync up all the VRFs with the selected row.

   The Select VRF Per Device table shows modifications for the devices that have a VRF selected. For devices that do not have a selected VRF, no modifications appear.

   You cannot modify the ISID number, and there is no add option on the device and VRF node context.
6. Click **Save**.

## Deleting an L3 ISID

Perform the following procedure to delete an L3 ISID from all the devices.

### Procedure steps

1. From the **VSN Manager** navigation tree, select an ISID.
2. From the **VSN Manager** toolbar, click **Delete**.

## Deleting a device from an L3 ISID

Perform the following procedure to delete a device from an existing L3 ISID.

### Procedure steps

1. From the **VSN Manager** navigation pane, select **L3–SPBm-VSNs**, and select a device from an ISID.
2. From the **VSN Manager** toobar, click **Delete**.

## Editing L3 SPBm tables

You can edit the configuration of the L3 Shortest Path Bridging MAC (SPBm) on multiple levels. After you select the required ISID, the information about that ISID appears in a table in the contents pane. In the ISID table, you can modify the following information:

- VRF ID
- VLAN ID
- VLAN Port members

### Procedure steps

To modify **VLAN ID** and **IP Interface**, click **L3 ISID**.

Or

To modify **VLAN ID**, **IP Interface**, and **Port Member**, click on a device.

# BGP-VPN

In the Virtual Services Network (VSN) Manager, the BGP-VPN node exists in both the VSN-centric view and the device centric view, and presents the overall configuration of the BGP-VPNs that exists in the network and the related VRFs, Route Targets and VLANs.

The VSN-centric view permits you to create Route Targets across multiple devices, and define VPNs using new or existing Route Targets and existing VLANs and VRFs.

The device-centric view permits you to inline edit existing VPN components in the table; you can add a route distinguisher from the VRF view.

### BGP-VPN tree layout

In the VSN-centric view, the BGP-VPN node presents a list of all the VPNs defined in all the discovered devices. In the device-centric view, the BGP-VPN node only presents the VPN Route Targets assigned to the device parent node.

### Navigation


- Configuring the BGP-VPNs on page 318
- Adding a Route Target in VSN Manager on page 318
- Associating a Route Target to a VRF on page 320
- Editing BGP-VPNs on page 321
- Deleting a Route Target node on page 321


## Configuring the BGP-VPNs

To configure the BGP-VPN over IS-IS, you must add BGP global and peer settings, and you must configure the following:

1. Add a Circuitless/Loopback IP address for iBGP peering
2. Add a Circuitless/Loopback IP address for IPVPN Lite
3. Add BGP global and peers settings
4. Create a VRF with VPN as RP trigger
5. Add Route Target and add RD

The VSN Manager supports the following:

1. Add a Circuitless/Loopback IP address for iBGP peering
2. Add a Circuitless/Loopback IP address for IPVPN Lite
3. Add Route Target and add RD

## Adding a Route Target in VSN Manager

To add a Route Target in the VSN Manager, you must perform the following procedures.

1. Adding a Route Target on page 319
2. Adding a Route Distinguisher to the VRF on page 319
3. Enabling the VPN status on page 320

## Adding a Route Target

Perform the following procedure to add a Route Target to the BGP-VPN node.

### Prerequisites

You must be in the VSN-centric view of the VSN Manager.

### Procedure steps

1. In the navigation pane of the **VSN Manager**, select **BGP-VPNs**.
2. In the **VSN Manager** toolbar, click **Add**.

   The Device Selection page appears.
3. To move a device from the Available Devices panel to the Selected Devices panel, double-click the device name or, click the required device and then click the right-pointing arrow.

   **Note:**
   To remove a device from the Selected Devices list, click on the required device, and then click the left-pointing arrow.
4. Click **Select**.

   The BGP-VPN Configuration page appears.
5. Enter information in the three fields, and click **Create Route Target**.

   COM performs a discovery, and the Operation Result dialog box appears.
6. Click **Ok**.
7. At the bottom of the **BGP-VPN Configuration** page, expand on the **Add Route Target to VPN(s)**.
8. In the **Direction** column, select the direction for the devices that you added.
9. Click **Save**.

## Adding a Route Distinguisher to the VRF

Perform the following procedure to add a Route Distinguisher to the VRF.

### Prerequisites

You must be in the BGP-VPN device-centric view. To change the view from the VSN-centric view to the BGP-VPN device-centric view, in the **Virtualized Networks** tool bar, click **Toggle Device/VPN centric view**.

### Procedure steps

1. In the **Virtualized Networks** panel, select the device **VRF**.
2. From the **Virtualized Networks** tool bar, click **Add**.
3. In the **Add Route Distinguisher** dialog box, enter the appropriate information.
4. Click **Save**.

   COM performs a discovery, and the Operation Result dialog box appears.
5. Click **Ok**.

## Enabling the VPN status

After you add a Route Distinguisher to the VRF, perform the following procedure to enable the VPN status.

### Prerequisites

You must be in the VSN-centric view. To change the view from the device-centric view to the VSN-centric view, in the **Virtualized Network** tool bar, click **Toggle Device/VPN centric view**.

### Procedure steps

1. In the **Virtualized Networks** panel, select the BGP-VPN.
2. In the **VPN Status** column, select **enable**.

# Associating a Route Target to a VRF

Perform the following procedure to associate a Route Target to a VRF.

### Prerequisites

You must be in the VPN centric view of the VSN Manager.

### Procedure steps

1. In the navigation pane of the **VSN Manager**, select **BGP-VPNs**, and select the required Route Target node.
2. From the **VSN Manager** toolbar, click **Add**.

   The Device Selection page appears.

3. To move a device from the Available Devices panel to the Selected Devices panel, double-click the device name or, click the required device and then click the right-pointing arrow.

   **Note:**

   To remove a device from the Selected Devices list, click on the required device, and then click the left-pointing arrow.

4. Click **Select**.

   The Create Route Target page appears..

5. Enter the BGP-VPN for the selected devices within this route target node, and click **Create Route Target**.

   The devices you selected are filtered out if there are already BGP-VPN associated route targets created.

## Editing BGP-VPNs

You can inline edit the BGP-VPN tables in both the VSN-centric view and the Device centric view for the fields that the device permits you to edit.

You can add, delete, or modify information through dialogs that you launch by pressing the add or delete buttons on the tree panel only in the VSN-centric view.

## Deleting a Route Target node

Perform the following procedure to delete a Route Target node from the network.

**Procedure steps**

1. From the **VSN Manager** navigation tree, select **BGP-VPNs**, and select a Route Target node.
2. From the **VSN Manager** toolbar, click **Delete**.

# Device centric view

The default view on the VSN Manager is the VPN centric view. To change the view to a device centric view, on the VSN Manager toolbar, click on the **Toggle Device/VPN centric view** button.

After you change the view to the device centric view, COM restores the node that you selected during the view change. The hierarchy that appears in the VPN centric view exists in the device centric view; however in the device centric view, the hierarchy appears under each single

device. Additional components exist under each device that you can view and configure, if required.

The following sections describe components of the VSN Manager device centric view.

**Navigation**

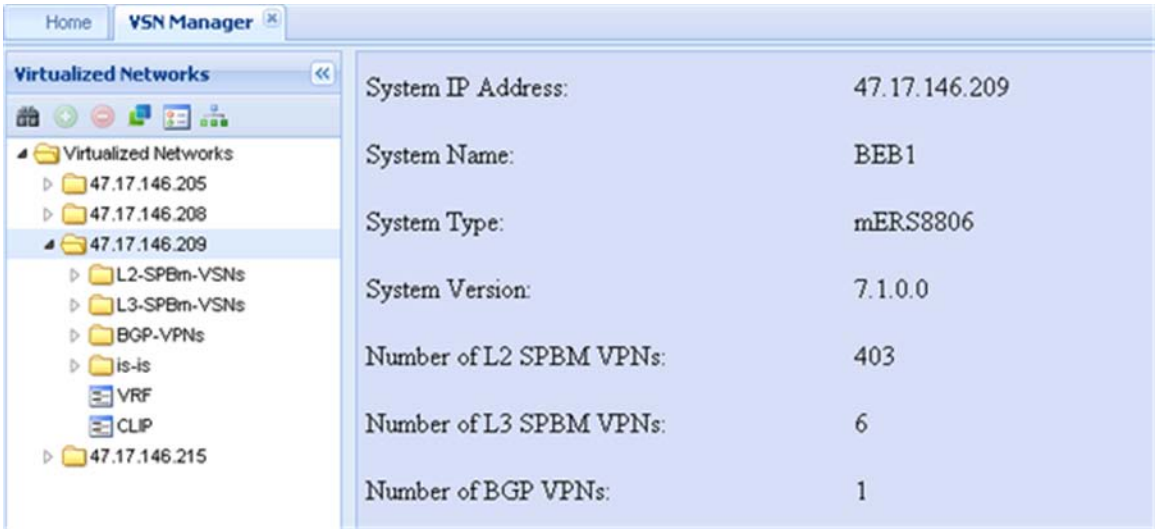


# Device node

After you select the required device node from the VSN Manager device centric view, the following device information appears in the contents pane:

- System IP Address
- System Name
- System Type
- System Version
- Number of various VSN instances configured on the device

The following figure is an example of the VSN Manager Device centric view.

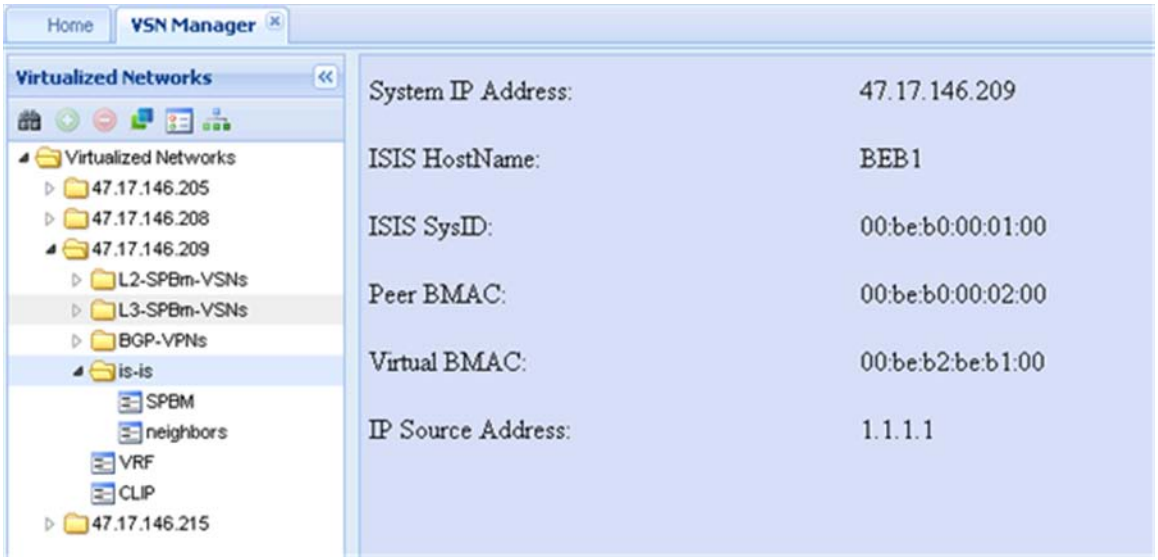


# IS-IS

After you select the is-is node from the device node, the following global IS-IS information appears in the contents pane:

- System IP Address
- ISIS HostName
- ISIS SysID
- Peer BMAC
- Virtual BMAC
- IP Source Address

The following figure is an example of the screen that appears after you select the is-is node.




The following sections describe the options under the is-is node.

- SPBM on page 323
- neighbors on page 324

## SPBM

The SPBM node exists under the is-is node and displays the Shortest Path Bridging MAC (SPBM) interfaces configured on the device.

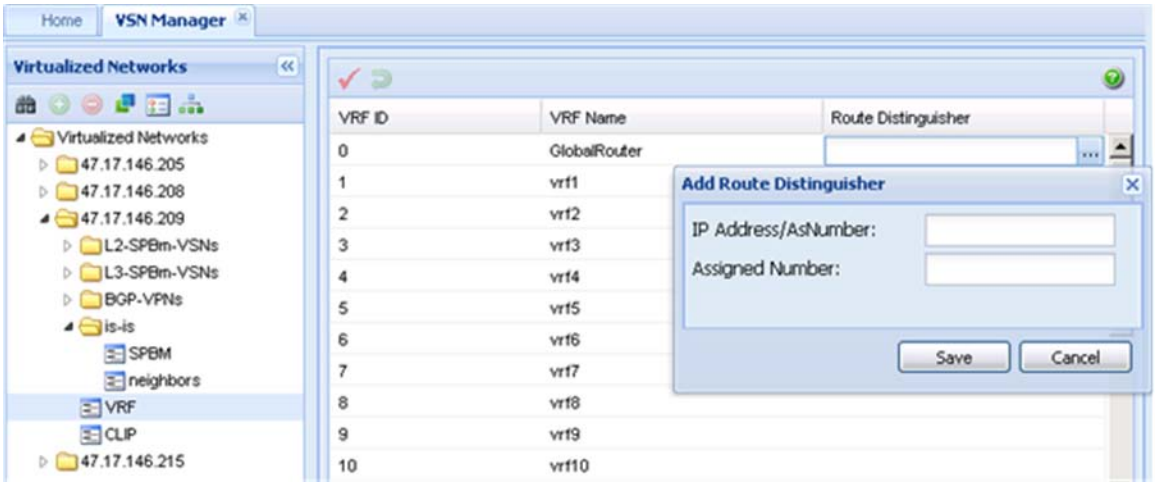
### neighbors

The neighbors node exists under the is-is node. After you select the neighbors node, the is-is adjacency table appears that lists the neighbors of the is-is interfaces on the device you selected.

## VRF table

In the VSN Manager device centric view, the VRF node appears under the device you select. After you select VRF, the VRF table appears in the contents pane and displays all the VRFs configured on the device you selected. You can configure a route distinguisher that is mapped to a particular VRF, by clicking on the Add button on the VSN Manager toolbar, or by editing the text in the Route Distinguisher column.

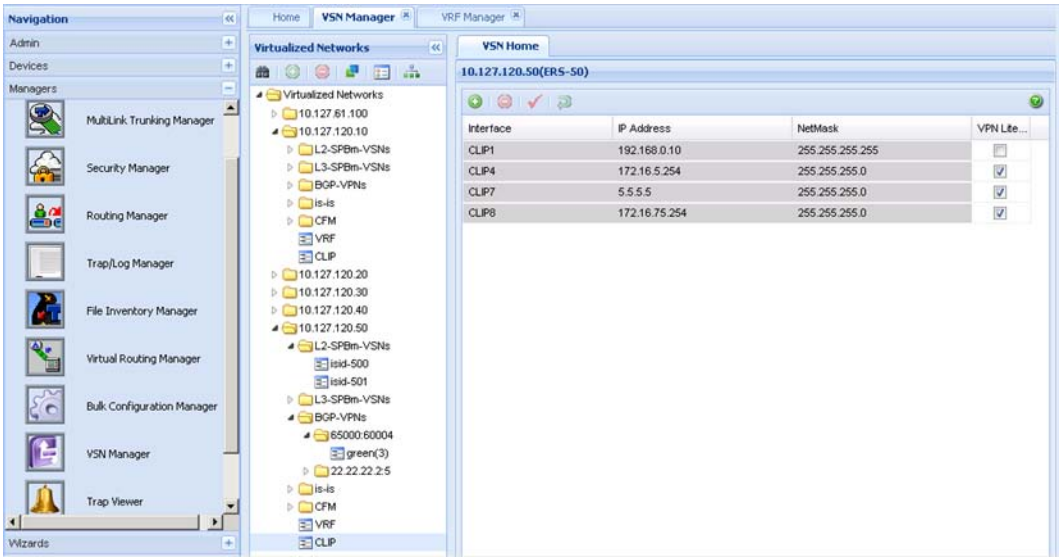
The following figure is an example of a VRF table showing the edit box for Route Distinguisher.



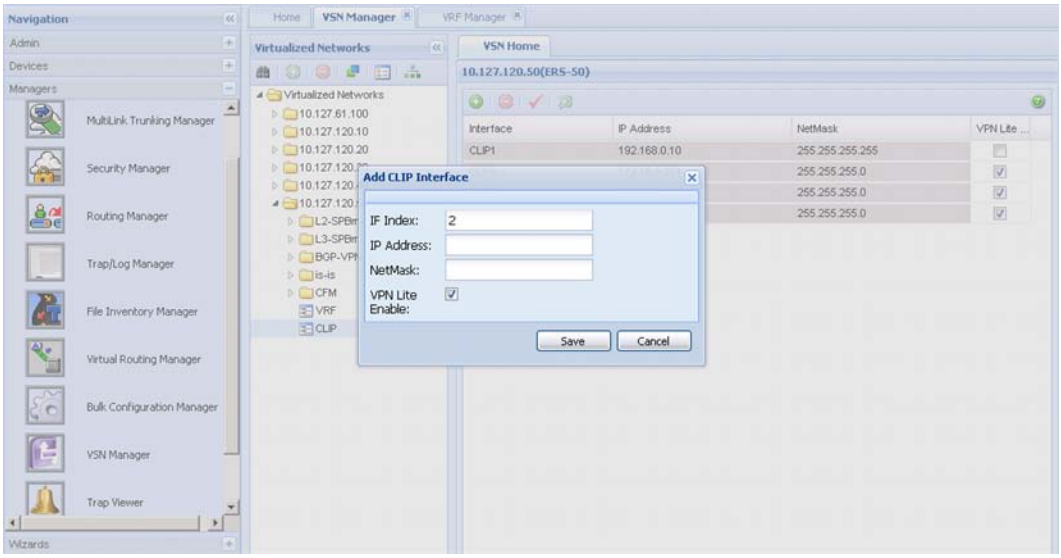

## CLIP

The CLIP node exists under the is-is node for a single device, and displays all the CLIPs configured on the device. To configure a CLIP address, on the VSN Manager toolbar, click on the add button, and enter the required fields in the Add CLIP Interface dialog box. You can also delete a CLIP address by clicking on the delete button on the Manager toolbar.

The following figure is an example of the CLIP contents pane.




The following figure is an example of the CLIP contents pane with the Add CLIP Interface dialog box.




## CFM

Connectivity Fault Management (CFM) components appear for each device, and are read-only. You can view a device configuration to help configure other devices with links to the device you are viewing, or you can view a device configuration to confirm that the CFM configuration is not the reason for a Layer 2 Ping or Trouceroute failure. You can initiate L2 Ping and Traceroutes after you launch and initiate the Enterprise Device Manager (EDM) from the device to another device in the network. The data for CFM appears in the tree, under the Global node and Maintenance Point Service node.

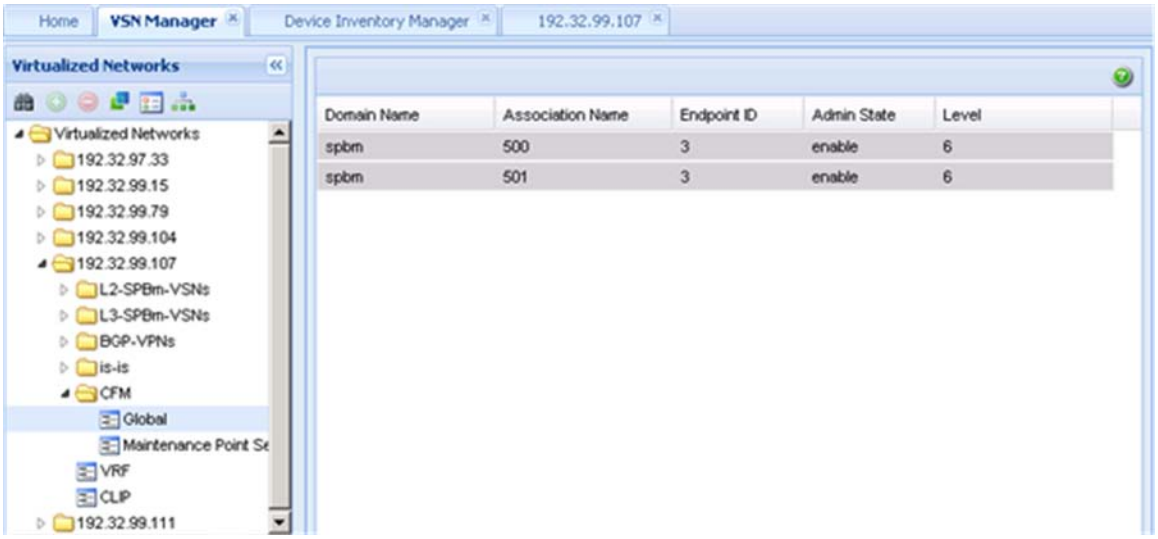
The following sections describe the Global node and the Maintenance Point Service node.


- Global on page 326
- Maintenance Point Service on page 327


## Global

After you select the Global node, the overall view of each Management Domain with Association and End Point appears in the contents pane.

The following figure is an example of a device with one Management Domain called SPBM at level 6, two Maintenance Associations that identify the VLAN id to which they are attached to, and each having an endpoint identifier of 3 that are enabled.



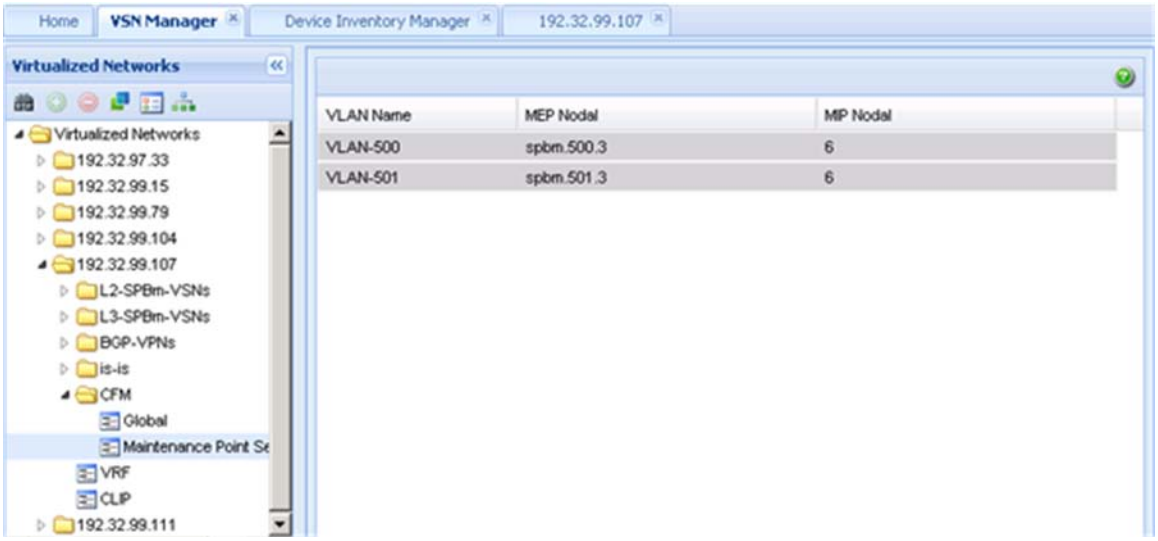

The following table describes the CFM Global table.

| Field | Description |
|---|---|
| Domain Name | Identifies the management domain of a device. |
| Association Name | Identifies the VLAN ids that are associated to the device. |
| Endpoint ID | Identifies the endpoint identifier of the VLANs that the device is associated to. |
| Admin State | Identifies whether or not the Admin State of the Maintenance End Point is enabled. The states are enable and disable. |
| Level | Identifies the level of the device management domain. |

## Maintenance Point Service

After you select the Maintenance Point Service node, a list appears that shows the VLANs that are configured as an SPBM type and are associated with CFM nodes that are listed in the Global table.

The following figure is an example of the Maintenance Point Service table.




The following table describes the CFM Maintenance Point Service table.

**Note:**

You can use EDM to configure the CFM components in the Maintenance Point Service table for each device.

| Field | Description |
|---|---|
| VLAN Name | Identifies the VLANs of the device. |
| MEP Nodal | Identifies the Maintenance End Points of the VLANs. The name of the MEP identifies the Maintenance Domain, the Association Name, and the End Point that are found in the Global table. |
| MIP Nodal | Identifies the level of the Maintenance Domain. |

# Virtual Services Network Manager SPBM

The Virtual Services Network (VSN) Manager Shortest Path Bridging MAC (SPBM) feature permits you to map and highlight SPBM meshes and trees.

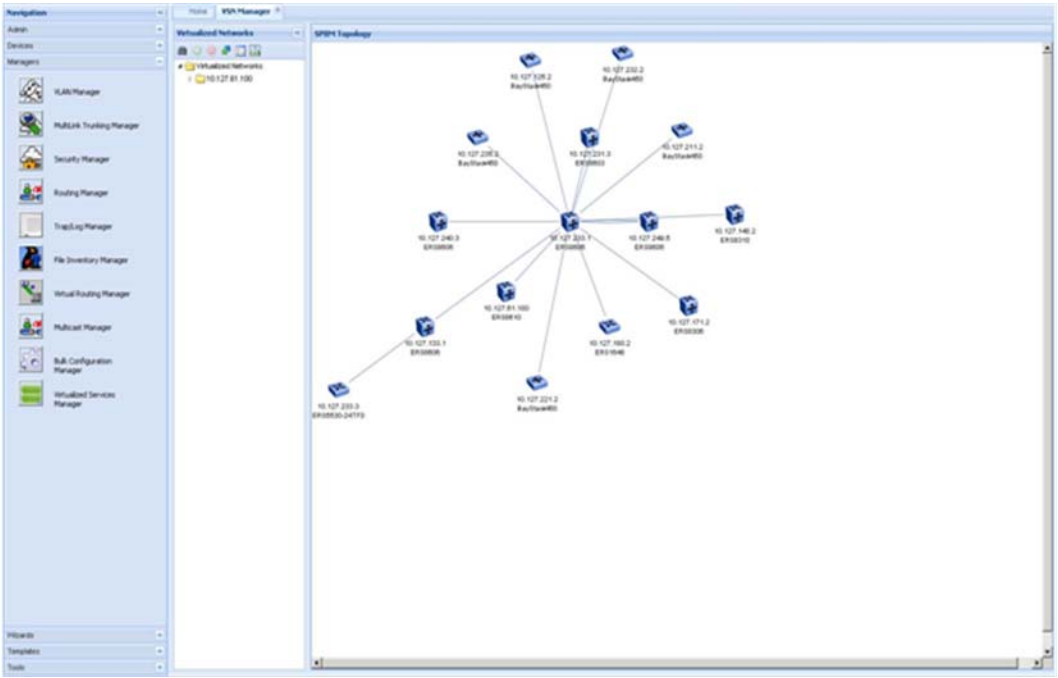
You can select the following views:

- SPBm infrastructure topology view—all IS-IS enabled devices
- All nodes tree view—generated by user device selection to show shortest path tree to all other SPM nodes
- ISID tree based view— pruned tree view to show iSIB based topology highlight over the SPBm enabled infrastructure
- Point to point view— user selection of two devices on map to show symmetric path between both nodes

The following table outlines the supported device list for the VSN Manager SPBM:

| Supported devices for VSN Manager | Version |
|---|---|
| ERS 8600 | v 7.1 |

The following figure is an example of the VSN Manager with SPBm Topology view.



### Navigation



## Generating an SPBm topology view

Perform the following procedure to generate an SPBm topology view of all ISIS enabled devices the VSN manager discovers.

### Procedure steps

1. From the **Configuration and Orchestration Manager**, select **Managers**, and then click **VSN Manager**.

   COM performs a discovery, and then the Operation Result dialog box appears.
2. Click **Ok**.
3. From the **VSN Manager** toolbar, click **Show SPBm Topology**.

   The SPBM Topology view appears in the center of the contents pane.

## Generating the shortest path view

Perform the following procedure to generate the shortest path (SP) view from the target device to all connected SPB nodes.

### Procedure steps

1. From the **Configuration and Orchestration Manager**, select **Managers**, and then click **VSN Manager**.
2. From the **VSN Manager** toolbar, click **Show SPBm Topology**.

   The SPBM topology view appears in the center of the contents pane.
3. From the topology view, right-click on a single device.
4. Select **Primary B-VLAN** or **Secondary B-VLAN**.
5. Select **Multicast Path**.

   The SP tree appears and shows the shortest path from the target device to all connected SPB nodes. The SP tree is highlighted and appears over the topology view.

## Generating an ISID view

Perform the following procedure to generate an ISID view to highlight all the devices in a particular ISID group.

### Procedure steps

1. From the **Configuration and Orchestration Manager**, select **Managers**, and then click **VSN Manager**.
2. From the **VSN Manage**r toolbar, click **Show SPBm Topology**.

   The SPBM Topology view appears in the center of the contents pane.
3. From the **Virtualized Network** panel, select an ISID group, and select the required ISID.

   All devices under the ISID you select appear in highlight on the topology map.

## Generating the L2 Ping or L2 Trace Route

In the SPBm topology, the VSN Manager displays SPBM-enabled devices only.

Perform the following procedure to generate the L2 Ping or L2 Trace Route of a device.

### Procedure steps

1. From the **Configuration and Orchestration Manager**, select **Managers**, and then click **VSN Manager**.

   COM performs a discovery, and the Operation Result dialog box appears.
2. Click **Ok**.
3. From the **VSN Manager** toolbar, click **Show SPBm Topology**.

   The SPBM Topology view appears in the center of the contents pane.
4. From the topology view, select two devices.
5. Right-click on a device, and select **Primary B-VLAN** or **Secondary B-VLAN**.
6. From the second menu, select **L2 Ping** or **L2 Trace Route**.

## Job aid

The following table describes the menu options after you right-click on a device from the SPBm topology map.

| Option | Description |
|---|---|
| Primary B-VLAN | Displays the primary VLAN map highlighting options.<br>The options are:<br>• Multicast Path<br>• Multicast Path by ISID<br>• Unicast Path<br>• Compare Unicast Path<br>• L2 Trace Route<br>• L2 Ping |
| Secondary B-VLAN | Displays the secondary VLAN map highlighting options.<br>The options are:<br>• Multicast Path<br>• Multicast Path by ISID<br>• Unicast Path<br>• Compare Unicast Path<br>• L2 Trace Route<br>• L2 Ping |
| Show Connections | Displays the connections between a device and the device neighbors. |
| Properties... | Displays the description of the device. |
| Launch Element Manager | Launches the on box element manager in a separate tab. |
| Port Status | Displays the status of all ports on a device. |
| Close | Closes the menu. |
| Multicast Path | Displays the SPF tree view; the path to all devices. |
| Multicast Path by ISID | Highlights the path from the selected device to all other members of the selected ISID group. For example, if the selected ISID is 500, COM highlights the path from the selected device to all members of the ISID group 500. |
| Unicast Path | Displays the configured Unicast path between two selected devices. |
| Compare Unicast Path | Compares the configured Unicast path defined on two selected devices. |

| Option | Description |
| --- | --- |
| L2 Trace Route | Performs an L2 Trace Route between two selected devices. |
| L2 Ping | Performs an L2 Ping between two selected devices. |

# Chapter 13: Using the Trap Viewer

The Trap Viewer is a Configuration and Orchestration Manager (COM) tool that permits you to view Traps/Notifications for devices.

### Navigation



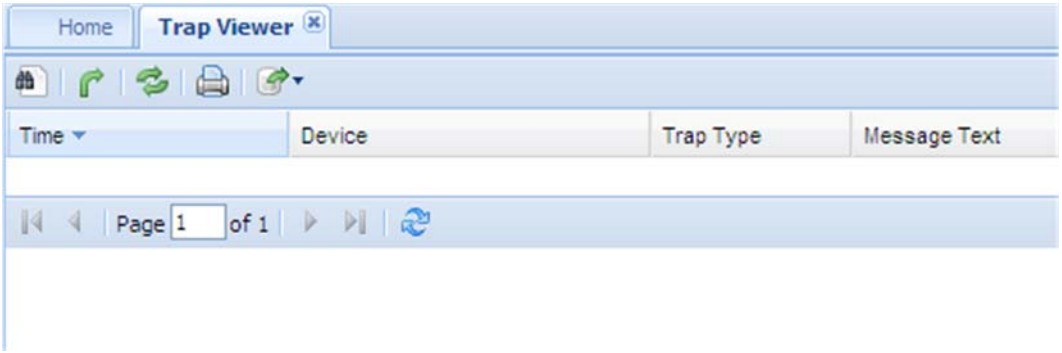
## Viewing the Trap log

Perform the following procedure to view the Trap log.

### Procedure steps

1. In the **Configuration and Orchestration Manager** Navigation tree, expand **Managers**.
2. Click **Trap Viewer**.

   The Trap Viewer window appears.




You cannot edit the cells in the Trap Viewer window.

To export information to a text file, from the **Trap Viewer** toolbar, click **Export**.

# Job aid

The following table describes the buttons in the Trap Viewer tool bar.

| Button | Description |
|---|---|
| Filter | Filters the traps based on the time traps in the system. |
| Forwarder | Permits the configuration of a trap receiver on the network so that COM can forward traps to the receivers on the list. |
| Refresh | Refreshes the traps in the table. |
| Print | Prints information on the traps. |
| Export | Exports trap information to CSV or XML formats.<br>The CSV format permits you to read the trap information in a spreadsheet.<br>The XML format permits you to read the trap information in other applications. |

# Chapter 14: Using the Syslog Viewer

The Syslog Viewer is a Configuration Orchestration Manager (COM) tool that permits you to view the system log.

**Navigation**



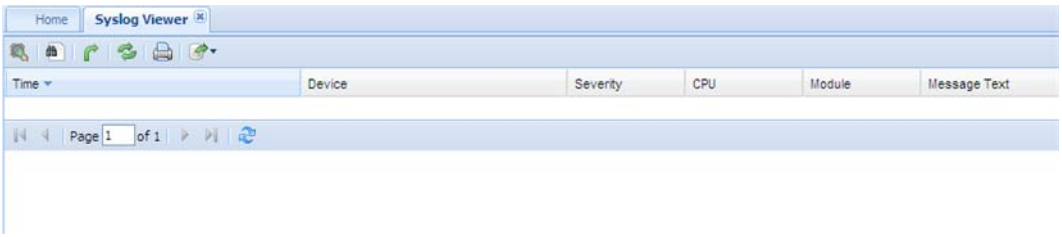
## Viewing System Log

Perform the following procedure to view the System Log.

**Procedure steps**

1. In the **Configuration Orchestration Manager** (COM), select the **Managers** panel.

   The Syslog Viewer window appears.
2. Click **Syslog Viewer**.




You cannot edit the cells in the Syslog Viewer.

To export information to a text file, in the Syslog Viewer toolbar, click **Export**.

## Job aid

The following table describes the buttons in the Syslog Viewer tool bar.

| Button | Description |
|---|---|
| Show Details | Displays more syslog message information for the message you select. |
| Show Filter | Filters the traps based on the time traps in the system. |
| Forwarder | Permits the configuration of a trap receiver on the network so that COM can forward traps to the receivers on the list. |
| Refresh | Refreshes the traps in the table. |
| Print | Prints information on the traps. |
| Export | Exports trap information to CSV or XML formats.<br>The CSV format permits you to read the trap information in a spreadsheet.<br>The XML format permits you to read the trap information in other applications. |

# Chapter 15: Configuration of devices

Device Inventory Manager enables you to manage the Configuration and Orchestration Manager (COM) inventory.

### Navigation

[Device Inventory interface](#) on page 337

## Device Inventory interface

This section details the Device Inventory Manager interface as shown in the following figure.

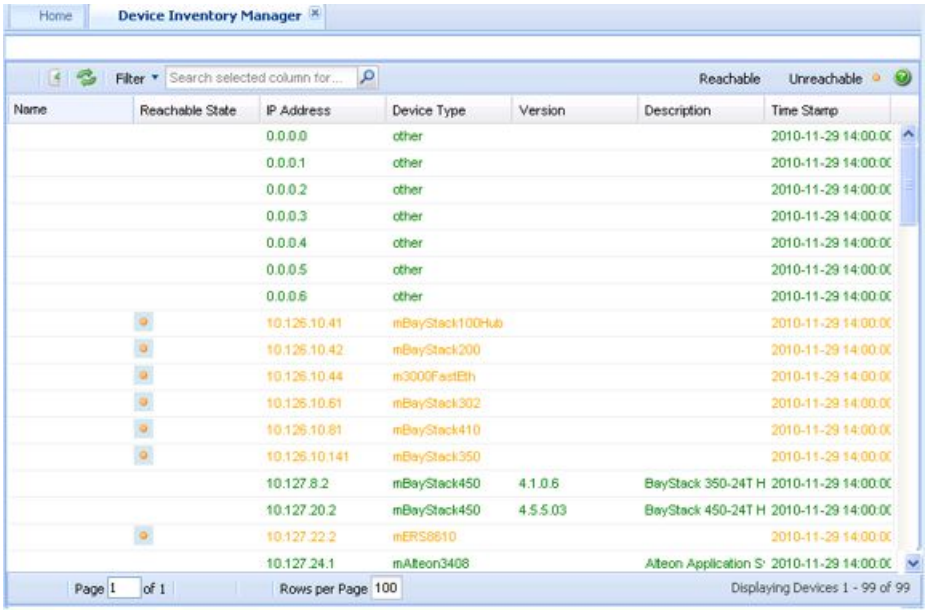



**Figure 29: Device Inventory interface**

The following table describes the parts of the device inventory interface.

**Table 102: Device inventory parts**

| Command | Toolbar button | Description |
|---|---|---|
| Launch Element Manager |  | Opens a new web page with the Element Manager for a device. |

| Command | Toolbar button | Description |
|---|---|---|
| Add |  | Opens the Insert dialog box, where you can manually add a device to the inventory. |
| Edit |  | Edit a device from the inventory. |
| Delete |  | Deletes the selected VRF from a specific device. |
| Import/Export inventory |  | Imports/Exports the inventory from/to a XML file. |
| Refresh |  | Refreshes the Device Inventory information. |
| Filter |  | Filters the inventory view based on the IP address or device type. |

**Important:**

The Add, Delete, and Edit buttons are displayed only in COM software with basic license.

### Navigation

- Viewing a device inventory manager on page 338
- Launching an Element Manager on page 339
- Importing devices on page 341
- Exporting devices on page 342

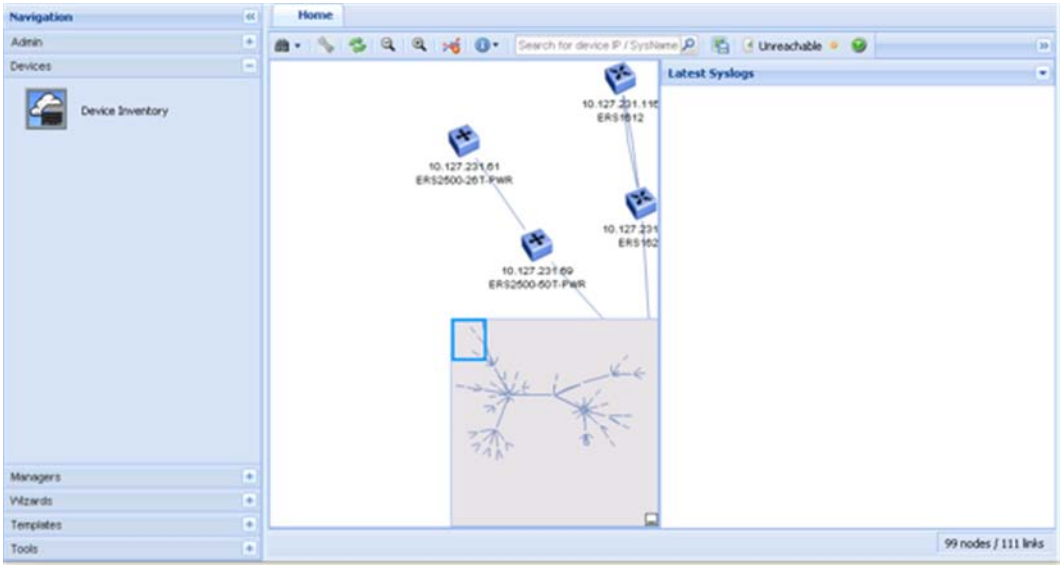
# Viewing a device inventory manager

Perform the following procedure to view a device inventory manager.

### Procedure steps

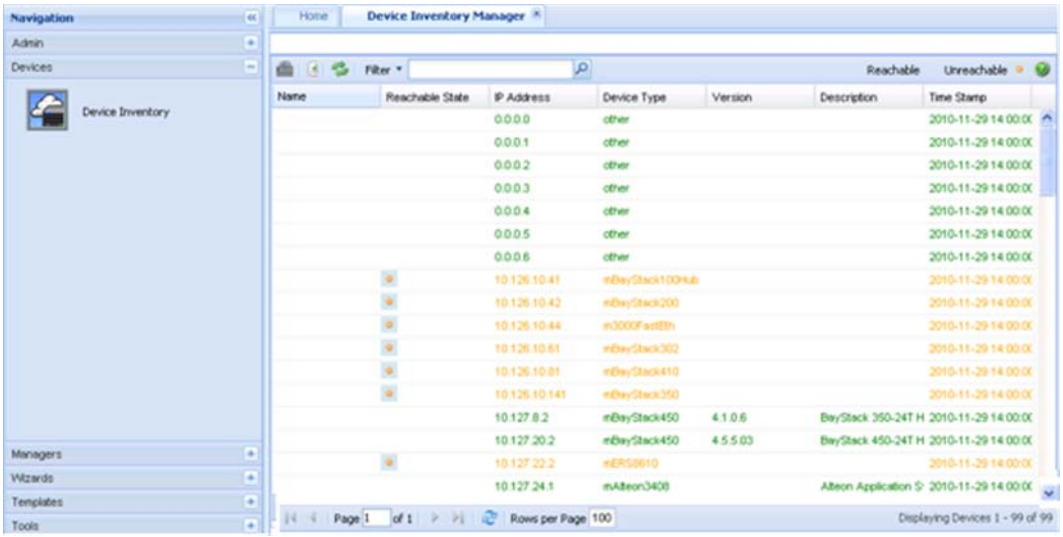
1. From the **Configuration and Orchestration Manager Navigation** pane, select **Devices**.

   The Devices panel appears.




2. From the **Devices** panel, click **Device Inventory** icon.

   The Device Inventory Manager dialog box appears.




# Launching an Element Manager

Perform the following procedure to launch an element manager.

### Procedure steps

From the **Configuration and Orchestration Manager** topology view, right-click on a device.

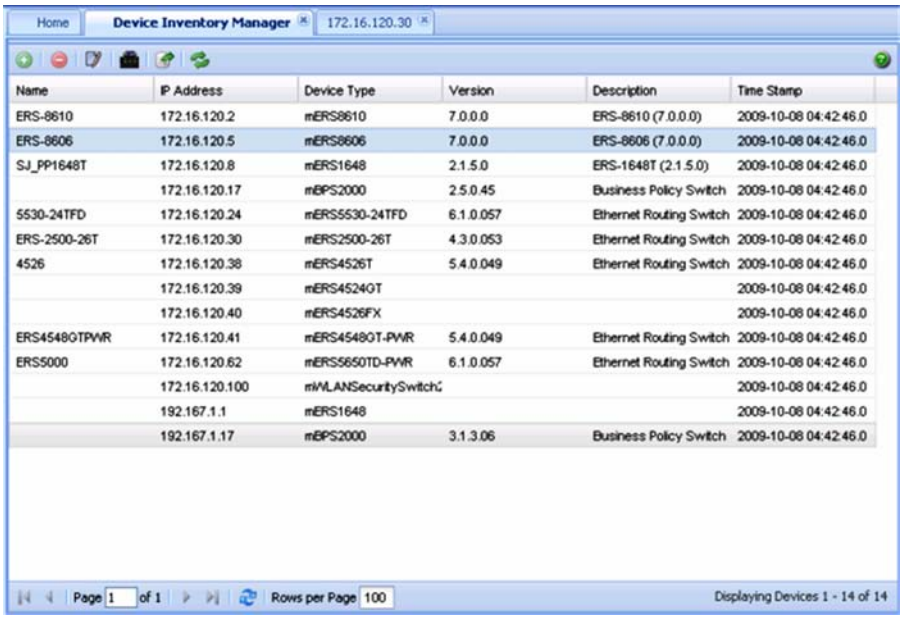
Select **Launch Element Manager**.

Or

From the **Configuration and Orchestration Manager** navigation pane, select **Devices**.

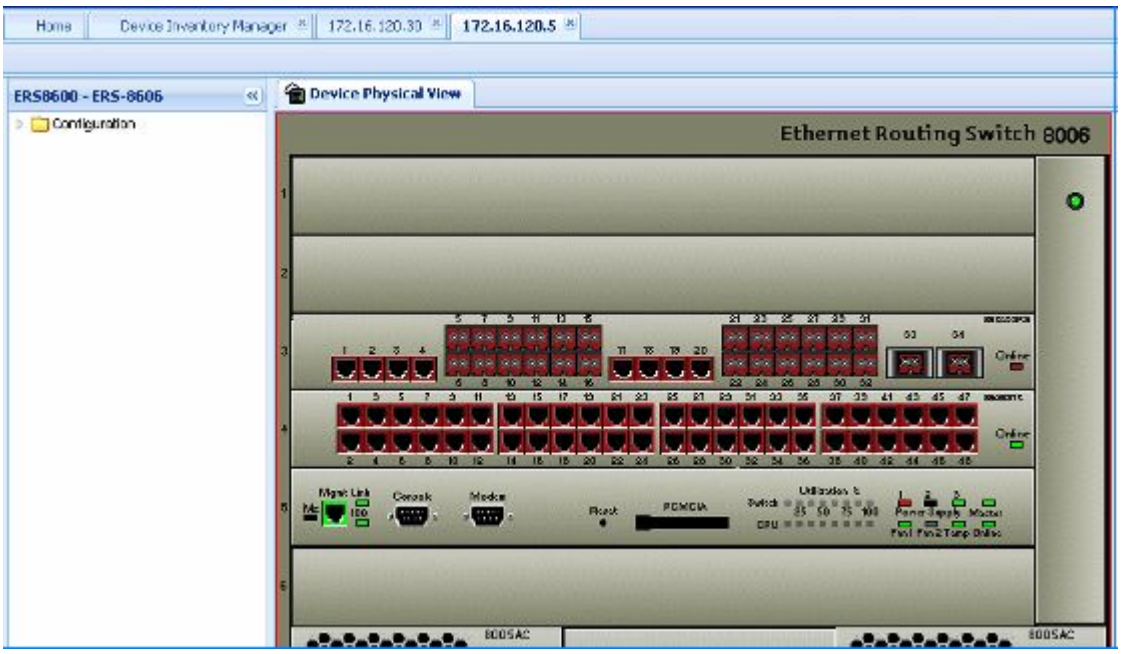
a. Click **Device Inventory**.

b. Select a device from the Device table.




c. From the **Device Inventory Manager** toolbar, click the **Launch Element Manager** icon.

The corresponding Device Physical View tab appears.




**Important:**

If you select a device that does not support EDM, then by default the Java Device Manager (JDM) of the corresponding device opens up. If Java Virtual Machine (JVM)1.6 application is not already installed in your system, the COM application prompts you to install the application.

# Importing devices

Perform the following procedure to import an inventory from the XML file.

### Procedure steps

1. From the **Configuration and Orchestration Manager** topology view, click on a device.

   From the topology view tool bar, select **Import/Export topology**.

   Or

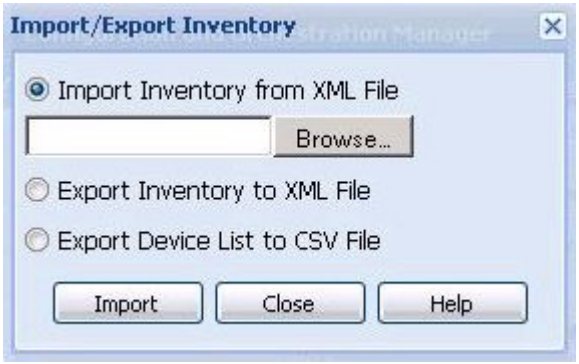
   From the **Configuration and Orchestration Manager** navigation panel, select **Devices**.

   a. Click **Device Inventory**.

   b. Select a device from the Device table.

   c. From the **Device Inventory Manager** toolbar, press the **Import/Export Inventory** button.

The Import/Export Inventory dialog box appears.




2. Click the **Browse** button to select the path of the .xml file.
3. Click **Import**. The COM imports the devices and auto refreshes the inventory table.

# Exporting devices

Perform the following procedure to export an inventory to the XML file, or to export a device list to the CSV File..

### Procedure steps

1. From the **Configuration and Orchestration Manager** topology view, click on a device.

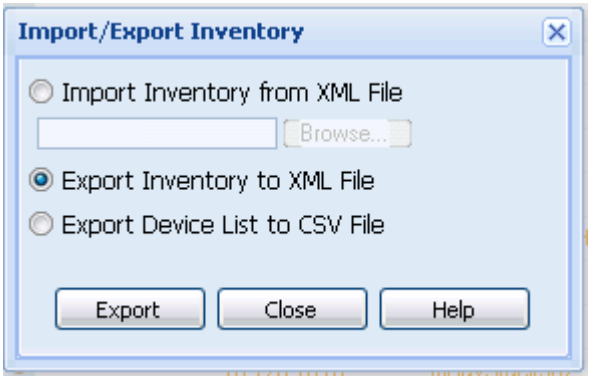
   From the topology view tool bar, select **Import/Export topology**.

   Or

   From the **Configuration and Orchestration Manager** navigation panel, select **Devices**.

   a. Click **Device Inventory**.
   b. Select a device from the Device table.
   c. From the **Device Inventory Manager** toolbar, press the **Import/Export Inventory** button.

   The Import/Export Inventory dialog box appears.




2. Select **Export Inventory to XML File**, or **Export Device List to CSV File**.
3. Click **Export** .

# Chapter 16: Configuration of wizards

Configuration and Orchestration Manager (COM) configuration wizards help you to configure complex network by using few steps. These wizards hide the network complexity and make multi device configuration easier and simple.

**Navigation**



## VLAN wizard

VLAN wizard has the following two sections as shown in the following figure:

- Steps—shows the current wizard step
- Wizard Description—shows the wizard description of current step

While running the wizard, you can select to save the wizard configuration as a template at any point. You can save it as a new template, or update an existing template. The access control of wizards depends on the specific Multi Element Manager. For example, if you have access to VLAN Manager, then you can also run VLAN Wizard. Similarly, the users who have access to Mulitlink Trunking Manager can also run SMLT Wizard.

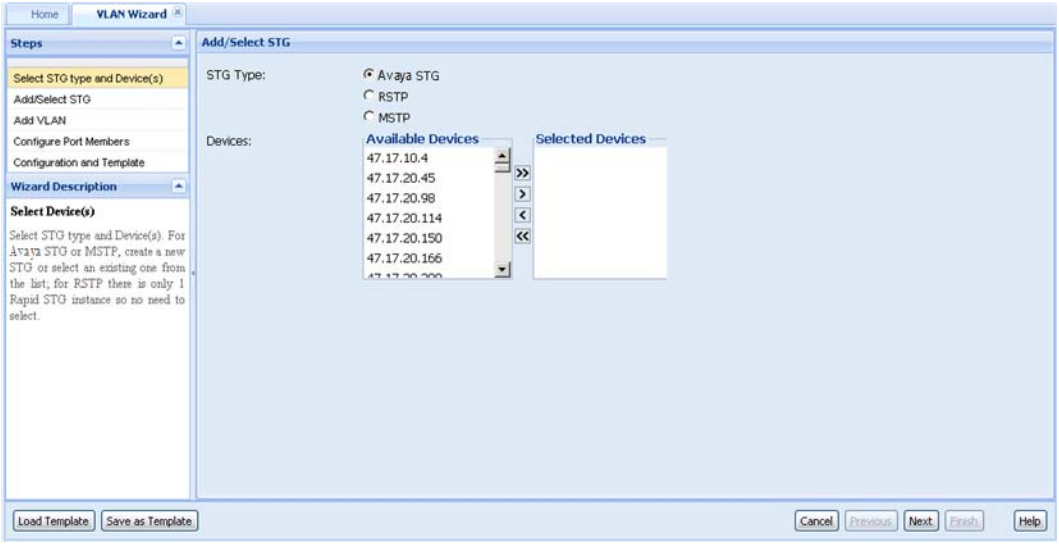



**Figure 30: VLAN Wizard**

### Navigation

- VLAN wizard functionality on page 346
- VLAN Wizard on page 347
- Loading a template on page 352
- Saving as template on page 353

## VLAN wizard functionality

VLAN wizard is used to configure spanning tree groups (STG) and VLAN in multiple devices. Following are the VLAN wizard functionalities:

- Select STG type and Device(s)
- Add/select an STG
- Add one or multiple VLANs
- Configure Port members
- Configuration and template

VLAN wizard can run in a standalone mode. The VLAN data which is used in VLAN wizard can be created on fly or loaded from a VLAN template.

The following table describes the buttons available on VLAN wizard.

**Table 103: VLAN wizard buttons**

| Button | Description |
|---|---|
| Load Template | Allows you to upload the data from a saved template. |
| Save as Template | Allows you to save the current data as a template. |
| Cancel | Allows you to cancel the current step. |
| Previous | Allows you to move to the previous step. |
| Next | Allows you to move to the next step. |
| Finish | Allows you to finish the current step. |
| Help | Opens Online Help file. |

# VLAN Wizard

Perform the following procedures, in the order listed below, to use the VLAN Wizard.

- Selecting STG type and devices on page 347
- Adding or selecting an STG on page 348
- Adding a VLAN on page 349
- Configuring port members on page 350
- Saving the VLAN configuration on page 351

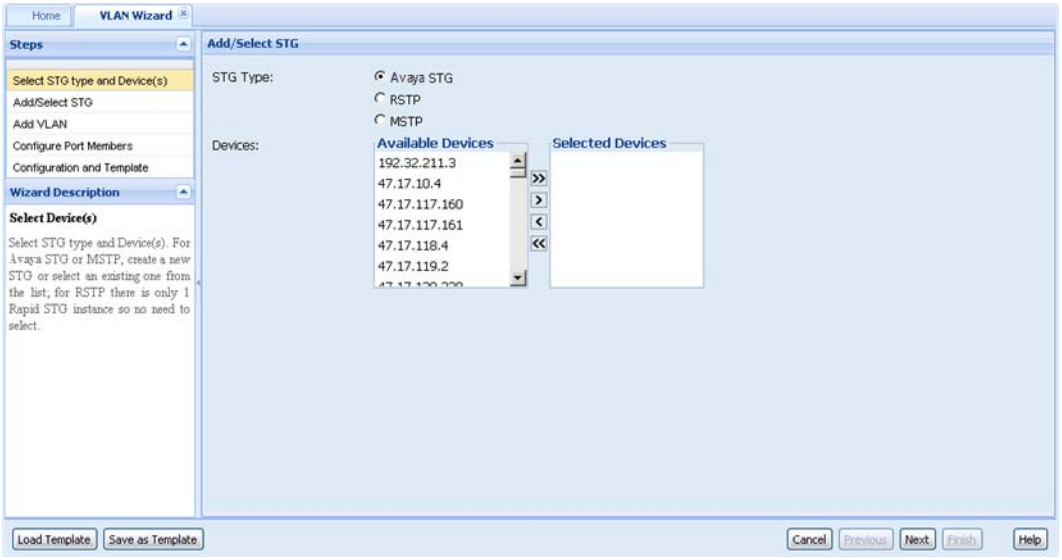
# Selecting STG type and devices

Perform the following procedure to select an STG type and devices.

### Procedure steps

1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizards**, and then click **VLAN Wizard**.

   The VLAN Wizard dialog box appears.




2. In the Add/Select STG dialog box, select the STG type.
3. Select the devices.
4. To move to the Add/Select STG page, click **Next**.

## Adding or selecting an STG

Perform the following procedure to add or select an STG in the VLAN wizard.

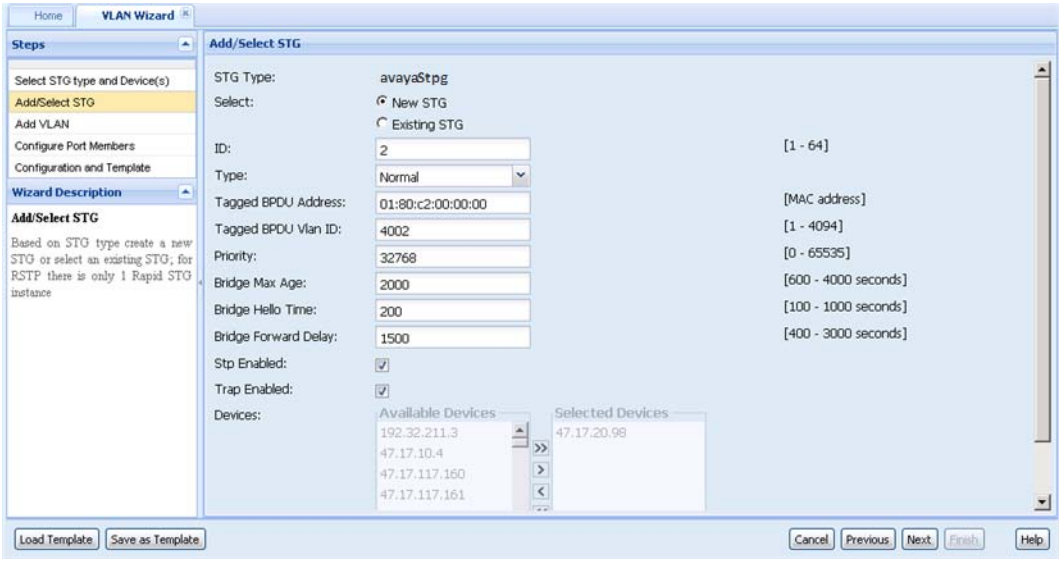
### Prerequisites

- In the Configuration and Orchestration Manager (COM) select VLAN Wizard.
- Perform the procedure for selecting STG type and devices.

### Procedure steps

1. In the **Add/Select STG** dialog box perform one of the following actions:
   - To add a new STG, choose **New STG** in the **Select** field.

     **OR**
   - To select an exiting STG, choose **Existing STG** in the **Select** field.




2. Enter appropriate values in all the fields, and then click **Next** to move on Add VLAN page.

## Adding a VLAN

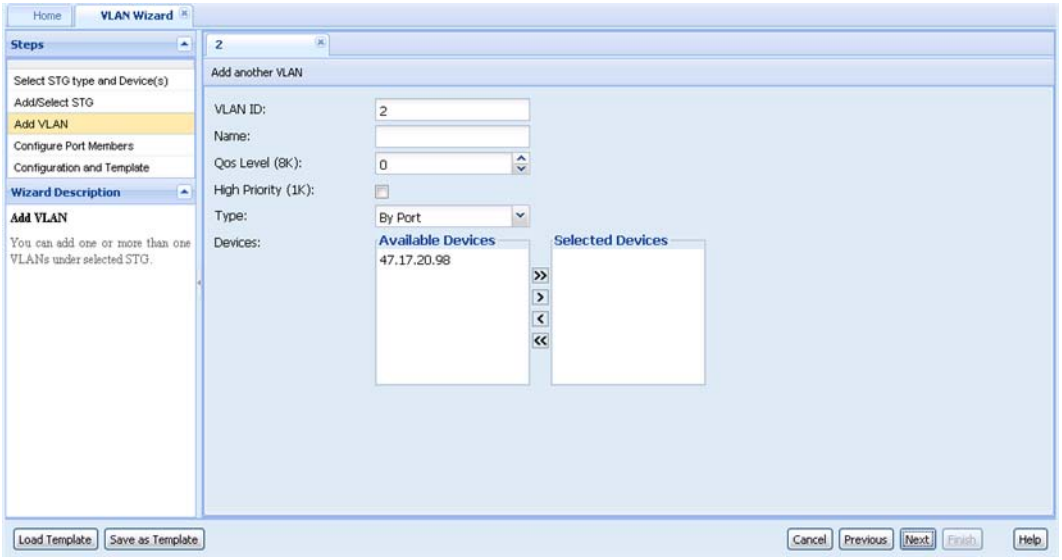
Perform the following procedure to add a VLAN in the wizard.

### Prerequisites

- In the Configuration and Orchestration Manager (COM), select VLAN Wizard.
- Perform the procedure for selecting STG type and devices.
- Perform the procedure for adding or selecting an STG.

### Procedure steps

1. In the **Add VLAN** page, enter information in all the fields to add a VLAN in the wizard.




2. Choose the devices you wish to add from the **Available Devices** list, and then click the right-pointing arrow to move the devices to the **Selected Devices** list.
3. Click **Add another VLAN** to add more VLANs. Repeat steps 3 and 4 as necessary.
4. Click **Next** to move on Configure Port Members page.

# Configuring port members

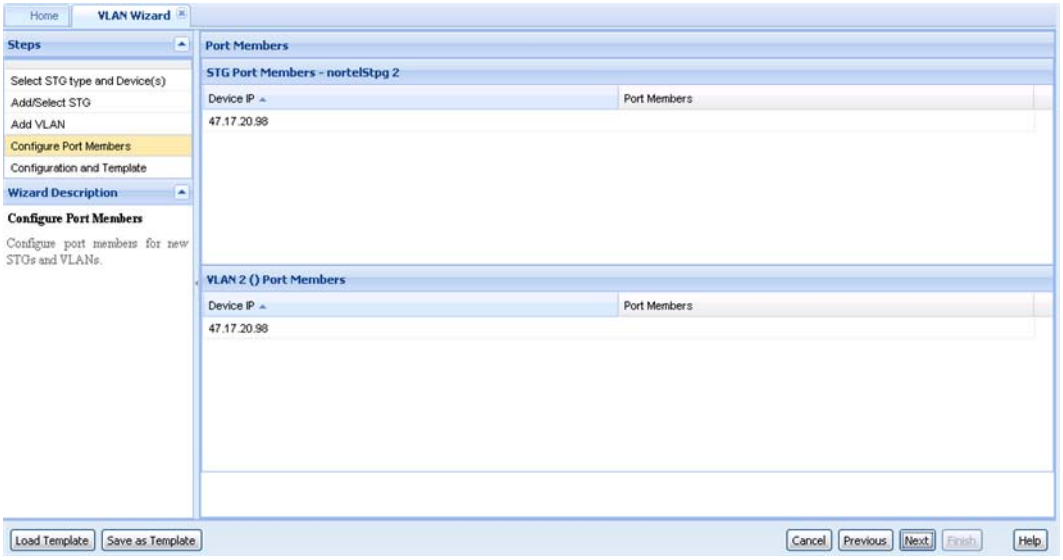
Perform the following procedure to view the configured port members.

### Prerequisites

- In the Configuration and Orchestration Manager (COM), select VLAN Wizard.
- Perform the procedure for selecting STG type and devices.
- Perform the procedure for adding or selecting an STG.
- Perform the procedure for adding a VLAN.

### Procedure steps

In the Configure Port Members page, click **Next** to move to the Configuration and Template page.




## Saving the VLAN configuration

Perform the following procedure to save the configuration as a template.

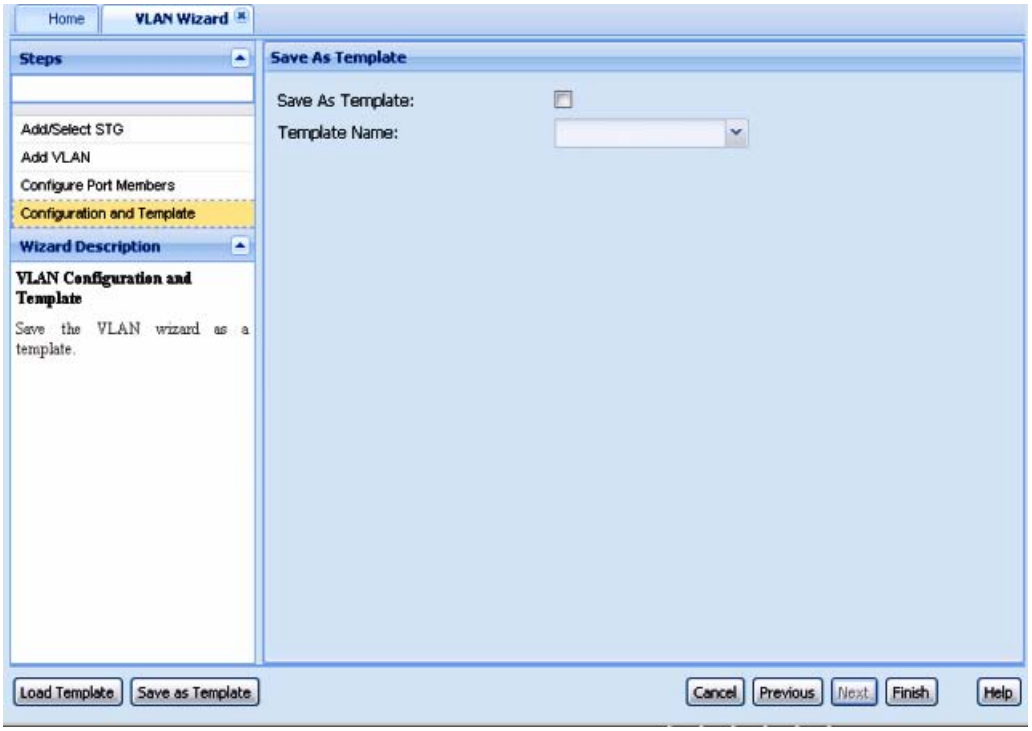
### Procedure steps

1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizards**, and then click the **VLAN Wizard** icon.

   The VLAN Wizard dialog box appears.

2. In Configure Port Members page, click **Next** to move on Configuration and Template page.

   The Configuration and Template page appears.




3. Select the **Save As Template** check box to save the configuration as a template.
4. Enter the name of the template file in **Template Name** field, and then click **Finish**.

   The result of VLAN wizard configuration appears.

## Loading a template

Perform the following procedure to load a template.

### Procedure steps

1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizards**, and then click the **VLAN Wizard** icon.

   The VLAN Wizard dialog box appears.
2. Click **Load Template**.

   The Please select a template to load into the wizard dialog box appears.


3. Enter the name of the template file in **Template Name** field, and then click **Load** to load the selected template.

## Saving as template

Perform the following procedure to save the current configuration as template.

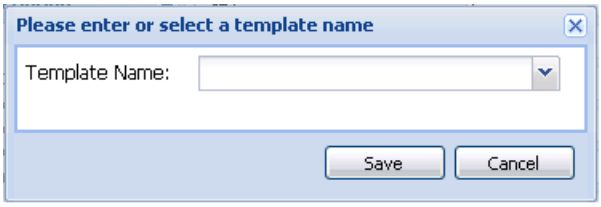
### Procedure steps

1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizards**, and then click the **VLAN Wizard** icon.

   The VLAN Wizard dialog box appears.

2. Click **Save as Template**.

   The Please enter or select a template name dialog box appears.




3. Enter the name of the template file in **Template Name** field, and then click **Save** to save the current configuration as template.

# SMLT wizard

The SMLT wizard is a simplified and workflow driven wizard in the Configuration and Orchestration Manager interface. The Wizard walks you through various trunk configuration, and simplifies the steps involved in the SMLT setup. It helps in reducing the complexity. Using this feature, you can configure as a single workflow.

The SMLT wizard appears different for the VSP 9000 devices because there is no SMLT ID, and VSP 9000 supports the NNCLI. If you are required to create a SMLT ID for a VSP 9000 device, you must enter a MLT ID. VSP 9000 devices can only be configured together, without a mix of devices, because the new SMLT protocol does not work across 8600 and 9000 devices.

For more information about the SMLT configuration wizard, see the following sections.

**Navigation**


- SMLT wizard functionality on page 354
- Launching SMLT Wizard on page 354


## SMLT wizard functionality

The SMLT Wizard helps you to create various trunk configurations like, VLANs creation, protocol enabling and miscellaneous device settings. The SMLT wizard functions are divided in to three steps:

- Selecting the device type and the targeted devices—represents the current supported device types, retrieves those devices from the inventory, and assigns to a current user.
- Creating interswitch trunking (IST)—provides the necessary Inter-Switch Trunk configuration to define SMLT Topology Objects (Triangles).
- Creating SMLT/SLT—helps you to create multiple trunks on the selected devices. The selections can be saved into a template, and reused if necessary.

SMLT configuration wizard has the following advantages over manual configuration:

- efficient configuration
- higher consistency of configuration
- consistent and easy CLI commands and steps across devices
- configures as a single workflow
- ability to save and restore configuration
- ability to apply the configuration to devices and view results

## Launching SMLT Wizard

The screens given in the procedure are not the latest one. The updated screens will be provided in the subsequent release.

Perform the following procedure to launch the SMLT Wizard.

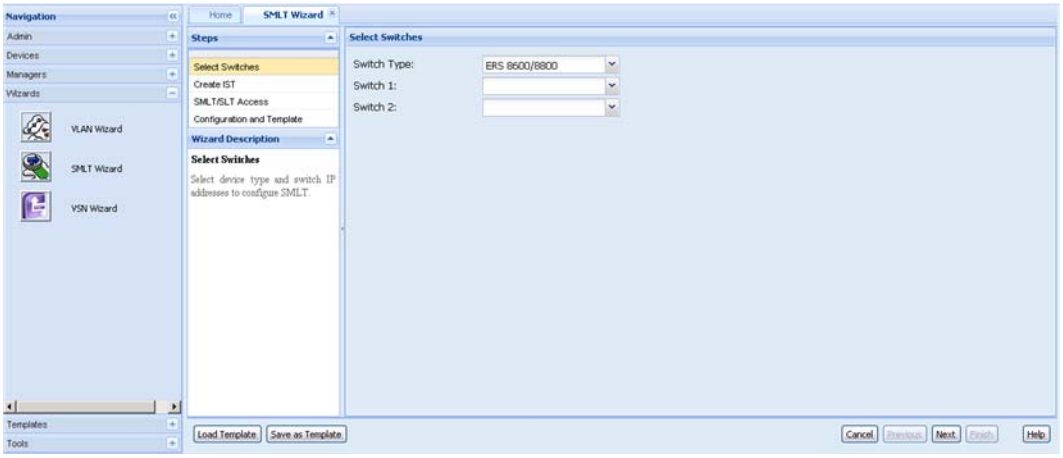
**Note:**

For VSP 9000 devices, there is no SMLT ID. To create a SMLT for VSP 9000 devices, you must enter a MLT ID. VSP 9000 supports the NNCLI.

## Procedure steps

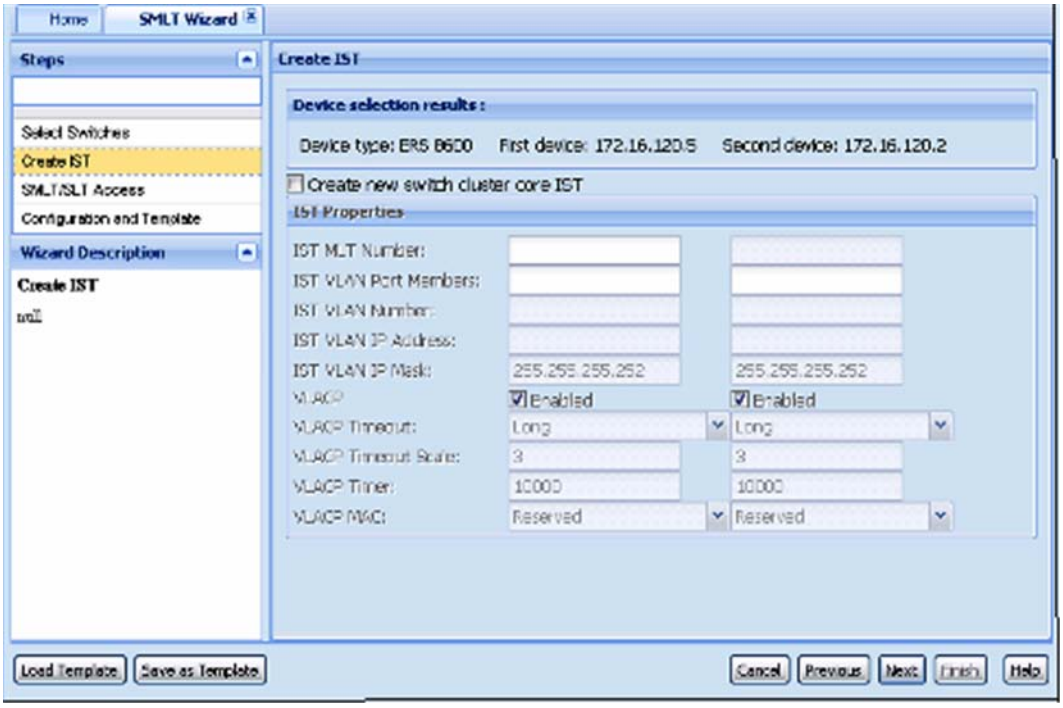
1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizards**, and then click the **SMLT Wizard** icon.

   The SMLT Wizard dialog box appears.




2. Choose the type of the switch from **Switch Type** field.
3. Choose the **Switch 1** and **Switch 2** from the drop down lists provided.
4. Click **Next**.

   The Create IST dialog box appears.




5. Select the **Create new switch cluster core IST** check box.

6. Enter the values for creating the IST in the fields provided.

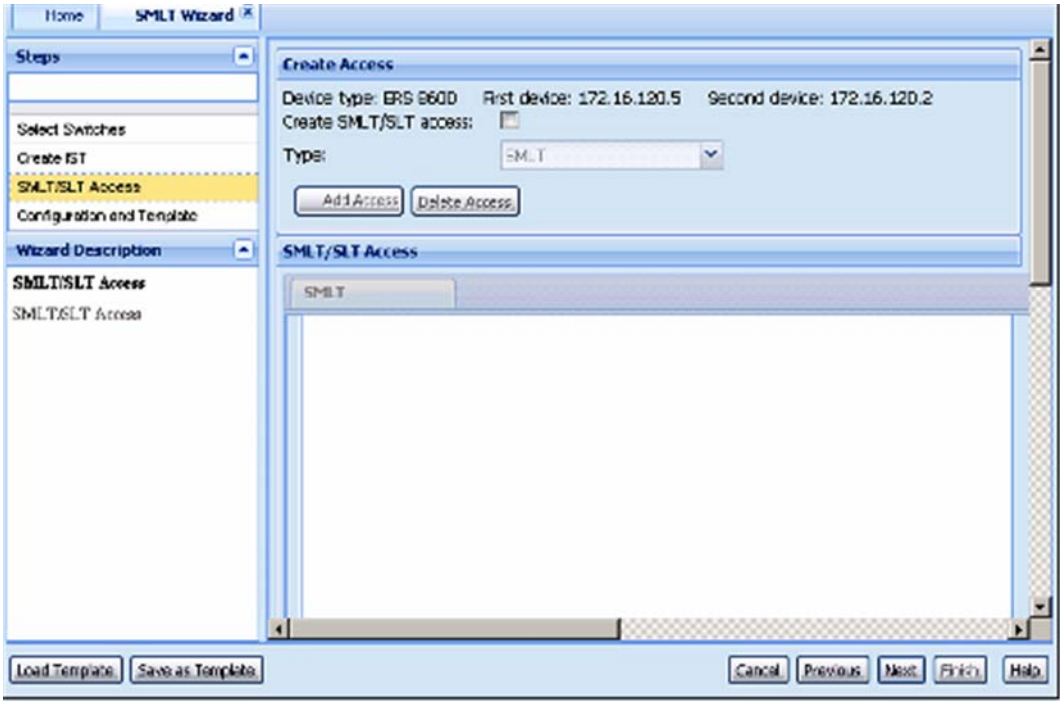
   Some of the fields are common for both the switches. For the second switch, the value of the common fields are filled automatically as you enter the value for the first switch.

   **Important:**

   Prepopulated values are available in some fields.

7. Click **Next**.

   The SMLT/SLT access dialog box appears.




8. Select the **Create SMLT/SLT access** check box , choose the access type from the **Type** list, and then click **Add Access** to provide access to a new SMLT.

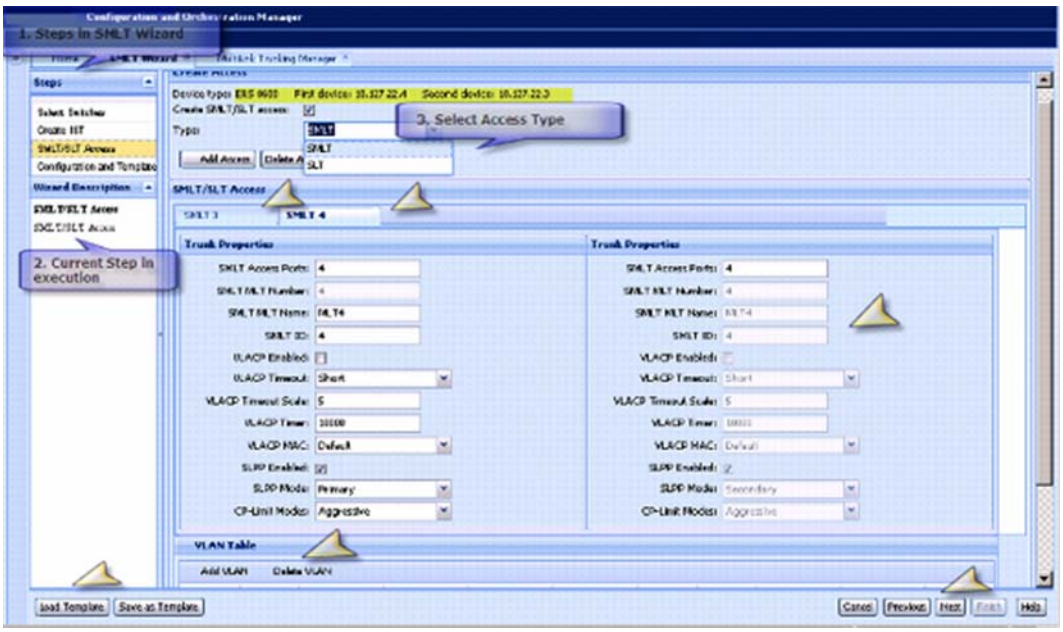
   A New Access dialog box appears asking for a SMLT ID or SLT ID.

   **Important:**

   To disable the access of an SMLT you can click **Delete Access**

9. Enter the ID of the new SMLT or SLT in the field of the New Access dialog box.
10. Click **OK**.

    The SMLT Access or SLT Access forms are enabled. Depending on the SMLT and SLT, two forms are created.

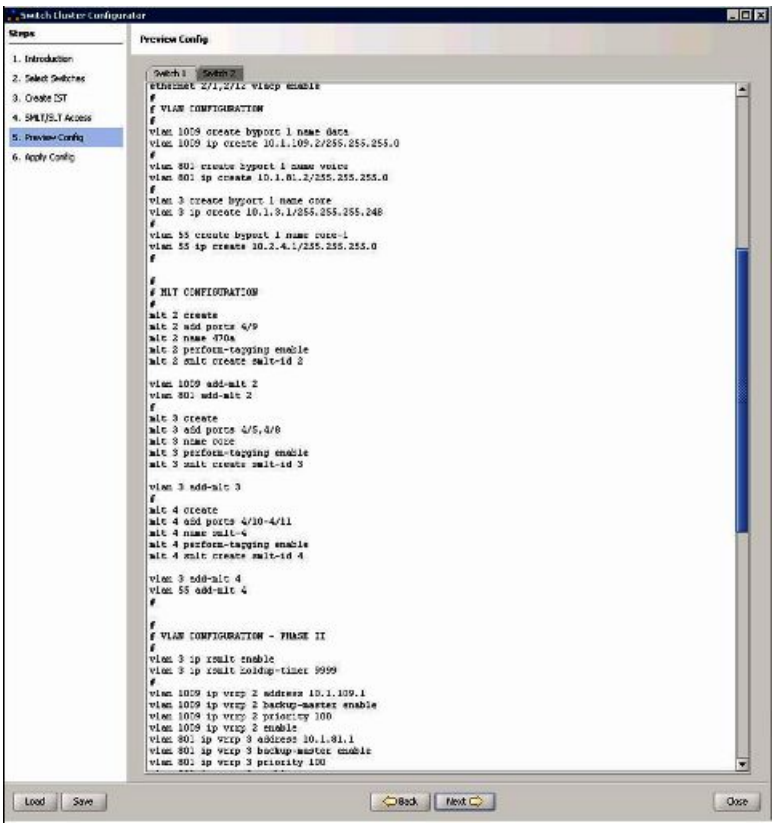



The SMLT/SLT Access form includes

- Trunk Properties table—specifies the trunk properties.
- VLAN Table—specifies the VLANs you want to create or use for the SMLT/SLT accesses.

11. Enter the values of trunk properties to create an SMLT/SLT access.
12. Click **Add VLAN** in VLAN Table to specify the properties of VLANs that you want to create or use for SMLT Access.
13. Enter the VLAN ID. If you provide a VLAN ID that does not exist, the Wizard creates the VLAN appropriately.
14. Select VLAN check box for the VLAN to be used for each access.
15. Click **Add Access Appropriately** to create multiple accesses at the same time.
16. Click **Next**.

    The Preview Config dialog box appears.




17. Click the **Switch 1** tab to view the switch based CLI commands.
18. Click the **Switch 2** tab to view the switch based CLI commands generated by the wizard.
19. Click **Next**.

    The Apply Config dialog box appears.

    You can view the CLI commands executed by the CLI command log wizard.
20. Click **Start Configuration** to execute the commands on both devices.

    The wizard runs the command to show the SMLT/MLT configuration.

## Job aid

The following table describes the fields of Truck properties screen:

**Table 104: Trunk properties**

| Field | Description |
|---|---|
| SMLT Access Ports | Specifies the SMLT access port. |
| SMLT MLT Number | Specifies the SMLT MLT number. |

| Field | Description |
|---|---|
| SMLT MLT Name | Specifies the SMLT MLT name. |
| SMLT ID | Specifies the SMLT ID. |
| VLACP Enabled | Specifies whether VLACP is enabled or disabled. |
| VLACP Timeout | Specifies the VLACP timeout. |
| VLACP Timeout Scale | Specifies the VLACP timeout scale. |
| VLACP Timer | Specifies the VLACP timer. |
| VLACP MAC | Specifies the VLACP MAC. |
| SLPP Enabled | Specifies whether SLPP is enabled or disabled. |
| SLPP Mode | Specifies the SLPP mode. |
| CP-Limits Modes | Specifies the CP-Limit mode. |

### Job aid

The following table describes the fields of VLAN table.

**Table 105: VLAN Table**

| Field | Description |
|---|---|
| VLAN ID | Specifies the VLAN ID. |
| Use VLAN | Allows you to use the VLAN for each access. |
| Add Access Appropriately | Allows you to create multiple accesses at the same time. |

You can modify the value of VLAN Table entries using in-line edit modes.

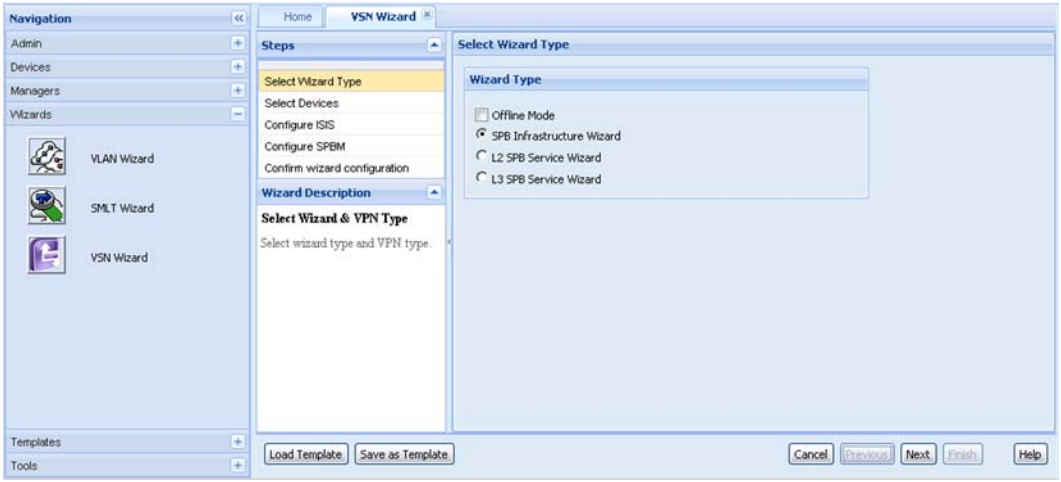
## VSN wizard

The Virtual Services Networks (VSN) wizard permits you to configure VSN service on multiple devices.

The following table outlines the supported device list for the VSN wizard:

| Supported device for VSN wizard | Version |
|---|---|
| ERS 8600 | v 7.1 |

The following figure shows the VSN Wizard.




**Navigation**

- VSN wizard functionality on page 360
- Using the SPB Infrastructure Wizard on page 360
- Using the L2 SPB Service Wizard on page 363
- Using the L3 SPB Service Wizard on page 366

## VSN wizard functionality

The VSN wizard has the following three sections:

- SPB Infrastructure Wizard
- L2 SPB Service Wizard
- L3 SPB Service Wizard

## Using the SPB Infrastructure Wizard

Perform the following procedure to create an SPB.

**Procedure steps**

1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizards**, and click the **VSN Wizard** icon.

   The VSN Wizard dialog box appears.

2. In the **VSN Wizard** dialog box, select **SPB Infrastructure Wizard**.

**Note:**
For information about working offline, see Offline Mode on page 370

3. Click **Next**.

   The Select Devices page appears.

4. To move a device from the **Discovered Devices** list to the **Managed Devices** list, from the **Available Devices** list, double-click on the device, or select the device, and click on the right pointing arrow.

   Or

   To move all devices from the **Discovered Devices** list to the **Managed Devices** list, click on the double right pointing arrow.

   **Note:**
   To unselect a device, from the **Managed Devices** list , select the required item and click on the left pointing arrow. To unselect all devices, click on the double left pointing arrows.

   **Note:**
   All ERS 8600 and ERS 8800 v 7.1 appear in the device list with or without SPBm infrastructure data configured. The devices are listed by IP address only.

5. Click **Next**.

   COM performs an ISIS discovery, and the Operation Results page appears.

6. Click **Ok**.

   COM performs an MLT discovery, and the Operation Results page appears.

7. Click **Ok**.

   The Configure ISIS page appears.

8. In the Configure ISIS page, enter the following information for each device:

   - System ID
   - Manual Area
   - CLIP Address
   - CLIP Mask
   - ISIS Interfaces

     i. In the ISIS interfaces column, click on **Please specify**.

        The ISIS Interfaces dialog box appears.

     ii. Enter the values.

     iii. Click **Save**.

9. Click **Next**.

   The Configure SPBM page appears.

10. In the Configure SPBM page, enter the following information for each device:
    - Instance ID
    - SPB Nickname
    - Primary BVLAN
    - Secondary BVLAN
    - SMLT Peer System ID
    - If required, in the IP Shortcuts column, select **enable**.
11. Click **Next**.

    The Confirm wizard configuration page appears with the generated script page for all devices.
12. Click **Finish**.

## Job aid

The following table describes the fields in the SPB Infrastructure Wizard.

| Field | Description |
|---|---|
| Discovered | Devices that have a configured SPB infrastructure. |
| Managed Devices | Devices you select . After you select the required devices, the rows are placed according to the sort selection currently specified for the Selected Devices table. |
| System ID | Sets the router system ID.<br>The required parameters are: <System ID> = System ID {xxxx.xxxx.xxxx - 6 bytes}<br>The command syntax is : system-id <System ID><br>The default is empty. If the System ID field is empty, the device autogenerates the system ID. |
| Manual Area | This field is required. The format is xx.xxxx...xxxx, where x is a hexadecimal digit, 1..13 bytes, each xx is one byte. |
| CLIP Address | This field is required. The format is ddd.ddd.ddd.ddd, where d is a decimal digit. |
| CLIP Mask | This field is required. The format is ddd.ddd.ddd.ddd, where d is a decimal digit. |

| Field | Description |
|---|---|
| ISIS Interfaces | This field is required. Specifies the ISIS Interfaces and MLT Interfaces for the devices. |
| Instance ID | This field is required. This field is for the SPBM instance ID.<br>The required parameters are: <instance-id> = plsb instance-id (1..100) {1..100}<br>The command syntax is: object <instance-id> |
| SPB Nickname | This field is required. The format is x.xx.xx, where x is a hexadecimal digit. |
| Primary BVLAN | This field is required. The value must be a number between 1 and 4094. The default value is 4001. |
| Secondary BVLAN | This field is required. The value must be a number between 1 and 4094. The default value is 4002. |
| SMLT Peer System ID | This field is required. The format is xxxx.xxxx.xxxx, where x is a hexadecimal digit. |
| IP Shortcuts | This field is required. This field configures the isis spbm instance ip command.<br>The required parameters are: <enable\|disable> = isis spbm ip shortcut state {disable\|enable}<br>The command syntax is: ip<enable\|disable><br>The states are enable and disable. The default is disable. |

## Using the L2 SPB Service Wizard

Perform the following procedure to use the L2 SPB Service Wizard.

### Procedure steps

1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizards**, and click the **VSN Wizard** icon.

   The VSN Wizard dialog box appears.
2. In the **VSN Wizard** dialog box, select **L2 SPB Service Wizard**.

**Note:**
For information about working offline, see Offline Mode on page 370

3. Click **Next**.

   The Select Devices screen appears.

4. To move a device from the **Available Devices** list to the **Selected Devices** list, from the **Available Devices** list, select the corresponding row, and click **Select >**.

   Or

   To move all devices from the **Available Devices** list to the **Selected Devices** list, click **Select All >>**.

   **Note:**
   To unselect a device, from the **Selected Devices** table, select the required item and click **< Unselect**. To unselect all devices, click **<< Unselect All**.

   **Note:**
   All ERS 8600 and ERS 8800 v 7.1 appear in the device list with or without SPBm infrastructure data configured. The devices are listed by IP address only.

5. Click **Next**.

   The Operation Result page appears.

6. Click **Ok**.

   The Select ISID & VLANs page appears.

7. In **ISID** field, enter an ISID number.

8. From the **VLAN** column drop-down box, select a VLAN.

   If there are no VLANs for a device, then you must add a VLAN.

   a. click on **Launch the VLAN Wizard**.

      For information about adding a VLAN, see Creating and configuring VLANs for an Avaya STG on page 40.

   b. After you complete the procedure for adding a VLAN, click the **VSN Wizard** tab.

   c. Click **Refresh**, and select the VLAN.

9. To view the information or make changes to the port or MLTs currently mapped to the VLANs, in the **Port Members** column, double-click on a cell for a specific device.

   The Port Members pop-up window appears.

10. Add or remove ports, then click **Save**.

11. In the wizard frame, click **Next**.

12. If you choose to save the wizard configuration as a template, perform the following procedure.

    a. Check the **Save as Template** check box.

b. Enter a Template name.

c. Click **Finish**

Or

If you do not want to save the wizard confirmation as a template, click **Finish**.

## Job aid

The following table describes the fields in the L2 SPB service wizard.

| Field | Description |
|---|---|
| Discovered Devices | Devices that have a configured SPB infrastructure. |
| Managed Devices | Devices you select . After you select the required devices, the rows are placed according to the sort selection currently specified for the Selected Devices table. |
| ISID | Presents a combo box, that you can edit, with all ISID numbers that COM discovers from all compatible devices. |
| VLAN Selection | Presents a table with all the devices that you selected in the Select Devices screen. The information includes the device IP/sysname, VLAN that you select, and port members for the VLAN you select. The VLAN table is visible only after you select the ISID number. |
| VLAN column | Presents a drop-down combo box with all VLAN numbers that COM discovers on the device. If there is a VLAN assigned to a selected ISID on a device, then COM automatically selects the VLAN number and the selection is disabled. |
| Port Members column | Presents ports and MLTs that COM maps to the VLAN you select from the VLAN column. If you change the VLAN number, COM updates or changes the content in the Port Members column for the required device. If you double-click on a Port Member cell for a specific device, the device slot/port pop-up panel appears, and you can add or remove slot/port combinations. |

The following table describes the toolbar buttons in the L2 SPB service wizard.

| Button | Description |
|---|---|
| Launch VLAN Wizard | Launches the VLAN Wizard to create a new VLAN. In the VLAN Wizard, you must manually select the required device. After you close the VLAN pop-up, COM rediscovers the information from the network and saves your settings. You must click Refresh after the VLAN Wizard completes. |
| Refresh | Refreshes ISIDs and VLANs for all devices. |

**Note:**

If you move back and forth from other steps and return to the Select ISID & VLAN screen, COM rediscovers the information from the network, and saves your selections if they are still valid. For example, if you remove the VLAN from a device, you can no longer select that device; you must select a new VLAN for the device.

## Using the L3 SPB Service Wizard

Perform the following procedure to use the L3 SPB Service Wizard.

### Procedure steps

1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizards**, and click **VSN Wizard**.

   The VSN Wizard dialog box appears.

2. In the **VSN Wizard** dialog box, select **L3 SPB Service Wizard**.

   **Note:**

   For information about working offline, see Offline Mode on page 370

3. Click **Next**.

   The Select Devices screen appears.

4. To move a device from the **Discovered Devices** list to the **Managed Devices** list, from the **Discovered Devices** list, double click on the device or select a device and click on the right pointing arrow.

   Or

   To move all devices from the **Discovered Devices** list to the **Managed Devices** list, click on the double right pointing arrows.

**Note:**

To unselect a device, from the **Managed Devices** list , select the required item and click the left pointing arrow. To unselect all devices, click the double left pointing arrows.

**Note:**

All ERS 8600 and ERS 8800 v 7.1 appear in the device list with or without SPBm infrastructure data configured. The devices are listed by IP address only.

5. Click **Next**.

   COM performs a VSN discovery, and the Operation Result box appears

6. Click **Ok**.

   The Select ISID & VRFs screen appears.

7. In **ISID** field, enter an ISID number.
8. If a VRF is not specified, then in the **VRF** column, enter a VRF from the selection available.

   **Note:**

   You can sort on all columns in the grid.

9. If a VLAN is not specified, then in the **VLAN** column, enter a VLAN from the selection available.
10. Optionally, in the **VLAN IP Address** and the **VLAN IP Mask** columns, type in the IP Address and Mask for the VLAN, or leave both empty.
11. Click **Next**.

    The Route Redistribution screen appears.

12. To redistribute SPB routes, check the check box next to the protocol name for all the protocols you require.
13. To stop redistribution of SPB routes, uncheck the check box next to the protocol name for all the protocols you require, and check the **Delete Unselected Redistributes** check box.
14. Click **Next**.

    The Confirmation screen appears.

15. Click **Finish**.

## Job aid

The following table describes the fields in the L3 SPB service wizard.

| Field | Description |
|---|---|
| Discovered Devices | Devices that have a configured SPB infrastructure. |
| Managed Devices | Devices you select . After you select the required devices, the rows are placed according to the sort selection currently specified for the Selected Devices table. |
| ISID | Presents a combo box that you can edit, with all ISID numbers that COM discovers from all compatible devices. After you change the ISID, COM refreshes the values in the VRF column to show only VRFs that are mapped to selected ISIDs for all devices. |
| VRF column | Presents a drop-down combo box with all VRF numbers that COM discovers for each device that appears in the table. Each drop down list shows the VRFs for one device. If there is a VRF assigned to a selected ISID on a device, then COM automatically selects the VRF number and disables the selection. |
| VLAN column | Presents a drop-down combo box with all VLAN ID numbers that COM discovers for each device that appears in the table. Each drop down list shows the VLANs for one device. If there is a VLAN assigned to a selected VRF on that device, then COM automatically selects the VLAN number and disables the selection. |
| VLAN IP Address column | Presents a text field that lets you optionally specify the IP Address for the VLAN selected on that device. If the selected VLAN has an IP Address configured, then it appears in the text field. Clearing the field removes the IP configuration from the selected VLAN. |
| VLAN IP Mask column | Presents a text field that lets you optionally specify the IP Mask for the VLAN selected on that device. If the selected VLAN has an IP Mask configured, then it appears in the text field. Values for both IP Address and Mask have to be specified or both values have to be empty. Changing only the Mask of the existing VLAN IP configuration is not supported. |

| Field | Description |
|---|---|
| Route Source | Redistributes routes from the protocols you select into ISIS. You can select one or more of the following protocols:<br>• Direct<br>• Static<br>• OSPF<br>• RIP<br>• BGP<br>• Delete Unselected Redistributes<br>For example, if the Direct protocol route redistribute is not configured on the device and you select the check box for Direct, COM generates the following CLI commands:<br>• ip vrf <vrfName> isis redistribute direct create<br>• ip vrf <vrfName> isis redistribute direct enable<br>• ip vrf <vrfName> isis redistribute direct apply<br>If the you select the Delete Unselected Redistributes check box, COM removes the unselected route redistributes from the device. For example, if you select the Direct protocol, and select Delete Unselected Redistributes, COM generates the following CLI commands:<br>• ip vrf {vrfName} isis redistribute static delete<br>• ip vrf {vrfName} isis redistribute ospf delete<br>• ip vrf {vrfName} isis redistribute rip delete<br>• ip vrf {vrfName} isis redistribute bgp delete<br>COM generates the delete commands only if the redistributes are already configured on the device. COM ignores all the selected route redistributes that are not configured on the device. After you select the Delete Unselected Redistribute check box, all the devices have the same routes redistribute configuration. |

The following table describes the toolbar buttons in the L3 SPB service wizard.

| Button | Description |
|---|---|
| Launch VLAN Manager | Launches a pop-up window to create a VLAN for the required device.<br>Refresh after the VLAN Manager updates. |
| Launch VRF Manager | Launches a pop-up window to create a VRF for the required device.<br>Refresh after the VRF Manager updates. |
| Refresh | Refreshes ISIDs and VRFs for all devices. |

**Note:**

If you move back and forth from other steps and return to the Select ISID & VRF screen, COM rediscovers the information from the network, and saves your selections if they are still valid. For example, if you remove the VRF from a device, you can no longer select that device; you must select a new VRF for the device.

# Offline Mode

All wizards support the Offline Mode.

The following list outlines the behavior of the wizard after you enable the offline mode.

- You can select the required devices.
- COM does not discover information from the devices.
- You can enter any value into form fields; COM provides only basic validation because the device configuration is unknown.
- COM replaces the pull down combination boxes and lists with text fields you can edit.
- COM generates the CLI script but does not send it to the devices.
- COM gathers the information you add and saves it as a template, only if you select the option to save as template on the last page before clicking Finish, or use the Save as Template button.
- After the template is loaded into the wizard with the offline mode turned off, the wizard validates all template data against the information that COM discovers from the devices.

Perform the following procedure to use the Offline Mode.

### Procedure steps

1. From the **Configuration and Orchestration Manager** navigation pane, click **Wizards**, and select a wizard.
2. On the first page, select the **Offline Mode** check box.

# Template support

All wizards in the Configuration and Orchestration Manager (COM) support loading and saving configurations into template files.

If you use the template feature within the COM wizards, you can load a template only on the first screen of the wizard; on all subsequent screens, the **Load Template** button is disabled. However, you can save a template on any screen to save the configuration you create.

### VSN Wizard

The Virtual Services Network (VSN) Wizard template contains the following information for each device you select:

- ISID number
- IP address
- VLAN ID
- mapped ISID number
- assigned port members

Because the VSN Wizard permits you to configure multiple devices at one time, some configuration values are connected to the device IP address; for example, in the L2 SPB VSN Wizard, the selected VLAN number is connected to the device IP address for all devices. However, not all configuration values are connected to the IP address; for example, the ISID number is not connected to the IP address.

After you load the template, and the device with the IP address in the template is no longer available in the network or in your inventory, the VSN wizard does not load the configuration values connected to that IP address. However, the VSN Wizard continues to discover the information from the network. The VSN Wizard verifies the values loaded from the template against the values the VSN Wizard discovers from the network. If you specify a value in the template that is invalid, then the VSN Wizard resets the template, and you must specify the value again.

The Template Manager manages templates that you create in the VSN Wizard. For more information about the Template Manager, see Configuration of Templates on page 373.

# Chapter 17: Configuration of Templates

The template contains a set of configuration attributes. Templates can be created by running the COM configuration wizards. While executing the wizard you can save the wizard configurations as a template. The saved templates can be viewed in the Templates window and can be used later to easily perform the same or similar configurations.

For more information on how to access the Templates Manager, see Starting Templates Manager on page 374.

Using Templates Manager, you can:

- view template name, type, last modified user, and last modified time
- filter template by template type
- view template details
- add new VLAN, SMLT or VSN template by launching the specific wizard
- load and apply an existing template into the specific wizard
- delete a template
- import a template from an XML file format
- export a template

For more information about Templates Manager, see the following sections.

### Navigation

# Starting Templates Manager

Perform the following procedure to start the Templates Manager.

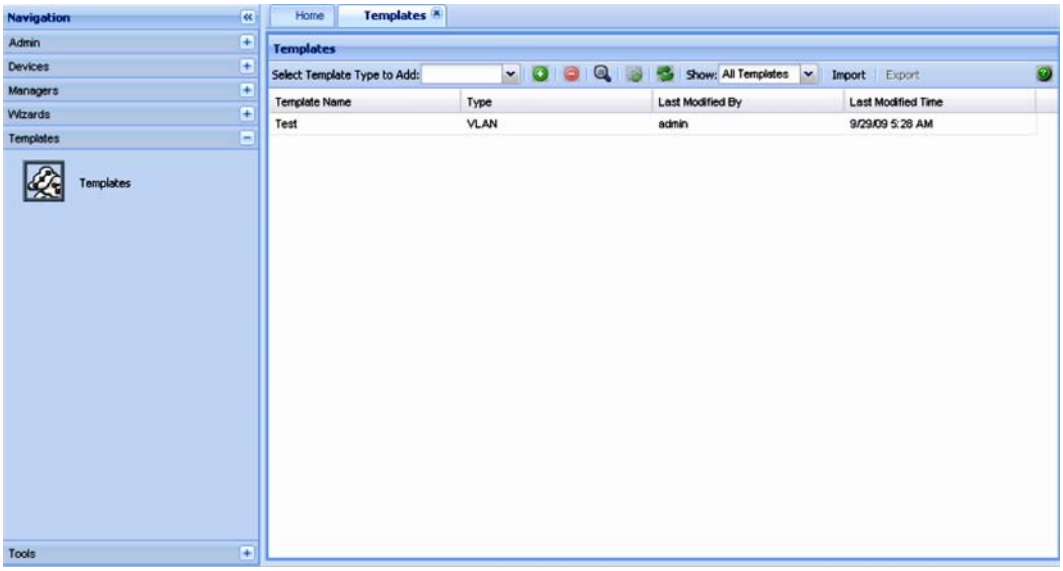
### Procedure steps

1. In the **Configuration and Orchestration Manager** navigation pane, select **Templates**.

   The navigation pane appears.

2. Click the **Templates** icon.

   The Templates window appears.




# Templates window

The following figure shows the Templates window.

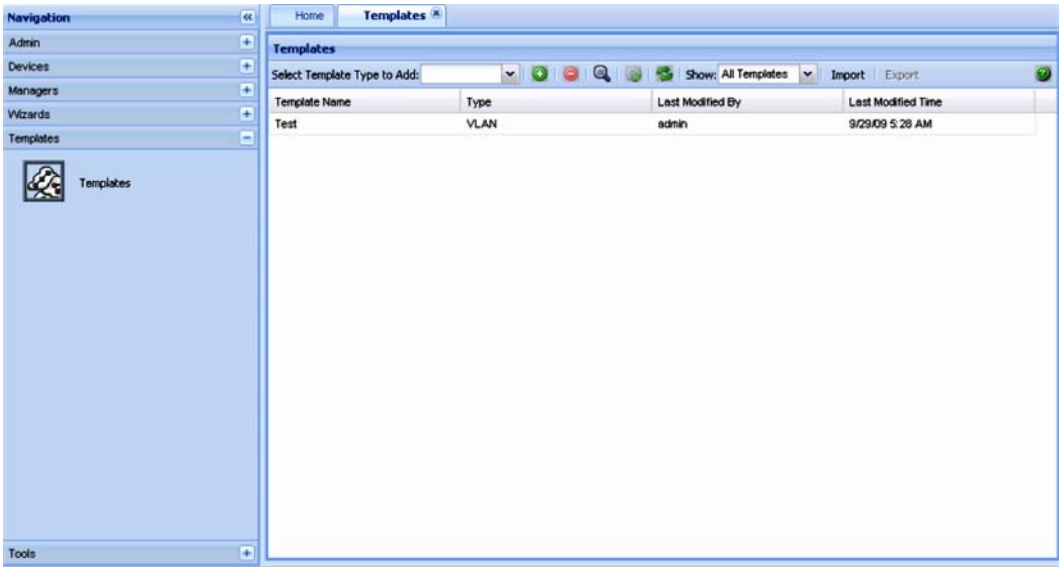



**Figure 31: Templates Window**

The following table explains the parts of the Templates window:

**Table 106: Parts of the Templates window**

| Part | Description |
|---|---|
| Tool bar | Provides quick access to commonly used Template commands. For more information, see Tool bar buttons on page 375. |
| Contents pane | Displays details of the templates. For more information, see Contents pane on page 376. |

### Navigation

- Tool bar buttons on page 375
- Contents pane on page 376

## Tool bar buttons

The following table explains the different buttons on the tool bar.

**Table 107: Description of tool bar buttons**

| Command | Tool bar button | Description |
|---|---|---|
| Select Template type to Add |  | Displays the list of the types of VLANs that can be created. The values are VLAN and SMLT. |

| Command | Tool bar button | Description |
|---|---|---|
| Add new template |  | Add a new VLAN or SMLT template. |
| Delete template |  | Deletes a selected template. |
| View selected template |  | Displays details of the selected template. |
| Run selected template |  | Runs the selected template. |
| Refresh |  | Refreshes the view and displays the newly created templates, if any. |
| Show |  | Displays the templates depending on the value selected. The available values are as follows:<br>• All Templates<br>• VLAN only<br>• SMLT only |
| Import |  | Imports the template from a specified file. |
| Export |  | Exports the template to a specified file. |
| Help |  | Opens Online help for the current folder or tab. |

## Contents pane

The Contents pane displays the details of the template based on the filter criteria set. The following details of the template appear:

- Template Name
- Type
- Last Modified By
- Last Modified Time

If you double-click on a particular template, you can view the details of it in the **Template Details** dialog box.

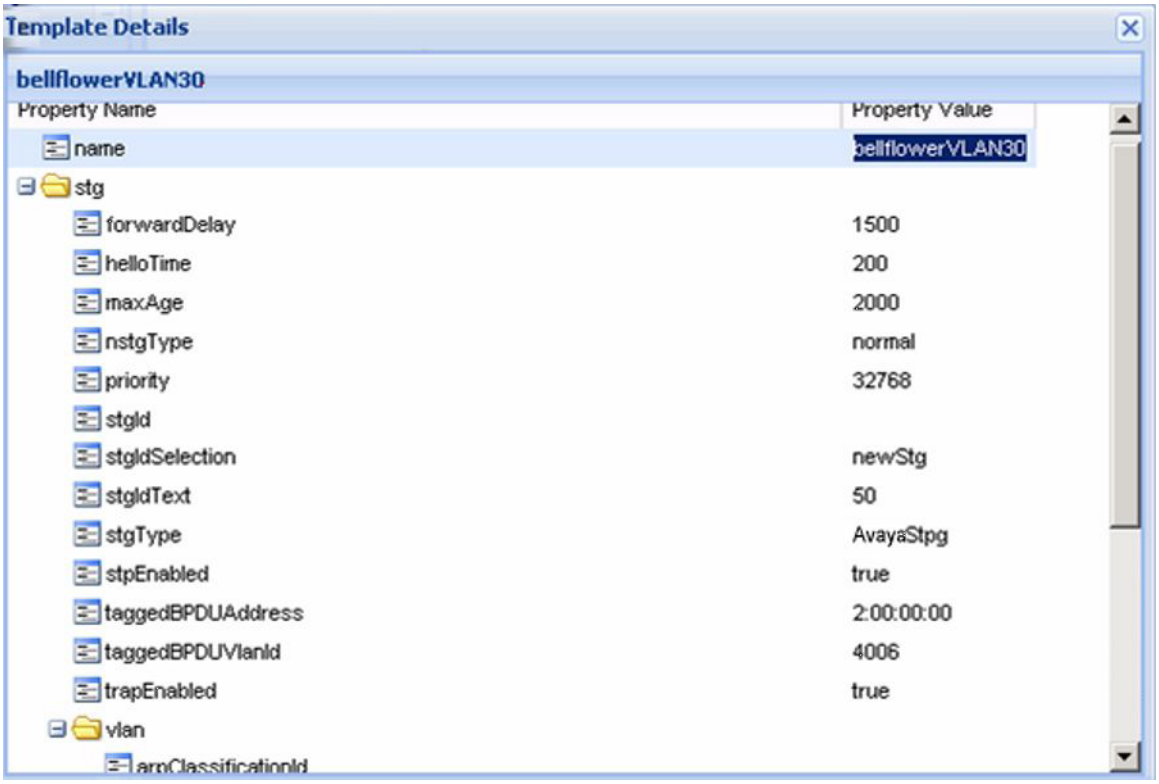



**Figure 32: Template Details dialog box**

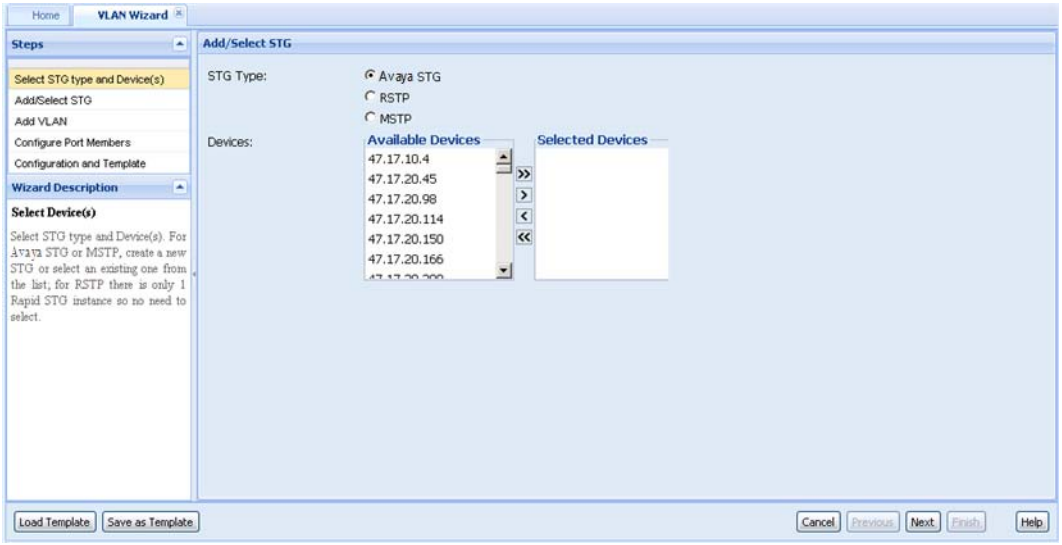
# Adding a VLAN template

Perform the following procedure to add a VLAN template.

### Procedure steps

1. In the **Templates** window, select the VLAN template type from the **Select Template Type to Add** field.
2. Click the **Add new template using wizard** button ((+) sign).

   The VLAN Wizard discovery occurs, and a Loading wizard data message appears. After the VLAN wizard discovery is complete, the VLAN Wizard window appears.




3. Select the **STG Type**.
4. From the **Available Devices** list, select a device and click the right-pointing arrow to move it to the **Selected Devices** list.
5. After you select the devices, click **Next**.
6. Enter the required values in the corresponding fields of Add/Select STG page.
7. Choose the devices you wish to add from the **Available Devices** list, and click the right-pointing arrow to move the devices to the **Selected Devices** list.
8. Click **Next** to move to the Add VLAN page.
9. In Add VLAN page, enter the required values in the corresponding fields, choose the devices you wish to add from the **Available Devices** list, and click the right-pointing arrow to move the devices to the **Selected Devices** list.
10. Click **Next** to move on Configure Port Members page to view configuration details.
11. Click **Next** to move on Configuration and Template page.
12. Click **Save as Template** to save the configurations as a VLAN template.

    For the more information about using the VLAN wizard, see VLAN Wizard on page 347.
13. From the Template window, click **Refresh** to view the newly added template.

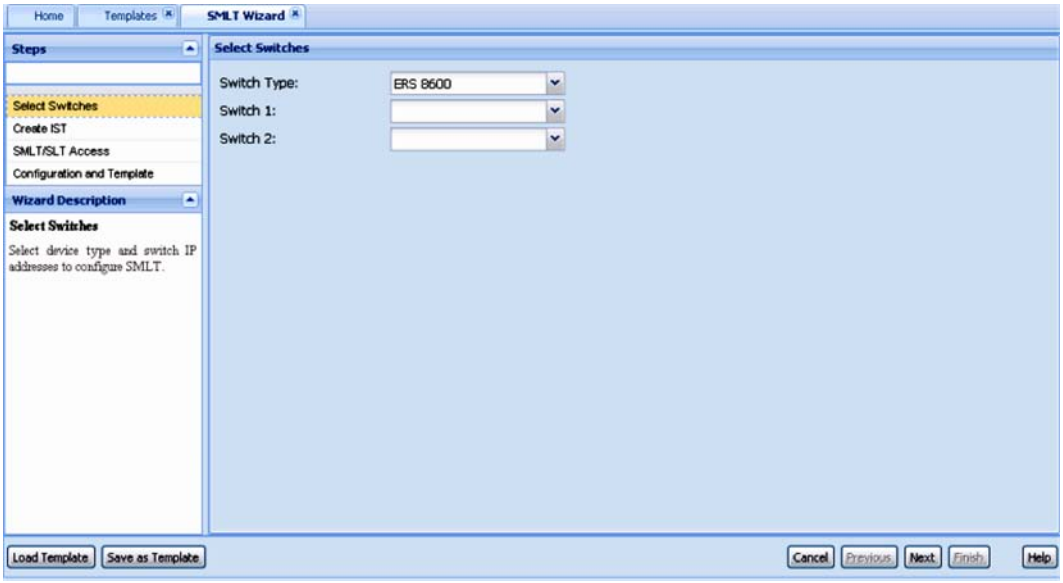
# Adding a SMLT template

Perform the following procedure to add a SMLT template.

## Procedure steps

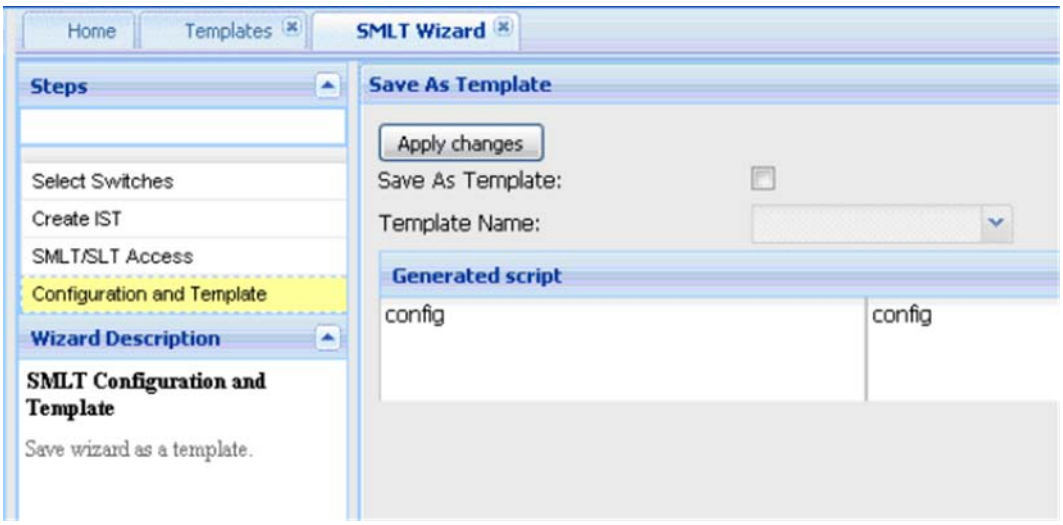
1. In the **Templates** window, select the SMLT template type from the **Select Template Type to Add** field.
2. Double click **Add new template using wizard** (+) sign.

   The SMLT Wizard dialog box appears.




3. In the Select Switches page, enter the required value in the corresponding fields, and then click **Next** to move on Create IST page.
4. In the Create IST page, enter the values for creating the IST in the fields provided, and then click **Next** to move on SMLT/SLT Access page.
5. IN SMLT/SLT Access page, enter the required value in the corresponding fields, and then click **Next** to move on Configuration and Template page.
6. To save the configuration as a template, do one of the following:

   - In the Configuration and Template window, select the check box corresponding to **Save as Template**, enter the file name in **Template Name** field, and then click **Finish**.




- Click **Save as Template** button, type the name of the template in the dialog box that pops up and click **Save**.

7. Click **Refresh** to view the new template.

   For more information about using the SMLT wizard, see SMLT wizard on page 353.

# Adding a VSN template

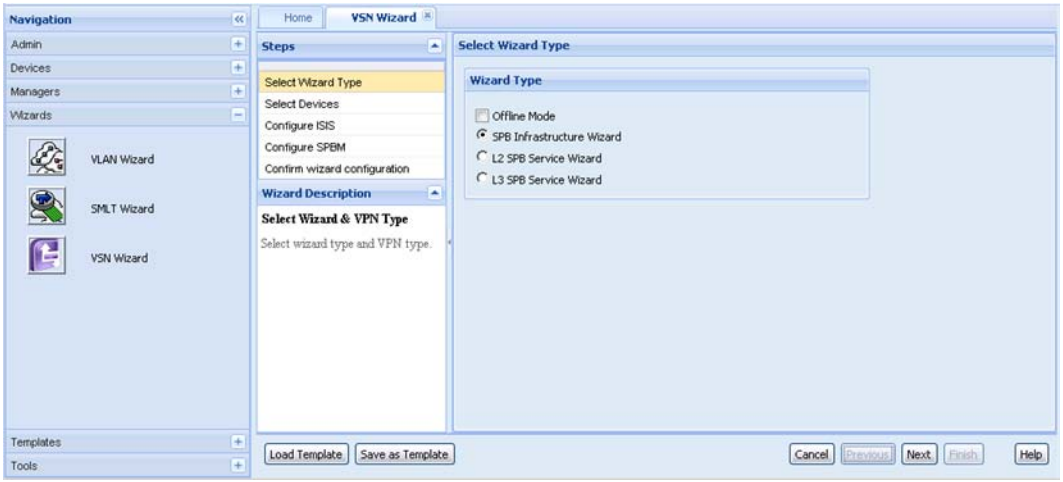
Perform the following procedure to add a VSN template.

### Procedure steps

1. In the **Templates** toolbar, in the **Select Template Type to Add** field, select **VSN**.
2. In the Templates toolbar, click **Add new template using wizard** ((+) sign).

   COM launches the VSN Wizard and displays the loading wizard data.

   The VSN Wizard window appears.




3. In the Select Wizard Type screen, select a Wizard Type.

   If you select the SPB Infrastructure Wizard, see Using the SPB Infrastructure Wizard on page 360.

   If you select the L2 SPB Service Wizard, see Using the L2 SPB Service Wizard on page 363.

   If you select the L3 SPB Service Wizard, see Using the L3 SPB Service Wizard on page 366.

# Deleting an existing template

Perform the following procedure to delete an existing template.

### Procedure steps

In the **Templates** window, click **Delete template** icon ((-) sign button) from the toolbar to delete the selected template.

The selected template is deleted from the list.

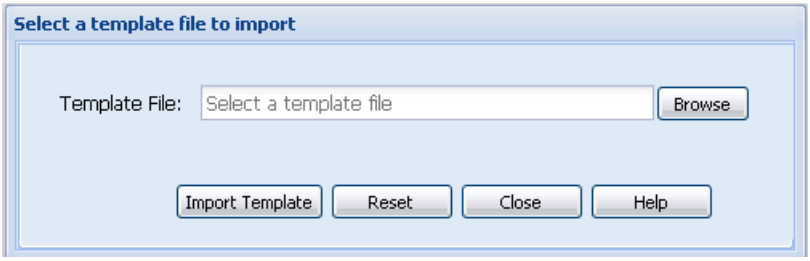
# Importing a template

Perform the following procedure to import a template in to the COM.

### Procedure steps

1. In the **Templates** window, click the **Import** from the toolbar.

   The Select a template file to import dialog box appears.




2. Enter the template file (in .xml format) you want to import in **Template File** field. Or click **Browse** to navigate to the file.
3. Click **Import Template** to import the selected file.

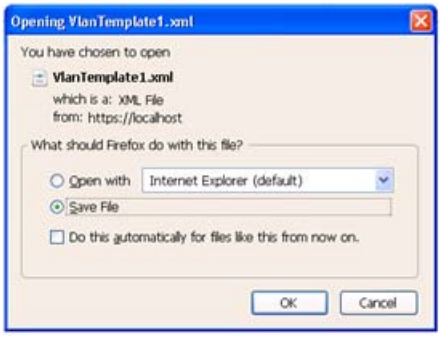
# Exporting a template

Perform the following procedure to export a template.

### Procedure steps

1. In the **Templates** window, select the template file you want to export and then click the **Export** button from the toolbar.

   The Opening Vlan template file dialog box appears.




2. Choose the **Open with** option to view the template file. OR Choose the **Save File** option to save the file on your desired location.
3. Click **OK**.

   The selected template is exported from the COM.

# Running a template

Perform the following procedure to run a template.

### Procedure steps

1. Select the required template from the **Templates** window.
2. Click **Run selected template**.

   The corresponding VLAN or SMLT wizard is launched with the template values.