Avaya Configuration and Orchestration Manager Administration

Release 3.1
NN47226-600
Issue 08.01
August 2014

© 2014 Avaya Inc.

All Rights Reserved.

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 may generally make available to users of its products and Hosted Services. 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 websites 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 Avaya hardware and software. 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 website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”, or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya Aura® is a registered trademark of Avaya Inc.

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), 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, Hosted Service(s) 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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 13
Purpose 13
Related resources 13
Chapter 2: New in this release 16
Features 16
Architecture 16
Browser requirements 16
Client requirements 17
Licensing requirements 17
Server requirements 17
Supported devices 17
ACLI mode support for ERS 8600/8800 18
ETREE and Private VLAN support 18
IP Multicast over SPBm 20
Enhanced memory management 20
Switched UNI 20
Transparent UNI 21
Chapter 3: Configuration and Orchestration Manager overview 22
Managers 22
Using Bulk Configuration Manager 27
Chapter 4: Topology and device discovery 30
About the topology view 30
Understanding the topology map 31
About the discovery 31
Configuring and performing a discovery 32
Configuring a network discovery 33
Performing a network discovery 35
Clearing a discovery 35
Viewing a discovery log 36
Updating discovery information 37
Scheduling a discovery 37
Managing a scheduled discovery 39
Viewing discovery results 40
Managing the discovery results 40
Displaying information on the topology map 42
Managing the discovered devices 43
Working with multiple topologies 47
Saving a topology 47
Drawing a topology 47

Exporting and importing a topology from the Device Inventory View 47
Exporting and importing a topology from the topology map 48
Using the Device Inventory View 49
Starting the Device Inventory View 49
Device Inventory View tool bar options 49
Device inventory management 50
Chapter 5: Create and manage device group assignments 53
Starting the Device Group Manager 53
Device Group Manager toolbar options 54
Device Group Manager group and user management 55
Creating a device group 55
Editing a device group 55
Highlighting a device group on the topology map 56
Creating a user group 56
Editing a user group 57
Chapter 6: Using VLAN Manager 59
About VLAN Manager 60
VLAN 60
Spanning Tree Protocol 60
VLAN Manager features 61
Starting VLAN Manager 62
Using the VLAN Manager window 63
Navigation pane 64
Contents pane 66
Status bar 67
Creating and configuring Avaya Spanning Tree Groups 67
Creating an Avaya Spanning Tree Group 67
Configuring Avaya STG parameters 69
Editing an Avaya Spanning Tree Group 70
Deleting an Avaya Spanning Tree Group 71
Adding members to an Avaya Spanning Tree Group 71
Deleting members from an Avaya Spanning Tree Group 71
Editing Avaya Spanning Tree Group port membership 72
Creating and configuring VLANs for an Avaya STG 72
Creating a port based VLAN 73
Creating a subnet based VLAN 75
Creating a protocol based VLAN 75
Creating a source MAC address based VLAN 76
Creating a sVLAN based VLAN 77
Creating an ID based VLAN 78
Creating an spbm-bvlan 78
Creating a spbm-switched Uni Vlan 79
Job aid 80

Synchronizing VLAN name 81
Managing Rapid Spanning Tree Protocol 81
Configuring RSTP properties 82
Creating and configuring VLANs for Rapid Spanning Tree Protocol 82
Adding a VLAN to the Rapid Spanning Tree 82
Deleting a VLAN from the Rapid Spanning Tree 83
Adding members to a VLAN group in Rapid Spanning Tree 83
Managing Multiple Spanning Tree Protocol instances 83
Adding an MSTI in Multiple Spanning Tree 84
Deleting an MSTI 84
Adding port members 84
Editing MSTP properties 85
Managing VLANs for MSTP 85
Adding a VLAN in Multiple Spanning Tree 85
Deleting a VLAN in Multiple Spanning Tree 85
Adding members to a VLAN in Multiple Spanning Tree 86
Private VLAN 88
Mark private Vlan ports 88
Add private VLANs in Multiple Spanning Tree 89
Add Private VLAN Ports 90
Deleting a Private VLAN in Multiple Spanning Tree 91
Configuring port members 91
Port membership types 91
Adding port members 92
Adding tagged ports 92
Configuring routing on a VLAN interface 93
Enabling OSPF on a VLAN interface 93
Inserting a VRRP interface on a VLAN 94
Viewing STG and VLAN information 95
Viewing STG information 95
Viewing VLAN information 97
Highlighting information on the topology map 105
Domain synchronization 106
Domain synchronization interfaces 107
Domain synchronization procedures 112
Creating a sync domain 112
Adding a VLAN to a sync domain server node 113
Modifying a sync domain 114
Modifying a sync domain server node VLAN 114
Deleting a sync domain 115
Deleting a server node VLAN 115
Chapter 7: Create and manage MultiLink Trunks 117
About MultiLink Trunking Manager 118

MultiLink Trunks in different switch types ... 118
MultiLink Trunking Manager features ... 118
Starting the MultiLink Trunking Manager ... 119
Using the MultiLink Trunking Manager window ... 120
Navigation pane ... 120
Navigation pane tool bar ... 126
Contents pane ... 126
Content pane tool bar ... 127
Managing MultiLink Trunks ... 128
Creating MLTs on ERS 1424/16xx, ERS 8000, VSP 9xxx, and VSP 4000 3.1 devices ... 128
Viewing MLT port information ... 134
Editing a port on an MLT ... 134
Deleting an MLT from ERS 1424/16xx, ERS 8000, VSP 9xxx, or VSP 4000 ... 135
Editing an MLT ... 135
Viewing MultiLink Trunking configurations ... 135
Viewing trunk connections ... 136
Viewing no trunk configurations ... 137
Viewing isolated devices ... 138
Viewing interswitch trunks ... 139
Viewing SMLTs ... 139
Viewing single port SMLTs ... 140
Updating information in the MultiLink Trunking Manager ... 140
Viewing devices and MLT links on the topology map ... 141
Managing SMLT configurations ... 142
Configuring IST links ... 143
Configuring IST links on a single device ... 143
Configuring SMLT links ... 144
Configuring IST peers ... 145
Configuring a single port SMLT ... 146
Deleting a single port SMLT ... 146
Chapter 8: Configure security on your network devices ... 147
About Security Manager ... 147
Supported devices ... 148
Starting Security Manager ... 149
Using the Security Manager window ... 149
Toolbar and Contents pane buttons ... 150
Navigation pane ... 151
Contents pane ... 152
Creating and managing security groups ... 153
Creating security groups ... 153
Adding new devices to a security group ... 154
Saving security group settings ... 155
Reloading Security Manager ... 155

Editing Security Groups ... 155
Deleting security groups ... 156
Configuring the authentication method ... 157
Configuring RADIUS authentication ... 157
Configuring TACACS authentication ... 161
Configuring management access ... 163
Configuring a security group for SSH access ... 163
Configuring a security group for CLI access ... 168
Configuring a security group for Web access ... 170
Configuring a security group for SNMP v1/v2c access ... 171
Configuring a security group for SNMP v3 access ... 172
Creating and configuring access policies ... 185
Adding access policies ... 185
Enabling or disabling access policies for devices in a security group ... 187
Enabling or disabling individual access policies ... 188
Deleting access policies ... 189
Chapter 9: Configuration of Routing Manager ... 191
Starting Routing Manager ... 191
Job aid ... 191
Navigation pane ... 192
Contents pane ... 193
Rediscovering Routing Manager ... 194
Discover Routing ... 195
Adding devices ... 195
Preferences ... 196
Routing Manager features ... 197
Supported devices for Routing Manager ... 197
Viewing and configuring IPv4 routing ... 199
Configuring IPv4 routing ... 199
Configuring IPv4 routing Globals ... 200
Configuring circuitless IP ... 202
Configuring IPv4 routing Static Route ... 202
Configuring IPv4 routing ARP ... 203
Configuring OSPF ... 203
Configuring RIP ... 211
Configuring VRRP ... 214
Viewing and configuring IPv6 routing ... 216
Configuring IPv6 routing ... 217
Configuring IPv6 OSPF ... 219
Configuring IPv6 VRRP ... 226
Chapter 10: Configuration of Virtual Routing and forwarding ... 229
Virtual Routing and Forwarding ... 230
Starting VRF in the COM ... 230

Adding VRF on a device or multiple devices ... 231
Setting VRF content for devices ... 232
Viewing all the VRFs and its statistics configured for a specific device ... 233
Editing a single configuration or multiple VRF configurations ... 234
Deleting a VRF configuration from a device ... 235
VRF enhancement—VLAN and routing ... 235
Chapter 11: Management of Multicast devices ... 236
About Multicast Manager ... 237
Starting Multicast Manager ... 237
Actions ... 238
Navigation tree structure ... 241
Using tables to change device configuration ... 241
IGMP and IGMP Snoop ... 241
DVMRP protocol folder ... 261
PIM SM protocol folder ... 268
MSDP Protocol folder ... 276
Multicast Route protocol folder ... 282
Policy folder ... 287
Highlight multicast data in the topology map ... 294
Chapter 12: Virtual Services Network Manager ... 297
VSN license ... 299
Starting the VSN Manager ... 299
Virtual Services Network Manager ... 299
VSN-centric view ... 300
Device centric view ... 301
Private VLAN overview ... 307
Etree overview ... 309
L2 SPBm functionality ... 311
Adding an L2 ISID ... 312
Adding devices to an L2 ISID ... 314
Deleting an ISID ... 315
Editing L2 SPBm tables ... 315
L3 SPBm functionality ... 316
Adding an L3 ISID ... 318
Adding a successful L3 VPN with the VSN Wizard ... 318
Adding a device to an L3 ISID ... 319
Deleting an L3 ISID ... 320
Deleting a device from an L3 ISID ... 320
Editing L3 SPBm tables ... 321
Editing Global Routing Table — IP Shortcuts ... 322
SPBm Multicast Route table ... 323
BGP-VPN ... 325
Configuring the BGP-VPNs ... 326

Adding a Route Target in VSN Manager ... 326
Associating a Route Target to a VRF ... 328
Editing BGP-VPNs ... 328
Deleting a Route Target node ... 328
CFM Globals ... 329
SPBm topology ... 329
Generating an SPBm topology view ... 330
Generating the shortest path view ... 333
Generating an ISID view ... 334
Generating the L2 Ping or L2 Trace Route ... 334
Chapter 13: Management of Auto Detection and Auto Configuration on the Avaya Switch ... 336
About Multimedia Manager ... 337
Starting the Multimedia Manager ... 337
Actions ... 338
Performing a Multimedia discovery ... 338
Selecting preferences for the Multimedia Manager ... 338
Adding a table row ... 339
Deleting a table row ... 340
Navigation tree structure ... 340
Using tables to change device configuration ... 340
ADAC tables ... 341
Global table ... 341
Ports table ... 343
Mac Ranges table ... 345
ADAC support by device and version ... 345
Resetting the ADAC MAC ranges ... 347
802.1ab LLDP tables ... 347
Global table ... 348
Ports table ... 349
Remote table ... 350
802.1ab Port dot1 tables ... 350
Local VLAN Id table ... 351
Local Protocol VLAN table ... 351
Local VLAN Name table ... 352
802.1ab Port dot3 tables ... 352
Power tables ... 353
Link table ... 354
802.1ab Port med tables ... 354
Policy table ... 355
Location table ... 356
PoE PSE table ... 356
Capabilities table ... 357

Inventory table 357
Chapter 14: Inventory Manager 359
About the Inventory Manager 359
File management features 359
Inventory management features 362
Starting the Inventory Manager 362
Using the Inventory Manager window 363
Tool bar commands 364
Menu bar commands 364
Navigation pane 365
Contents pane 367
Understanding the Inventory Manager navigation tree 367
Setting Inventory Manager preferences 389
Setting device management preferences 389
Chapter 15: Management of Traps and Logs 391
Configuration of Audit log 391
Launching the audit log 391
Audit Log Report Viewer tabs 391
Audit log management 392
Configuration of Trap/Log Manager 397
Starting Trap/Log Manager 397
Trap/Log Manager window 398
Discovering devices 399
Displaying Preferences 399
Configuring Traps 400
Configuring System Log 408
Configuration of trap parsers 411
Starting the Trap Viewer 411
Trap Viewer toolbar options 412
Trap parser object management 413
Using the Syslog Viewer 416
Viewing System Log 416
Chapter 16: Configuration of wizards and templates 418
Configuring wizards 418
VLAN wizard 418
SMLT wizard 427
VSN wizard 432
Offline mode 449
Template support 449
Configuration of Templates 450
Starting Templates Manager 451
Templates window 451
Adding a VLAN template 454

Adding a SMLT template..... 455
Adding a VSN template..... 457
Deleting an existing template..... 458
Importing a template..... 458
Exporting a template..... 458
Running a template..... 459

Chapter 1: Introduction

Related Links

Purpose on page 13
Related resources on page 13

Purpose

This document provides the information and procedures you require to install, license, uninstall, and troubleshoot the Avaya Configuration and Orchestration Manager (COM).

COM provides you with an intuitive interface to configure, manage, and provision Avaya enterprise family of devices, such as Avaya Ethernet Routing Switches, Avaya Ethernet Switches, Legacy BayStack switches, Business Policy Switches 2000™ operating within the same local area network, Avaya Virtual Services Platform (VSP) devices, and Wireless Local Area Network (WLAN) devices. COM is a management system that manages multiple network devices, and provides management for services across different elements.

The *Avaya Configuration and Orchestration Manager Installation* guide is intended for installers of the COM application.

Related Links

Introduction on page 13

Related resources

Related Links

Introduction on page 13
Documentation on page 14
Training on page 14
Viewing Avaya Mentor videos on page 14
Support on page 15

Documentation

See the following related documents:

Title	Purpose	Link
Avaya Configuration and Orchestration Manager Fundamentals (NN47226-100)	Fundamentals	http://support.avaya.com
Avaya Configuration and Orchestration Manager Installation (NN47226-300)	Deployment	http://support.avaya.com
Avaya Configuration and Orchestration Manager Administration (NN47226-600)	Administration	http://support.avaya.com
Avaya Bulk Configuration Manager Fundamentals (NN48021-100)	Fundamentals	http://support.avaya.com
Avaya System Manager Common Services Fundamentals (NN48014-100)	Fundamentals	http://support.avaya.com

Related Links

Related resources on page 13

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Related Links

Related resources on page 13

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support web site, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support site, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Related Links

Related resources on page 13

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Related Links

Related resources on page 13

Chapter 2: New in this release

The following sections detail what is new in *Avaya Configuration and Orchestration Manager Administration* (NN47226-600) for COM Release 3.1.

- Features on page 16

Features

See the following sections for information about feature changes.

Architecture

Prior to Release 3.1, the Avaya Configuration and Orchestration Manager (COM) application was deployed on the Unified Communications Management-Common Services (UCM-CS) platform. In Release 3.1, COM is deployed on the System Manager-Common Service based on Avaya Aura System Manager version 6.3.

As a result of Avaya's strategic decision to use a single platform for all J2EE applications, the System Manager (SMGR) platform was chosen. SMGR is a J2EE compliant platform already being used in Avaya's Aura products. Like all other SMGR applications, COM 3.1 migrates from the UCM-CS platform to SMGR-CS platform. SMGR-CS is a scaled down SMGR platform that contains only those platform services required for Avaya NMS applications. COM 3.1 moves to SMGR platform that further provides a common integrated management solution for Avaya voice and data customers.

For more information about the SMGR-CS platform, refer to *Avaya System Manager Common Services Fundamentals* (NN48014-100).

Browser requirements

Avaya Configuration and Orchestration Manager (COM) Release 3.1 supports Internet Explorer versions 8.x, 9.x, and 10.x, and Firefox versions 19, 20, and 21.

Client requirements

Avaya Configuration and Orchestration Manager (COM) Release 3.1 supports Internet Explorer versions 8.x, 9.x, and 10.x, and Firefox versions 19, 20, and 21.

Licensing requirements

Avaya Configuration and Orchestration Manager (COM) Release 3.1 uses FlexLM based licensing. A new FlexLM license is required for COM Release 3.1.

Server requirements

Avaya Configuration and Orchestration Manager (COM) Release 3.1 is supported on the following servers:

- Red Hat Enterprise Linux v5.6 and v5.7 (both 64-bit only)
- Microsoft Windows 2008 Server R2 (64-bit, standard and enterprise flavors)

Note:

The server requirements apply to a new installation of COM Release 3.1 and to an upgrade to COM 3.1.

Supported devices

Avaya Configuration and Orchestration Manager (COM) Release 3.1 supports the following new devices and new software versions.

Device	Support	Version
ERS 45xx and ERS 48xx	Full	5.6.3 and 5.7
	Partial	5.8 (Discovery and EDM Plugin launch)
ERS 5000	Full	6.2.7, 6.3.1, and 6.6
VSP 8000	Full	4.0
ERS 3500	Full	5.1.1 and 5.2
VSP 4000	Full	3.0.1 and 3.1
	Partial	4.0 (Discovery and EDM Plugin launch)
VSP 9000	Full	3.4 (Sapphire Chassis) and 4.0
VSP 7000	Full	10.2.1, 10.3, and 10.3.1
	Partial	Discovery and EDM Plugin launch) for 10.3.1 (New model type support - VSP 7024XT)

ACLI mode support for ERS 8600/8800

Avaya Command Line Interface (ACLI) is a text-based interface used to configure, manage, and monitor the Avaya devices. Earlier releases of Avaya Configuration and Orchestration Manager (COM) supported ERS8x00 devices running in Passport CLI only.

COM Release 3.1 supports Passport CLI and ACLI mode for ERS8600/ERS8800 v7.2 and v7.2.10, and ERS8300 v4.2 devices.

ACLI features are supported in the following modules:

- BCM tools
  - Backup and Restore
  - Configuration Update Generator
  - Device Password Manager
  - Software Version Updater
- Configuration Auditing Tool
- Inventory Manager
- Wizard
  - SMLT wizard
  - VSN wizard

For information about ACLI and Passport CLI commands for ERS8600/ERS8800 and ERS8300 devices, see *Avaya Command Line Interface Commands Refererence* (NN46205–106) and *Command Line Interface Reference* (NN46205–105), respectively.

ETREE and Private VLAN support

Avaya Configuration and Orchestration Manager (COM) Release 3.1 provides support for ETREE configuration and private VLANs for Virtual Services Platform 4000 (VSP 4000) devices v3.0.x.

Private VLAN

Private VLANs are used to provide isolation between ports within a Layer-2 service. A Layer-2 (L2) service is typically realized as a VLAN or a L2VSN. All the access-points in the service can communicate with one another using standard L2 MAC address lookup operations. Broadcast, Multicast, and Unknown Unicast traffic within a L2 service flood to all the access-points within the service.

A Private VLAN behaves differently from a traditional VLAN by providing isolation between some of the ports within the private VLAN. The ports that are members of a private VLAN can be classified into the following three groups:

- Promiscuous Ports: Ports within this group can communicate with all other ports within the private VLAN. These ports can be tagged or untagged ports and can be standalone ports or a member of an MLT.
- Isolated Ports: Isolated ports can communicate with promiscuous ports, but not with any other isolated port. These ports can be tagged or untagged ports and can be standalone ports or a member of an MLT.
- Trunk Ports: Trunk ports are used to carry traffic between other port members within the private VLANs. These ports are always tagged ports and can be standalone ports or a member of an MLT

Each private VLAN instance is associated with two different VLAN_ID values: primary VLAN and secondary VLAN.

The following rules describe how the VLAN_ID values are used:

1. On tagged promiscuous ports – only the primary VLAN is used.
2. On tagged isolated ports – only the secondary VLAN is used.
3. On untagged ports – there is not tag on the packets. Untagged ports are not allowed to be trunk ports.
4. On trunk ports – traffic that originated from isolated ports is tagged with the secondary VLAN_ID.
5. On trunk ports – traffic that originated from a promiscuous port is tagged with the primary VLAN_ID.

There is a combined L2 MAC table for both the primary and secondary VLANs within a private VLAN. MAC addresses from both promiscuous and isolated ports are both learnt into the same table. This means that traffic between an isolated and a promiscuous port can be forwarded in unicast fashion even though one of them is learnt on the primary VLAN_ID and the other is learnt on the secondary VLAN_ID.

Etree

An ETREE instance consists of islands of a private VLAN connected by a SPB Core network. Transport within the SPB core network by associating the private VLAN with a pair of I-SID values.

- ETREE: A PRIVATE VLAN whose core transport is done using SPBM.

  Note:

  This still allows for TRUNK ports to be present in the access networks connecting to an SPBM core.

- HUB: An access-point into the ETREE that is allowed to communicate with all other access-points in the ETREE. It is also used interchangeably with the PROMISCUOUS port definition in the context of ETREE.
- SPOKE: An access-point into the ETREE that is **not** allowed to communicate with any other SPOKE in the ETREE. A SPOKE is only allowed to communicate with HUBs. Used interchangeably with the ISOLATED port definition in the context of ETREE.

- PRIMARY/SECONDARY ISID: The I-SID used to carry traffic from a HUB/ SPOKE inside the SPBM network.

IP Multicast over SPBm

Avaya Configuration and Orchestration Manager (COM) Release 3.1 provides support for IP Multicast over Shortest Path Bridging MAC (SPBM). IP Multicast over SPBM greatly simplifies multicast deployment, with no need for any multicast routing protocols, such as Protocol Independent Multicast-Sparse Mode (PIM-SM) or Protocol Independent Multicast-Source Specific Multicast (PIM-SSM). A BEB can forward a multicast stream anywhere in an SPBM network where IS-IS advertises the stream to the rest of the fabric.

IP Multicast over SPB is supported for the following devices:

- ERS 8600/8800 v7.2 and above
- VSP 9000 v3.4 and above
- VSP 4000 v3.1 and above

For more information about configuring IP Multicast over SPBM, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000 Release 3.1* (NN46251-510).

.

Enhanced memory management

For the better memory (JVM Heap) management, the following constraints are added in COM Release 3.1:

- Limit the number of COM user sessions to 5

  To limit the sudden demand in heap space, COM 3.1 actively restricts the number of user sessions to the maximum 5 user sessions.

- Limit the number of open manager tabs to 12

  COM 3.1 restricts the number of manager tabs, which can be opened per user session to maximum 12 tabs.

Switched UNI

Switched UNI VLAN information is added to this document.

Switched User Network Interface (UNI) allows the association of local endpoints to I-SIDs based on local port and VLAN together. With switched UNI, the same VLAN can be used on one port to create an endpoint to one I-SID, and on another port to create an endpoint to another I-SID.

This feature impacts the following Avaya Configuration and Orchestration Manager (COM) components:

- VLAN Manager
- VSN Manager
- VLAN Wizard
- VSN Wizard

Switched UNI VLAN is supported on the following devices:

- VSP 7000 v10.2 and above
- ERS 4800 v5.7 and above

For information about Switched UNI support on VSP 7000 and ERS 4800 devices, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 7000 Series* (NN47202-510) and *Configuring Avaya VENA Fabric Connect on Avaya Ethernet Routing Switch 4000 Series* (NN47205-507), respectively.

Transparent UNI

Avaya Configuration and Orchestration Manager (COM) Release 3.1 provides support for Transparent user-network interface (T-UNI) feature for VSP 4000 v3.1 and above and VSP 7000 v10.3 and above. Transparent UNI is a feature that maps an entire port or MLT to an I-SID. Transparent UNI configures a transparent port where all traffic is MAC switched on an internal virtual port using the assigned I-SID. No VLAN is involved in this process. Devices transmit tagged and untagged traffic in the assigned I-SID regardless of the VLAN ID. The T-UNI port or MLT is not a member of any VLAN or STG and is always in the forwarding state.

Transparent UNI is supported for the following devices:

- VSP 4000 v3.1 and above
- VSP 7000 v10.3 and above

Chapter 3: Configuration and Orchestration Manager overview

This section provides an overview of Configuration and Orchestration Manager (COM).

Managers

Avaya Configuration and Orchestration Manager (COM) supports submanagers that provide detailed device information and management capabilities. The submanagers are designed to provide specialized information in an easy-to-use interface that is consistent in layout across the submanagers. A submanager can query COM and instruct the primary application to update the topology view with information relevant to the submanager view. For example, VLAN Manager can instruct COM to highlight all the devices in the view that include members of a particular VLAN.

Configuration and Orchestration Manager supports the following submanagers:

- VLAN Manager
- MultiLink Trunking Manager
- Security Manager
- Routing Manager
- Trap/Log Manager
- Virtual Routing Manager
- Multicast Manager
- Bulk Configuration Manager
- VSN Manager
- Multimedia Manager
- Inventory Manager

The following table lists the supported devices for each COM Manager.

Note:

Not all manager features are supported for each device or device version.

Manager	Device
VLAN Manager	• Passport 1000 Series switch • Virtual Services Platform 9xxx • Virtual Services Platform 4xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 16xx • Ethernet Switch/Ethernet Routing Switch 25xx • Alteon • Legacy Baystack • Legacy Ethernet Routing Switch 1424 • Ethernet Routing Switch 5xxx/4xxx/35xx • Wireless Controller 8xxx • WLAN AP • Business Policy Switch 2000
MultiLink Trunking Manager	• Virtual Services Platform 9xxx • Virtual Services Platform 4xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 16xx • Ethernet Switch/Ethernet Routing Switch 25xx • Alteon • Legacy BayStack • Legacy Ethernet Routing Switch 1424 • Ethernet Routing Switch 5xxx/4xxx/35xx • Ethernet Routing Switch 380, 410/450, 325/425/420, 460/470 • Wireless Controller 8xxx • WLAN AP • Passport 1000 Series switch • Business Policy Switch 2000 • OM 1000
Security Manager	• Passport 1050/1150/1200/1250 • Ethernet Routing Switch 8xxx

Manager	Device
	• Ethernet Routing Switch 5xxx/4xxx/35xx • Ethernet Routing Switch 16xx • Ethernet Routing Switch 325/425/420, 460/470 • Ethernet Switch/Ethernet Routing Switch 25xx • Wireless Controller 8xxx • Business Policy Switch 2000 • Virtual Services Platform 9xxx • Virtual Services Platform 4xxx • Virtual Services Platform 7xxx • Virtual Services Platform 8xxx
Routing Manager	• Virtual Services Platform 9xxx • Virtual Services Platform 4xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 16xx • Ethernet Switch/Ethernet Routing Switch 25xx • Alteon • Legacy Baystack • Legacy Ethernet Routing Switch 1424 • Ethernet Routing Switch 5xxx/4xxx/35xx • Wireless Controller 8xxx • WLAN AP
Trap/Log Manager	• Virtual Services Platform 9xxx • Virtual Services Platform 4xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 16xx • Ethernet Switch/Ethernet Routing Switch 25xx • Alteon • Legacy Baystack • Legacy Ethernet Routing Switch 1424 • Ethernet Routing Switch 5xxx/4xxx/35xx

Manager	Device
	• Wireless Controller 8xxx • WLAN AP
Virtual Routing Manager	• Virtual Services Platform 9xxx • Virtual Services Platform 8xxx • Virtual Services Platform 4xxx • Ethernet Routing Switch 8300/8600 • Ethernet Routing Switch 8800 • Ethernet Routing Switch 5xxx
Multicast Manager	• Passport 1000 Series switch • Virtual Services Platform 9xxx • Virtual Services Platform 4xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 16xx • Ethernet Switch/Ethernet Routing Switch 25xx • Alteon • Legacy Baystack • Legacy Ethernet Routing Switch 1424 • Ethernet Routing Switch 5xxx/4xxx/35xx • Wireless Controller 8xxx • WLAN AP
Bulk Configuration Manager	• Secure Router 1000/3100 • Secure Router 4134 • VPN Router 600-5000 • Secure Network Access Switch 4050/4070 • Ethernet Routing Switch 460/470 • Ethernet Routing Switch 5xxx/4xxx/35xx • Ethernet Switch/Ethernet Routing Switch 25xx • Business Secure Router 222/252 • Ethernet Routing Switch 8xxx • VPN Gateway 3050/3070 • Virtual Services Platform 9xxx • Virtual Services Platform 8xxx

Manager	Device
	• Virtual Services Platform 4xxx • Virtual Services Platform 7xxx • WLAN 8180
VSN Manager	• Ethernet Routing Switch 4800 • Virtual Services Platform 9xxx • Virtual Services Platform 4xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 16xx • Ethernet Switch/Ethernet Routing Switch 25xx • Alteon • Legacy Baystack • Legacy Ethernet Routing Switch 1424 • Ethernet Routing Switch 5xxx/4xxx/35xx • Wireless Controller 8xxx • WLAN AP
Multimedia Manager	• Virtual Services Platform 9xxx • Virtual Services Platform 4xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 16xx • Ethernet Switch/Ethernet Routing Switch 25xx • Alteon • Legacy Baystack • Legacy Ethernet Routing Switch 1424 • Ethernet Routing Switch 5xxx/4xxx/35xx • Wireless Controller 8xxx • WLAN AP • Ethernet Routing Switch 460/470
Inventory Manager	• Ethernet Routing Switch 8000 • Legacy BayStack • Ethernet Routing Switch 16xx

Manager	Device
	• Legacy Ethernet Routing Switch 1424 • Ethernet Routing Switch 5xxx/4xxx/35xx • Ethernet Switch/Ethernet Routing Switch 25xx • Alteon • WLAN AP • Wireless Controller 8180 • Virtual Services Platform 9xxx • Virtual Services Platform 4xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx

For more information about supported devices including supported device versions and supported features, see the following sections:

- For VLAN Manager, see Using VLAN Manager on page 59
- For MultiLink Trunking Manager, see Create and manage MultiLink Trunks on page 117.
- For Security Manager, see Configure security on your network devices on page 147.
- For Routing Manager, see Configuration of Routing Manager on page 191.
- For Trap/Log Manager, see Management of Traps and Logs on page 391.
- For Virtual Routing Manager, see Configuration of Virtual Routing and Forwarding on page 229.
- For Multicast Manager, see Management of Multicast devices on page 236.
- For Bulk Configuration Manager, see *Avaya Bulk Configuration Manager Fundamentals* (NN48021–100).
- For VSN Manager, see Configuration of Shortest Path Bridging on page 297.
- For Multimedia Manager, see Management of Auto Detection and Auto Configuration on the Avaya Switch on page 336.
- For Inventory Manager, see Inventory Manager on page 359.

Using Bulk Configuration Manager

Avaya Bulk Configuration Manager (Avaya BCM) is an application within the Configuration and Orchestration Manager (COM) that consists of a suite of tools with which you can perform a variety of management tasks across multiple device types using a Web-based interface.

Avaya BCM requires a separate license to enable the feature set.

Node based licensing for BCM

Avaya Bulk Configuration Manager (BCM) depends on Configuration and Orchestration Manager (COM). The Avaya BCM resides in COM and follows the same COM rules and restrictions, except that as a BCM user, you get all supported devices automatically, and skip the device assignment process. To enable 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 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:

Bulk Configuration Manager supports device imports from COM.

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

Launching the BCM main window and navigation

To launch the Bulk Configuration Manager (BCM) main window and navigation, perform the following procedure.

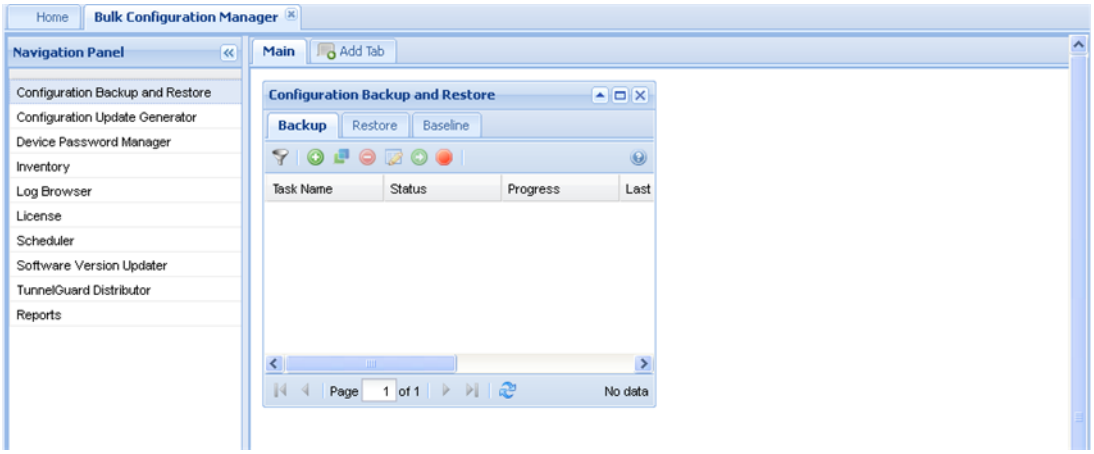
Procedure steps

1. From the Configuration and Orchestration Manager window Navigation pane, click **Managers**.
2. In the navigation tree, click **Bulk Configuration Manager**.

   The Bulk Configuration Manager is launched and appears in the content pane, under a new tab.

   Bulk Configuration Manager 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 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 Distributor
- Reports

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

Chapter 4: Topology and device discovery

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

About the topology view

The topology feature in Configuration and Orchestration Manager (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.
- save the current topology. 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.
- import and export the topology to an XML file, which you can load into COM again.
- 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 Fundamentals* (NN47226–100).

The first step in managing your network with COM is to use the topology view to perform a discovery. A discovery is a snapshot taken of part, or all, of a network. When you perform a

discovery, the information that COM collects 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)

  Note:

  ERS 8000, VSP 4000, VSP 8000, and VSP 9000 devices do not support 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.

For COM to discover the devices in a topology, you must first configure the device credentials. To properly perform a discovery, COM uses the SNMPv1/v2/v3 credentials of 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 SMGR-CS. For more information about configuring device credentials, see *SMGR-CS 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 40. For information about the tools and utilities that you can use to work with devices on the topology map, see Managing the discovered devices on page 43.

About the discovery

You can use the discovery feature to manage devices on your network. You also can use the discovery feature to add or update device attributes and IP addresses on the network database. When you launch a discovery, the system either creates or updates network topologies and inventories. When the discovery is finished, the system connects the discovered devices to the other devices in the network inventory.

Before you launch a discovery, you must properly configure the discovery settings. You have the option to start a discovery manually or through a scheduled event. You also have the option to determine the landing page the system uses to display the discovered devices.

Depending on your discovery landing page setting, the system displays either a map topology or an inventory grid in the COM application. On the **Home** tab, the topology map provides a view of all the

discovered devices and their relationships. On the **Device Inventory View**, the inventory grid provides a view of all the discovered devices and their respective connection statuses and attributes.

Important:

You cannot perform COM operations while discovery is in progress.

You can launch the following types of discoveries: new or merge.

New discovery

Run a new discovery when you introduce a device to your network. A new discovery process builds a topology for the network. The system creates a map showing all the discovered devices and the connections between these devices. Also, the network database is updated with the new device inventory and attributes.

Merge discovery

Run a merge discovery when you need to amend your device inventory without a new discovery. Changes to the inventory are limited to a smaller number of devices. You can perform a merge discovery when you want to add a new subnet or new device to the current network topology.

When you launch a merge discovery, the system performs the following actions when any of the following conditions are met:

- If a newly discovered device is already in the system database, the system updates the database with the new attributes of the newly discovered device.
- If a newly discovered device is already in the system database and the discovered device has a new IP or alias address, the system drops the discovered device and maintains the pre-existing attributes.
- If the new device is the only reachable device, the system updates the database with the attributes of the newly discovered device.
- If a link is a newly discovered link, the system updates the database with the link value.

Configuring and performing a discovery

You can configure the Configuration and Orchestration Manager (COM) application to perform a discovery to manage devices on your network. The discovery preferences that you set can determine the type of discovery the system performs and the landing page the system uses to display discovery results. Configuration and Orchestration Manager uses the information that you configure to discover devices and to create a topology map or an inventory grid.

You have the option to launch a new or merged network discovery. The new or merged discovery creates or updates the topology map or inventory grid, respectively.

Configuring a network discovery

You can configure the Configuration and Orchestration Manager (COM) application to perform a discovery to manage devices on your network. The discovery preferences that you set can determine the type of discovery the system performs and the landing page the system uses to display discovery results. Configuration and Orchestration Manager uses the information that you configure to discover devices and to create a topology map or an inventory grid.

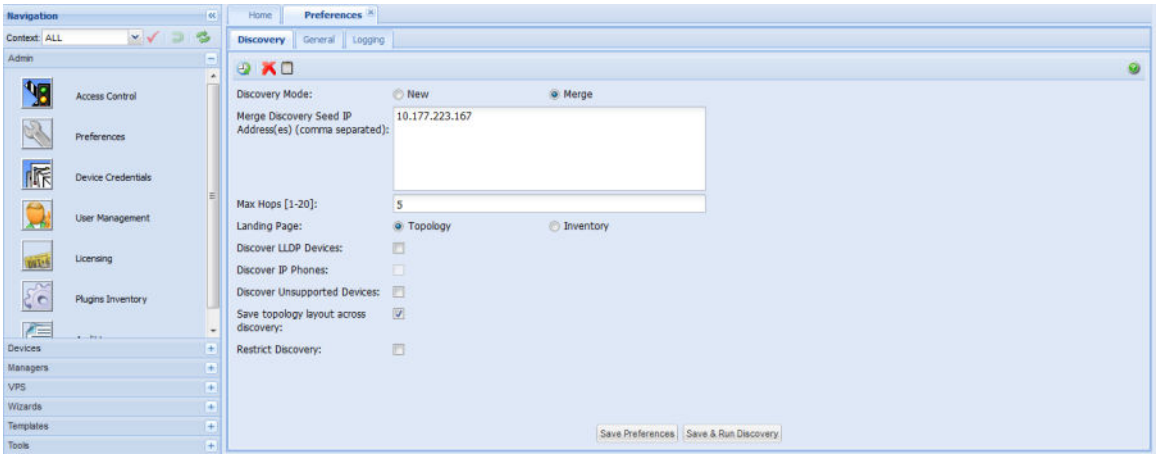
You have the option to launch a new or merged network discovery. The new or merged discovery creates or updates the topology map or inventory grid, respectively.

Perform the following procedure to configure a network discovery.

Procedure

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

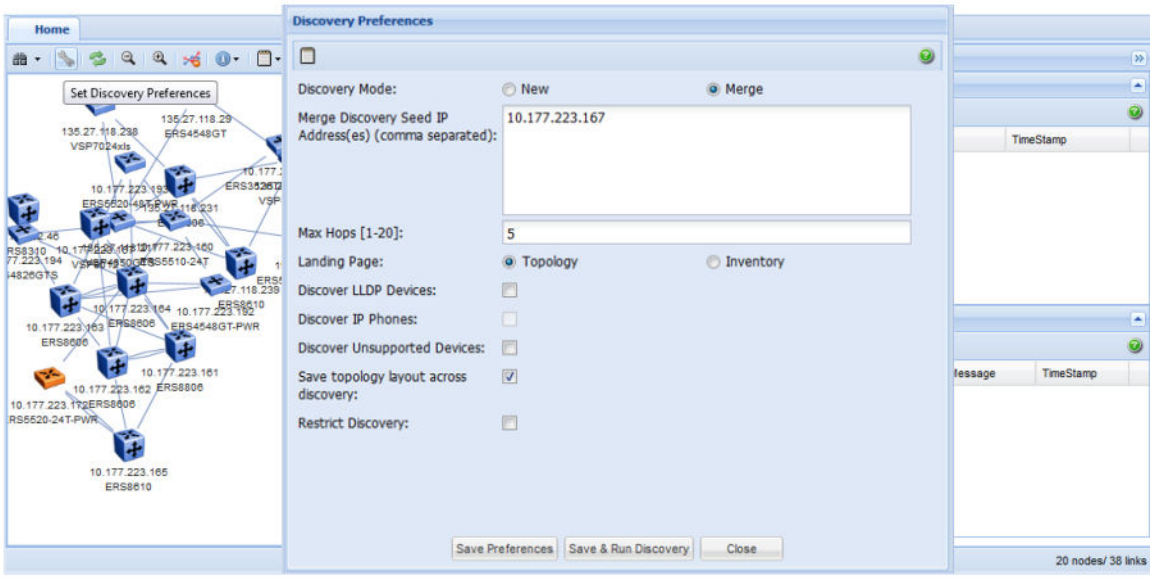
   The network discovery information displays in the contents pane.



   Or

   Navigate to the **Home** tab tool bar, and click **Set Discovery Preferences**.

   The Discovery Preferences window displays.



2. Specify whether you want to configure a new or a merged discovery:
   - New discovery—Run a new discovery when you want to introduce a device to your network.
   - Merged discovery—Run a merged discovery when you want to amend your device inventory without a new discovery.
3. In the **New Discovery Seed IP Address(es)** field, enter the IP address of one, or more than one, device in the network.

   Separate multiple IP addresses with a comma.
4. In the **Max Hops** field, enter the maximum number of hops.
5. Choose a landing page by selecting the corresponding **Landing Page** option.

   The default value is set to Topology. If you select the Inventory value, you are directed to the device inventory grid at log in.
6. Select the **Discover LLDP Devices** check box to discover Devices that support LLDP discovery. If this option is not selected, the **Discover IP Phones** option is disabled automatically.
7. Select the **Discover IP Phones** check box to discover the IP phones and to display the IP phones in the topology map. **Discover IP Phones** check box is enabled only if **Discover LLDP Devices** is selected.
8. Select the **Discover Unsupported Devices** check box to enable discovery of unsupported devices.
9. Select the **Save topology layout across discovery** check box to save the topology map.
10. Select the **Restrict Discovery** check box to restrict device discovery to only the devices entered in the subnets.

In the IP Address/addrLen dialog box, perform one of the following procedures:

- Click **Insert** to enter IP addresses.
- Click **Delete** to delete IP address.

11. Click **Save Preferences** or **Save and Run Discovery**.

Performing a network discovery

You can launch a network discovery to add or update device attributes and IP addresses on the network database. When you launch a discovery, the system either creates or updates network topologies and inventories. When the discovery is complete, the system connects the discovered devices to the other devices in the network inventory.

For information about setting device credentials, see *System Manager-Common Services Fundamentals* (NN48014-100).

Prerequisites

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 Configuration and Orchestration Manager (COM) to properly discover the device.

Procedure steps

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

   Note:

   To cancel the discovery process, click **Stop Discovery** on the dialog box.

2. An Info dialog box displays to confirm that the discovery is complete. Click **OK**.

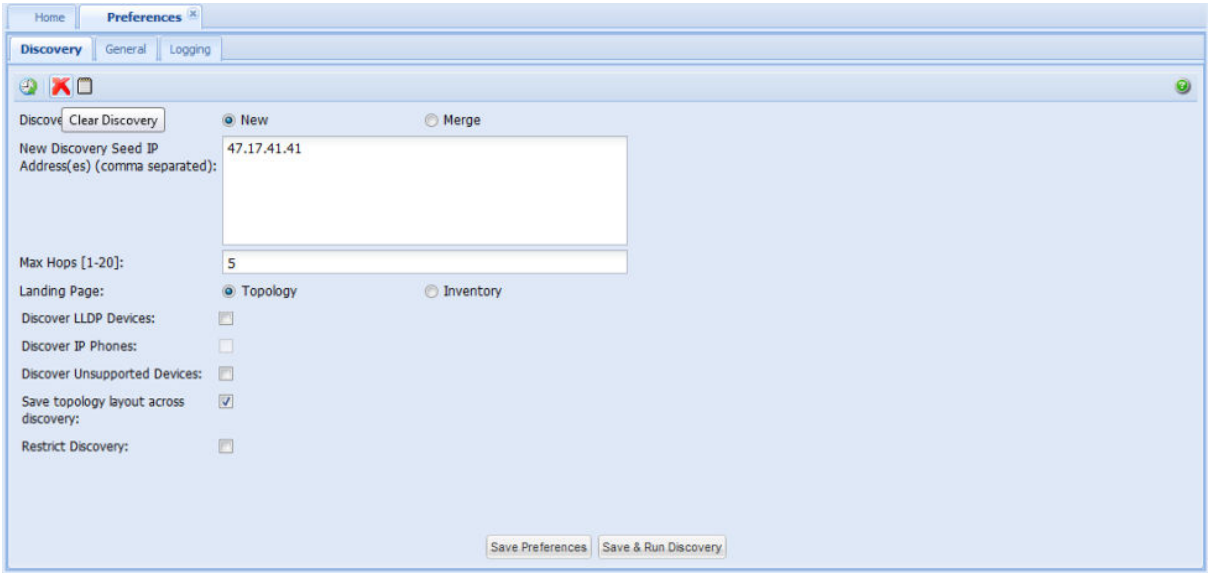
Clearing a discovery

Perform the following procedure to clear a discovery. If you clear a discovery, you clear all the devices in the topology map.

Procedure

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

2. From the Discovery tool bar, click **Clear Discovery**.



3. Click **Yes**.

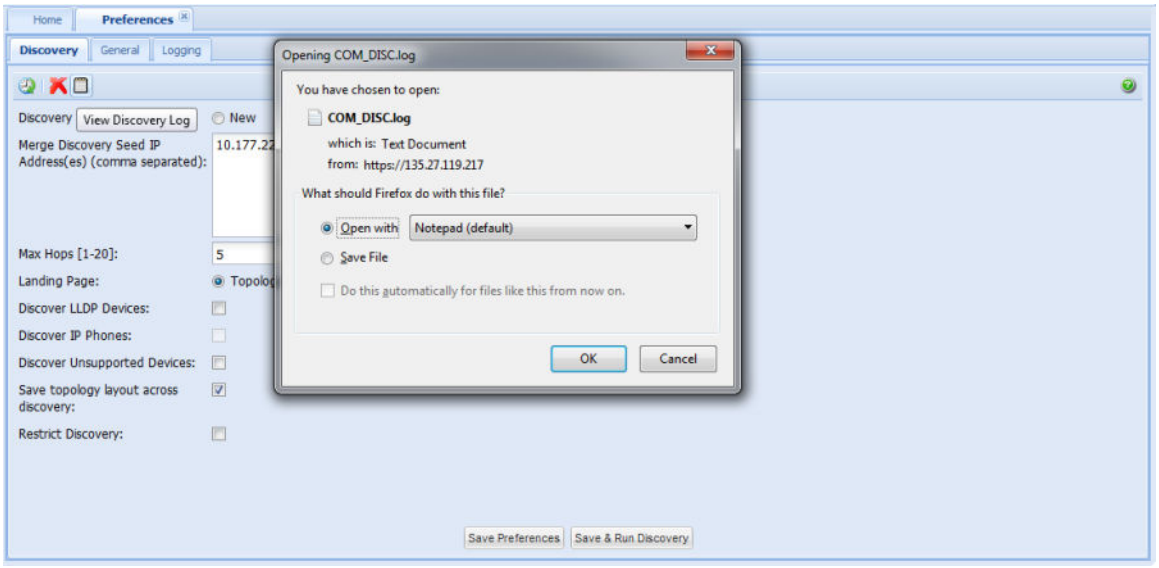
Viewing a discovery log

Perform the following procedure to view a discovery log.

Procedure

1. From the Navigation pane, open **Admin**, and then click **Preferences**.
2. From the Discovery tab tool bar, click **View Discovery Log**.

   The COM_DISC.log page displays.



3. Select **Open with** or **Save File** to open the COM Discovery log.
4. Click **OK**.

Updating discovery information

Perform the following procedure to refresh the topology view, and update the topology to include new devices.

Procedure steps

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

Scheduling a discovery

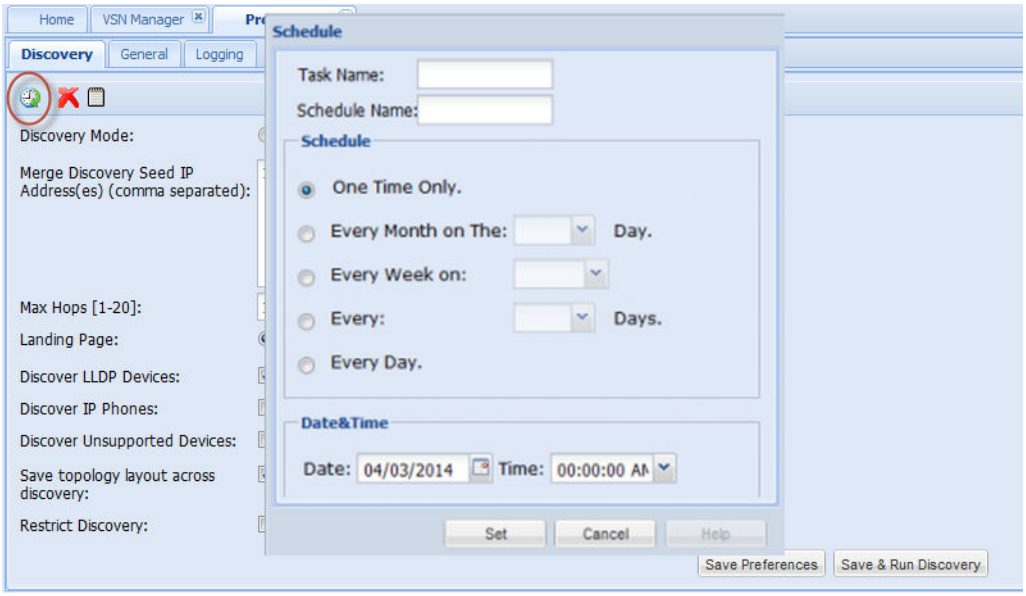
You can configure the Configuration and Orchestration Manager (COM) application to run scheduled network discovery jobs. You can set your discovery launch to occur one time, or repeatedly according to specific months, days of the week, date, and time. By scheduling your discovery event, you can run the discovery process without manual intervention. You also can schedule the discovery process to occur during off hours, therefore freeing up network resources.

Perform the following procedure to schedule a network discovery.

Procedure

1. From the Navigation pane, open **Admin**, select **Preferences**, and from the Discovery tab, click **Schedule Discovery**.

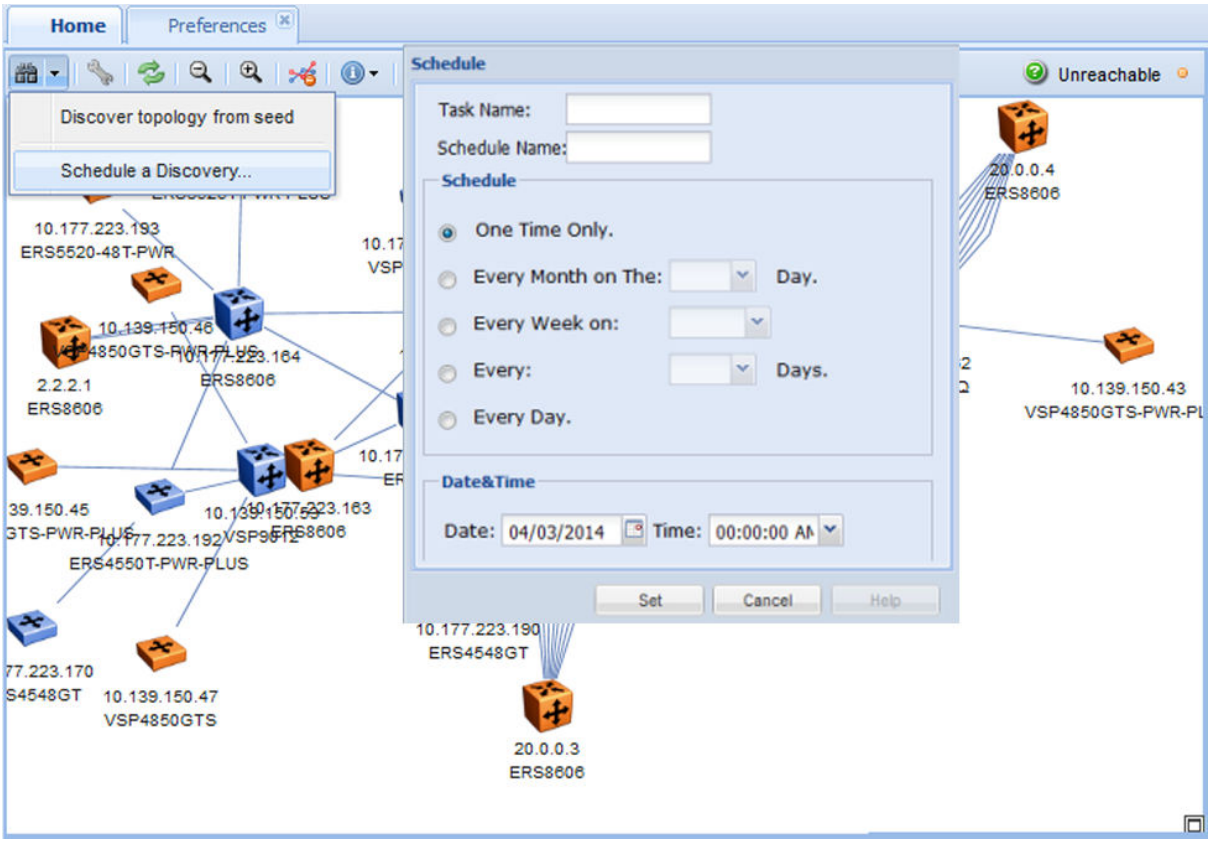
   The Schedule window displays.



Or

Navigate to the Home tab toolbar, and select **Discover Topology** > **Schedule a Discovery**.

The Schedule window displays.



2. In the **Task Name** field, enter a value to identify the task name.
3. In the **Schedule Name** field, enter a value to identify the discovery schedule.
4. In the Schedule section, select one of the following scheduling interval options:
   - One Time Only
   - Every Month on The: x Day.
   - Every Week on: x
   - Every: x Days.
   - Every Day.
5. In the Date section, specify the starting date and time values for the scheduled event in the **Date** and **Time** fields.
6. Click **Set**.

Next steps

You can manage a scheduled discovery event on the View Scheduled Task tab. You have the option to delete, stop, reschedule, or run a scheduled discovery event.

Managing a scheduled discovery

When you configure and save a scheduled discovery event, Configuration and Orchestration Manager (COM) adds the scheduled task to the system database. You then can access the discovery task list in the COM user interface to manage all scheduled events. On the View Scheduled Task tab, you can delete, stop, reschedule, and run a scheduled discovery event.

On the View Scheduled Task tab, you can view a list of scheduled discovery events. The list contains the information that you entered when you configured each scheduled discovery event. Also, the Executed column on the Task Details table, indicates how many times each scheduled task has run.

Perform the following procedure to manage a scheduled discovery event.

Procedure

1. From the Navigation pane, select **Tools**, and then select **Scheduled Tasks**.
2. On the Task Details table, select the event listing that you want to manage.
3. Use the buttons on the tool bar to manage the scheduled discovery event.

   The following table lists the options available.

Refresh	Refreshes the scheduled discovery event. You must refresh the listing after the scheduled discovery event has run.
Delete Task	Deletes the scheduled discovery event.
Cancel Task	Cancels the scheduled discovery event.

Reschedule Task	Reschedules the scheduled discovery event. When you select this option, the Schedule dialog box displays. Enter the new **Schedule** and **Date** field values, and click **Set** to save the new settings. Finally, perform a refresh to update the rescheduled discovery event listing on the Task Details table.
Run Task	Immediately runs the scheduled task. You must refresh the listing after the scheduled discovery event has run.

Viewing discovery results

This section provides information about managing the discovery results and displaying information on the topology map.

Managing the discovery results

You can use the tool bar buttons on the Home tab to manage the topology map. For example, you can zoom in and out of the device view, import or export device view values, or discover a topology.

Procedure steps

1. Select the **Home** tab.
2. Use the buttons on the tool bar to navigate the topology map.

   The following table lists the tool bar options that you can use to manage your topology map.

Table 1: Home tab tool bar options

Option	Description
Discover Topology	Use this option to perform the following actions: • Discover topology from seed • Schedule a Discovery You have the option to run a discovery based on a seed value. You also have the option to configure the COM application to run scheduled network discovery events. These events can occur one time or repeatedly according to specific months, days of the week, date, and time.
Set Discovery Preferences	Before starting a discovery for the COM system, you can enter the discovery preferences such as Seed, Hop Count, and Landing Page. You also can set the COM application to run one of the following types of discoveries: new or merged.
Refresh Device Topology	Use this option to refresh the topology view. The COM application communicates with the server to get the latest discovered devices.
Zoom Out	Use this option to zoom out the topology view.

Option	Description
Zoom In	Use this option to zoom in the topology view.
Clear Highlights	Use this option to clear the existing highlights on the topology map.
View Device Information	Use this option to display the port names, device types, and link details like link speed, type, mismatch, and duplex for devices in your topology. The View Device Information button has the following: • Display port names — Select this button to display port names on the topology map. • Toggle Addr / Name — Select this button to toggle the name and address of the device. • Link data — Select this button to perform the following actions: view link speeds, duplex, types, mismatch, and clear highlights.
Perform Device Action	Use this option to perform the following actions on a topology map device: • view port status • view connections • ping devices • view device properties • view a topology dump • view learned MAC addresses • launch an element manager • perform the following administrative actions: - create a group - update device topology - change IP address You also can access these options through the right-click menu of a device on the topology map or inventory grid.
Search for device IP / SysName	Use this option to search and highlight an IP address you are looking for. You can search based on: • a partial or full IP address • IPv4 format • IPv6 format **Important:** If the device is not found, then a topology dialog box appears showing, `No additional matches found`.

Option	Description
Save Topology	Use this option to 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. In previous versions of COM, if you saved the layout of a topology and rediscovered the network, the previously discovered devices maintain their layout position thereby eliminating the need to relay out the topology after each discovery.
Clear saved Topology	Use this option to return to the topology that you had previously saved.
Import/Export Topology	Use this option to export in xml and csv, and import in xml formats.
Reachable/Unreachable state	Use this option to display the connection status of the listed devices. 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 is down, or because the SNMP credentials provided to COM are not correct for the device in the unreachable state.
Device navigation window	Use the device navigation window, also called the panning window, to easily pan through the whole map to focus on a specific area of the network. Use Minimize and Maximize to show and hide the area behind the device navigation window.

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. From the tool bar, click **View Device Information**.

   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.

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

Managing the discovered devices

You can use Perform Device Action to manage the discovered devices on the topology map or inventory grid. Your device management takes place on the Home and on the Device Inventory View.

One set of device actions includes query management, such as ping devices, connection information, device properties, and port status. The second set of device actions includes administration management, such as update device topology and change IP address.

You can access these device actions through the tool bar buttons, or the menu options for a device you select.

Procedure steps

1. On the **Home** tab or **Device Inventory View** tab, select a device on the topology map or inventory grid and right-click on the device.

   Or

   On the **Home** tab or **Device Inventory View** tab, select a device on the topology map or inventory grid, and then click **Perform Device Action** on the tool bar.

2. Select an option from the drop-down menu.

   The following tables describe the device management options available from the Home tab and the Device Inventory View.

   - Device management options from the right-click menu on the topology on page 44
   - Device management options from the Home tab Perform Device Action button on page 45
   - Device management options from the Device Inventory View Perform Device Action button on page 46

The following table lists the device management options available after you click on a device on the topology.

Table 3: Device management options

Menu option	Description
Ping...	Use this option to ping the selected device from the server.
Show Connections	Use this option to display the neighbors of a device on the topology map. It does not display live connections, only what is on the topology map.
Properties	Use this option to display the following properties of the device: • Name • IP address • Device type • Location • Contact • Version • Uptime • Description
Launch Element Manager	Use this option to launch the element manager for the selected device.
Show All Traps For Device	Use this option to show all traps for a device.
Show Trap Highlight Details	Use this option to show trap highlight details of a device.
Port Status	Use this option to display the status of the port. • green—the port is in-service • red—the port is out-of-service • blue—the port is being tested
Dump Topology	Use this option to display the topology based on the real-time queries of devices.
Learned Mac Addresses	Use this option to display the learned Mac addresses on the selected device.
Administrative Actions	Use this option to change the device attributes. Perform one of the following actions: • Create a Group—This option appears on the topology map of the COM Home tab only. • Update device topology • Change device IP Address • Close The administrative actions prompt the system to discover a change to a single device with a one hop count. When the discovery is complete,

Menu option	Description
	the COM application updates the database with the discovered information.
Close	Closes the drop down menu.

The following table lists the device management options available after you select a device on the topology map, and then click Perform Device Action from the Home tool bar.

Table 4: Device management options from the Home tab Perform Device Action button

Menu option	Description
Show Port Status	Use this option to display the status of the port. • green—the port is in-service • red—the port is out-of-service • blue—the port is being tested
Show Connections	Use this option to display the neighbors of a device on the topology map. It does not display live connections, only what is on the topology map.
Ping Device	Use this option to ping the selected device from the server.
Show Properties	Use this option to display the following properties of the device: • Name • IP address • Device type • Location • Contact • Version • Uptime • Description
Dump Topology	Use this option to display the topology based on the real-time queries of devices.
Learned Mac Addrs	Use this option to display the learned Mac addresses on the selected device.
Launch Element Manager	Use this option to launch the element manager for the selected device.
Administrative Actions	Use this option to change the device attributes. Perform one of the following actions: • Create a Group—This option appears on the topology map of the COM Home tab only. • Update device topology • Change device IP Address The administrative actions prompt the system to discover a change to a single device with a one hop count. When the discovery is complete,

Menu option	Description
	the COM application updates the database with the discovered information.

The following table lists the device management options available from the Device Inventory View after you right-click on a selection on the inventory grid, or after you click Perform Device Action on the Device Inventory View tool bar.

Table 5: Device management options from the Device Inventory View Perform Device Action button

Menu option	Description
Show Port Status	Use this option to display the status of the port. • green—the port is in-service • red—the port is out-of-service • blue—the port is being tested
Ping Device	Use this option to ping the selected device from the server.
Show Properties	Use this option to display the following properties of the device: • Name • IP address • Device type • Location • Contact • Version • Uptime • Description
Dump Topology	Use this option to display the topology based on the real-time queries of devices.
Learned Mac Address	Use this option to display the learned Mac addresses on the selected device.
Launch Element Manager	Use this option to launch the element manager for the selected device.
Administrative Actions	Use this option to change the device attributes. Perform one of the following actions: • Update Device Topology • Change IP Address The administrative actions prompt the system to discover a change to a single device with a one hop count. When the discovery is complete, the COM application updates the database with the discovered information.

Working with multiple topologies

The Home tab on the Configuration and Orchestration Manager (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 View, and then discovery a new topology. To work with the saved topology, you can import it using the topology view or the Device Inventory View. When you import a saved topology, the existing topology is overwritten by the data in the imported file.

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 **Save Topology** on the toolbar, located to the right of the Search for device IP window.
3. In the confirmation dialog box, click **OK**.

Drawing a topology

You can create a network topology map from the inventory grid view. The system displays an inventory grid on the Device Inventory View tab after you set the discovery landing page preference to Inventory. After you select Draw Topology, the Configuration and Orchestration Manager (COM) application renders a logical topology map of your network.

Perform the following procedure to draw a topology form the inventory grid view.

Procedure

1. From the COM Navigation pane, select **Devices**.
2. From the Devices panel, click **Device Inventory View**.
3. From the Device Inventory View tool bar, click **Draw Topology**.

   The topology map renders and displays on the **Home** tab of the COM application.

Exporting and importing a topology from the Device Inventory View

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 Configuration and Orchestration Manager (COM).

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

Procedure steps

1. To save an existing topology, from the COM Navigation pane, select **Devices**.
2. From the **Devices** panel, click **Device Inventory View**.
3. From the Device Inventory View tool bar, click **Import/Export Inventory**.
4. Select **Export inventory to an XML file**, and then 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 View**.
10. From the Device Inventory View tool bar, click **Import/Export Inventory**.
11. Select **Import inventory from an XML file**, and then click **Browse** to navigate to the location of the file.
12. Select the file, and then click **Open**.
13. Click **Import**.

    The table in the Device Inventory View 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 Configuration and Orchestration Manager (COM).

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

Procedure steps

1. To save an existing topology, select the **Home** tab.
2. Click **Import/Export Topology**, located on the right side of the tool bar.
3. Select **Export inventory to an XML file**, and then 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 **Import/Export Topology** from the navigation pane.
8. Select **Import inventory from an XML file**, and then click **Browse** to navigate to the location of the file.

9. Select the file, and then click **Open**.
10. Click **Import**.

    The table in the Device Inventory View and the topology view are updated.

Using the Device Inventory View

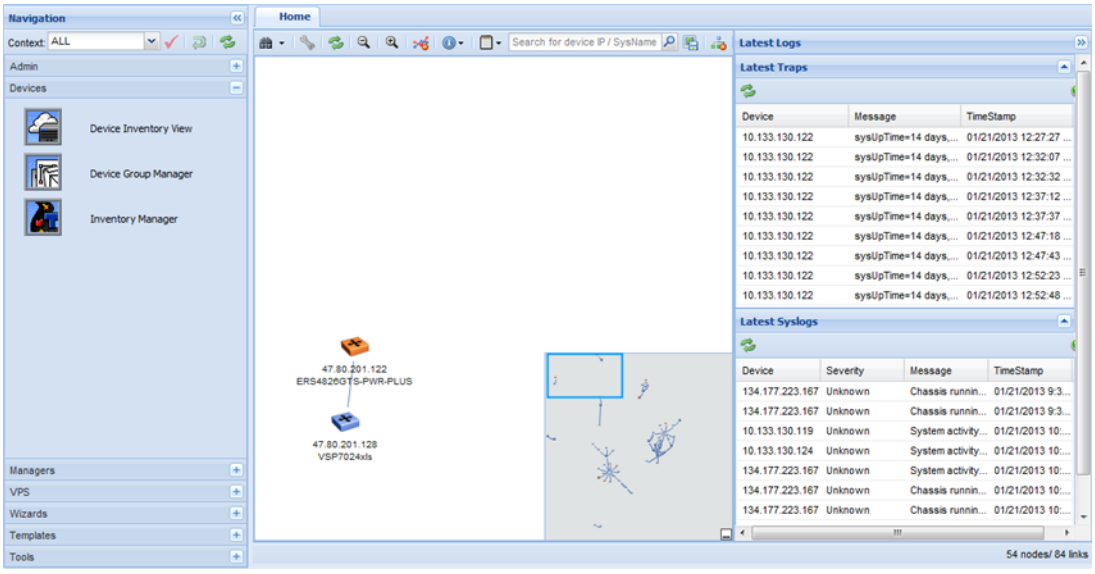
With the Device Inventory View, you can manage the Avaya Configuration and Orchestration Manager (COM) inventory. Configuration and Orchestration Manager provides a device inventory view of all the devices that are currently discovered in the network. You can sort the inventory list based on various device attributes.

Starting the Device Inventory View

Perform the following procedure to start the Device Inventory View.

Procedure steps

1. From the Configuration and Orchestration Manager Navigation pane, select **Devices**.



2. From the **Devices** panel, click **Device Inventory View**.

Device Inventory View tool bar options

You can use the tool bar options on the Device Inventory View to manage devices on the inventory grid. For example, you can launch the element manager, and perform device actions such as pinging and viewing connections.

You also can use the Device Inventory View to draw a device topology from the inventory grid.

The following table lists and describes the Device Inventory View tool bar options.

Table 6: Device Inventory View tool bar options

Option	Description
Perform Device Action	Use this option to perform the following actions on a topology map device: • Show Port Status—View port status. • Ping Device—Ping devices. • Show Properties—View device properties. • Dump Topology—View a topology dump. • Learned Mac Address—View learned MAC addresses. • Launch Element Manager—Open a new web page with the Element Manager for a device. • Administrative Actions—Perform the following administrative functions: - Update Device Topology - Change IP Address You also can access these options through the right-click menu of a device on the topology map or inventory grid.
Import/Export Inventory	Imports or exports the inventory from or to a XML file.
Refresh	Refreshes the device inventory information.
Draw Topology	Use this option to create a network topology map from the inventory grid view.
Filter	Filters the inventory view based on the following: • Device Type • IP Address (default) • Version • Name
Show All Inventory	Use this option to display all of the devices in the inventory as opposed to the ones in the device group.
Reachable	Indicates that the device is reachable.
Unreachable	Indicates that the device is unreachable.

Device inventory management

This section provides information about device inventory management.

Launching an Element Manager

Perform the following procedure to launch an element manager.

Procedure steps

1. From the Configuration and Orchestration Manager topology view, right-click on a device, and then select **Launch Element Manager**.

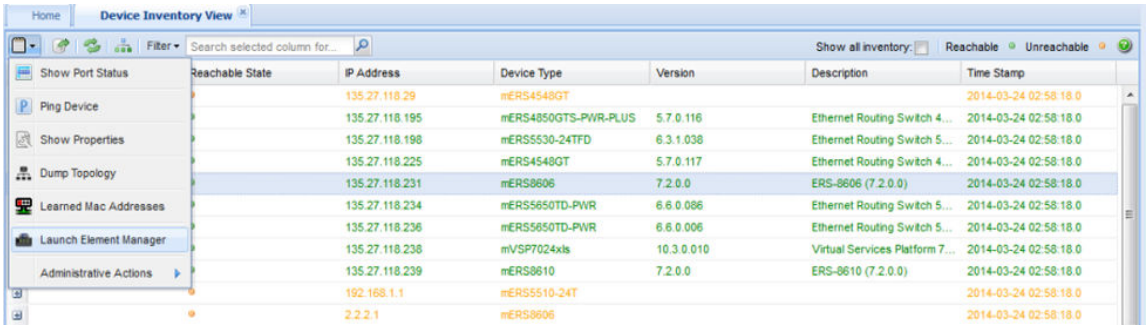
   Or

   From the Configuration and Orchestration Manager navigation pane, select **Devices**.

   a. Click **Device Inventory View**.

   b. Select a device from the Device table.

   c. From the Device Inventory View tool bar, click the down arrow next to Perform Device action, and then click **Launch Element Manager**.



   The system displays the Device Manager for the device.

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 the Java Virtual Machine (JVM) 1.6 application is not already installed in your system, then COM prompts you to install the application.

Note:

Before you can launch EDM, you must install the required EDM plugins using the Admin-> Plugin Inventory -> Install option. For more information installing EDM plugins, see *Avaya Configuration and Orchestration Manager Fundamentals* (NN47226–100).

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, and then from the topology view tool bar, select **Import/Export topology**

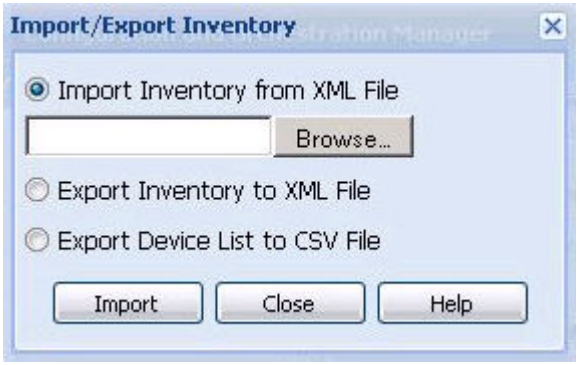
   Or

   From the Configuration and Orchestration Manager navigation panel, select **Devices**.

   a. Click **Device Inventory View**.

   b. Select a device from the Device table.

   c. From the Device Inventory View tool bar, click **Import/Export Inventory**.



2. To select the path of the .xml file, click **Browse**.
3. Click **Import**. Configuration and Orchestration Manager 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, and then click **Import/Export topology**

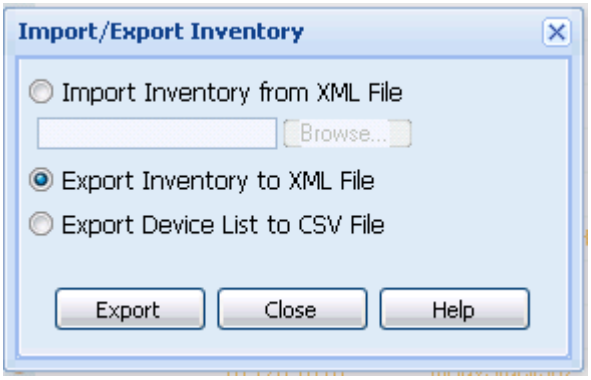
   Or

   From the Configuration and Orchestration Manager navigation panel, select **Devices**.

   a. Click **Device Inventory View**.

   b. Select a device from the Device table.

   c. From the Device Inventory View tool bar, click **Import/Export Inventory**.



2. Select **Export Inventory to XML File**, or **Export Device List to CSV File**.
3. Click **Export** .

Chapter 5: Create and manage device group assignments

You use the Device Group Manager to create and manage device and group assignments. You can use device groups to group a number of discovered devices from a single repository. You can use group assignments to control access to these grouped devices through context settings. The context setting defines device group accessibility for users based on their domain of responsibility. The context setting also determines whether device map topologies render for users at login.

The Device Group Manager contains two notable features: groups and user groups.

Groups

Groups are a collection of devices that you can create from the device repository. You use the **Groups** tab in Devices –> Device Group Manager to create device groups. When you create device groups, you then have the ability to create and assign user groups to device groups. The group and user assignments determine the devices that users see on a topology map when they log in to the COM application.

Group assignments

User groups are a collection of users that you create to control access to device groups. You use the **Group assignments** tab in Devices –> Device Group Manager to create user groups. When you create user groups, you must associate users these groups. The user and user group assignments, along with the context assignment, determine the devices that a user can access.

Starting the Device Group Manager

You can launch Device Group Manager to gain access to device and user groups. In the Device Group Manager you can create device groups to group discovered devices from the single repository. You also can create user groups to assign device group accessibility to COM users.

The Device Group Manager is included in the COM_50_base license.

Complete the following steps to start the Device Group Manager:

Procedure

1. In the Configuration and Orchestration Manager Navigation tree, expand **Devices**.
2. Click the **Device Group Manager** icon.

The Device Group Manager window displays the device and user groups in the **Groups** and **Group Assignments** tabs.

Next steps

Click **Add** on the **Groups** or **Group Assignments** tab to create and manage device and user groups.

Device Group Manager toolbar options

You can use the toolbar options on the **Device Group Manager** tab to create and manage device and group assignments. For example, you can create device and user groups, edit devices or users in the individual groups, and highlight groups on a topology map.

You use device groups to group a number of discovered devices from the single repository. You then assign device groups to users. Each user can have multiple group assignments, but only on context setting or device group. You can access the **Device Group Manager** tab by selecting the **Device Group Manager** icon in the Configuration and Orchestration Manager Navigation tree.

The following table lists and describes the Device Group Manager toolbar buttons available for your use in both the **Devices** and **Group Assignments** tabs.

Table 7: Device Group Manager toolbar options

Option	Description
Refresh	Use this option to refresh the device and user group view. The COM application communicates with the server to get the latest list of device and user groups.
Add Device Group or Add User Group	Use this option to add a device group or a user group. When you select **Add Device Group** or **Add User Group** the Add Group window displays.
Delete Device Group or Delete User Group	Use this option to delete a device group or a user group from the system. You can delete a group only if the group is not associated to a user. If you delete a user group, the current context of the user is also removed from the system; no device list is displayed.
Apply Changes	Use this option to apply any changes that you make to the device group or user group.
Revert Changes	Use this option to revert any changes that you make to the device group or user group.
Highlight on Topology	Use this option to highlight a device group on the topology map. **Note:** Option is visible on **Groups** tab only.

Device Group Manager group and user management

This section provides information about device and user group management.

Creating a device group

You create a device group to group a number of discovered devices from the single repository. When you create device groups, you then have the ability to create and assign user groups to device groups. The group and user assignments determine the devices that users see on a topology map when they log in to the COM application.

When you create a device group, the devices that you add to the group must be in the device inventory at the time of the group creation. If you should remove devices from the inventory and then run a merged discovery, the removed devices are highlighted in red.

By default, the COM application has a standard device group called ALL. The ALL group contains all the devices in the inventory. The ALL group device list is updated every time that you run a discovery. You do not have the ability to edit the ALL device group.

You can create device groups in the **Device Group Manager** tab. You can access the Device Group Manager tab by selecting the **Device Group Manager** icon in the Configuration and Orchestration Manager Navigation tree.

Perform the following procedure to create a device group.

Procedure

1. On the Groups tab, select **Add Device Group**.

   The Add Group window displays.

2. In the **Group Name** field, enter a name that uniquely identifies the device group.
3. In the **Devices** field list, select the devices that you want to add to the device group.

   You can use the **Search** field to search or filter devices that are displayed on the list. You can search for a complete or partial device IP.

4. Click **Save**.

Editing a device group

You can edit a device group to add or remove devices from the selected device list. With the exception of the ALL group, you edit any device group in the COM database. The devices that you add or remove from the device list impact the devices that users see when they log in to the COM application.

Perform the following procedure to edit a device group.

Procedure

1. On the **Group** tab in the **Device Group Manager** tab, double click the device group listing that you want to modify.
2. Edit the appropriate fields.
3. Select **Apply Changes**.

Result

A notification window displays and informs all users that are associated to the applicable device group that device group changes have taken place. Users must select **Refresh** to update their device lists.

Highlighting a device group on the topology map

You can use **Highlight on Topology** on the **Device Group Manager** tab to highlight device groups on a topology map. This map highlighting feature provides a visual indication of the user-assigned device groups on the topology map.

Procedure

1. On the **Groups** tab, select the device group row that you want to work with.
2. Select **Highlight on Topology**.

   The system highlights the device group on the topology map.

Creating a user group

You create a user group to group a number of users that are listed in the COM database. You use user groups to control access to grouped devices through context settings. The context setting defines device group accessibility for users based on their domain of responsibility. The context setting also determines whether device map topologies render for users at login.

When you create user groups, you must associate users to these groups. The user and user group assignments, along with the context assignment, determine the devices that a user can access. The context value represents a device group.

You can create user groups in the **Device Group Manager** tab. You can access the **Device Group Manager** tab by selecting the **Device Group Manager** icon in the Configuration and Orchestration Manager Navigation tree.

Perform the following procedure to create a user group.

Procedure

1. On the **Group Assignments** tab, select **Add User Group**.

   The Add User Group window displays.

2. In the **User** field, enter the name of the user that you want to add to the user group.
3. In the **Current Context** field, enter the name of the group that you want to add.
4. In the **Groups** field list, select the user groups that you want to associate to the user.

   You can use the **Search** field to search or filter user group that are displayed on the list. You can search for a complete or partial group name.
5. Click **Save**.

Editing a user group

You can edit a user group to modify the current context value that is associated to a user. With the exception of the ALL group, you edit any user group in the COM database. The context values that you add or remove from the user group list impact the devices that users see when they log in to the COM application.

You can edit a user group using the user group using Device Group Manager or you can edit a user group using the Context option in the Navigation panel.

Editing a user group using the Device Group Manager

About this task

Perform the following procedure to edit a user group using the Device Group Manager.

Procedure

1. On the **Group Assignments** tab in the Device Group Manager, double click the user group listing that you want to modify.
2. Edit the **Current Context** field.
3. Select **Apply Changes**.

Result

A notification window displays and informs all users that are associated to the applicable user group that group changes have taken place. Users must select **Refresh** to update the context settings.

Editing a user group in the Navigation panel

About this task

Perform the following procedure to edit a user group using the Context option in the Navigation panel.

Procedure

1. In the Context field, select the user group listing that you want to modify.
2. Edit the **Current Context** field.
3. Select **Save Context**.

Result

A notification window displays and informs all users that are associated to the applicable user group that group changes have taken place. Users must select **Refresh Groups** to update the context settings.

Chapter 6: 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 an STG, the device uses 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 9000 because they are not supported.

  Note:

  In the VLAN Manager, Wireless Controller (WC) devices do not support the MSTP mode.

  Note:

  In VLAN Manager, VSP 8000 devices do not support STG, IPV6, and NSNA Only byPort, byProtocol and spbm-bvlan vlan types are supported.

- **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.

  Switched UNI Vlans can be created for VSP 7000 v10.2 and above and ERS 4800 v5.7 and above devices under Avaya STG and MSTP instances.

  Note:

  Switched UNI Vlan type cannot be created under RSTP instances as SPBM is not supported in RSTP mode.

- **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 ERS5600 devices. The workflow of VLAN manager for the WC is similar to the ERS5600 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.

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.

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 devices support RSTP and MSTP, but do not support Avaya STG protocol.

Note:

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

Table 8: Maximum STGs and VLANs supported by switches on page 61 lists the details for different switches.

Table 8: 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
Virtual Services Platform 9000	64	4096
Virtual Services Platform 7000	8	4096
Virtual Services Platform 4000	0	4084
Virtual Services Platform 8000	64	4060
Wireless Controller	8	256

VLAN Manager features

The VLAN Manager supports the following types of VLANs and STGs:

- VLANs:
  - port-based
  - protocol-based
  - subnet-based
  - source MAC address-based

- sVLAN-based
- ID-based
- spbm-bvlan-based
- private type

- STGs:
  - Avaya STGs
  - RSTP
  - MSTP

The VLAN Manager allows you to do the following:

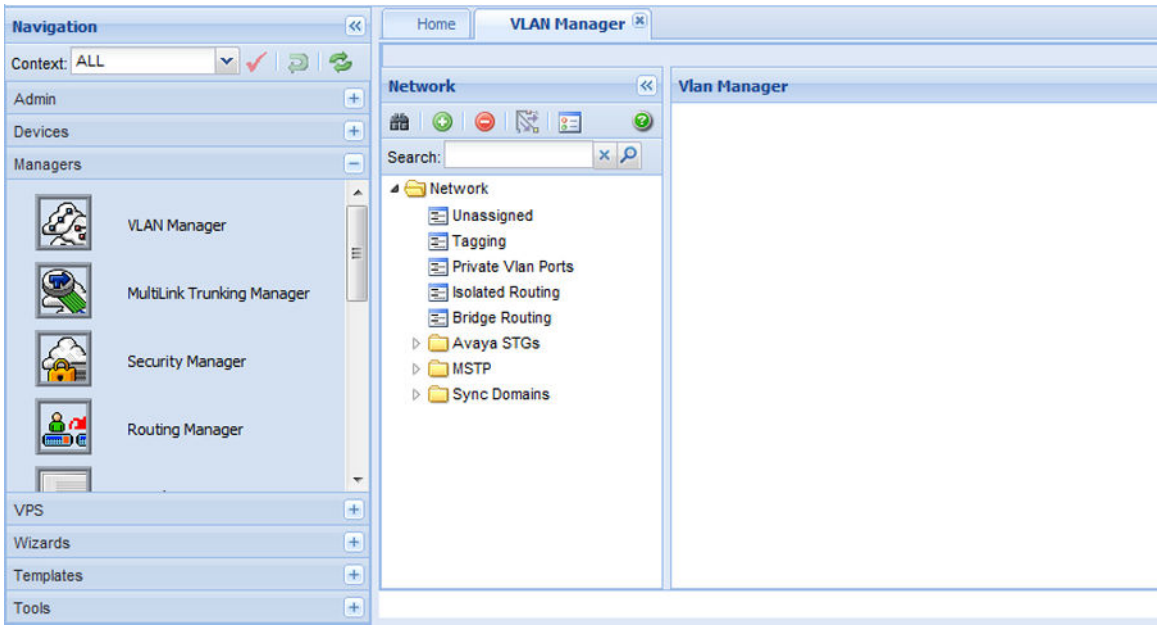
- Configure and monitor VLANs and STGs across one or multiple devices.
- View and edit port membership information for the following:
  - ports not belonging to an STG
  - ports belonging to multiple STGs
  - individual routing ports and brouter ports

  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 95.

Starting VLAN Manager

In the COM Navigation pane, expand the managers and click **VLAN Manager**. The VLAN Manager launches and displays in the content pane.



Using the VLAN Manager window

This section details the VLAN Manager interface.

Table 9: VLAN Manager window on page 64 describes the parts of the VLAN Manager window.

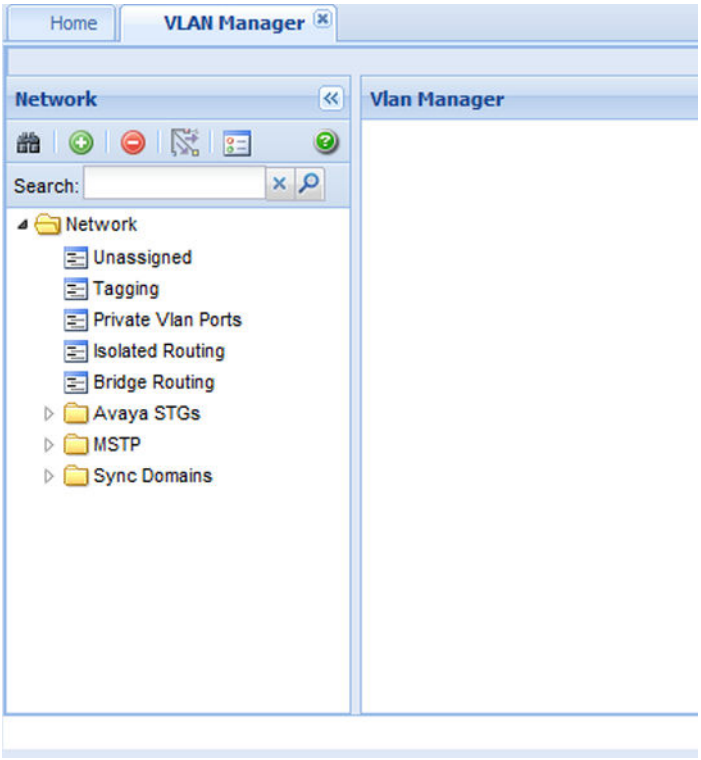


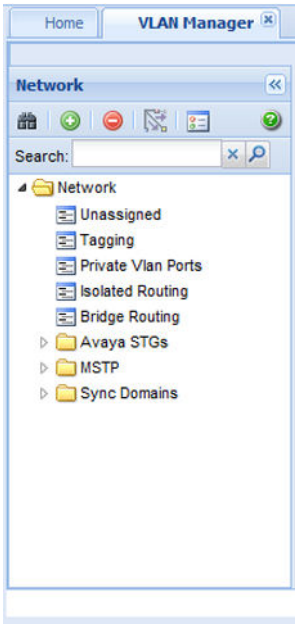
Table 9: VLAN Manager window

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 64.
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 66.
Status bar	Displays status information, it includes discovery information, type of node highlighted, and command status. For more information, see Status bar on page 67.

Navigation pane

The VLAN Manager Navigation pane provides access to all VLAN Manager resources.

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.



The following table details the VLAN Manager Navigation pane.

Table 10: 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, Private VLAN Ports, Isolated Routing, and Bridge Routing. For more information, see Port membership types on page 91.
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 95.
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 106.

Navigation pane toolbar

You can add, or delete VLANs and STGs using the Navigation pane toolbar. You can also highlight MLT constructs on the Topology Map using the Highlight on Topology buttons as shown in the following figure.

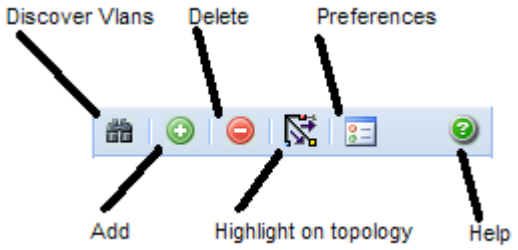


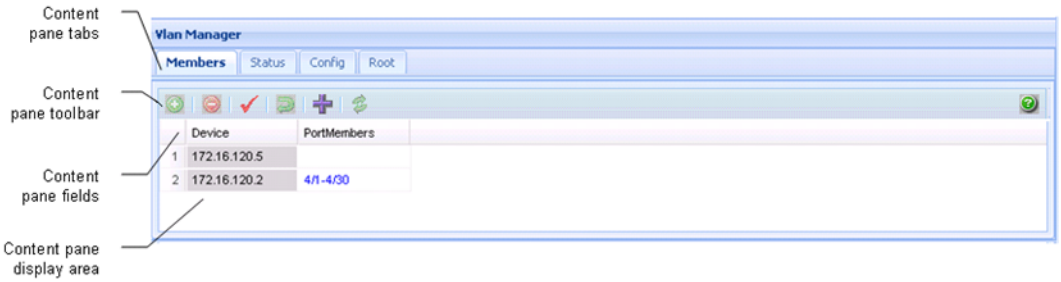
Table 11: Navigation pane toolbar fields

Button	Description
Discover Vlans	Manually starts the Vlan discovery process.
Add	Adds Vlans and STGs to the network.
Delete	Removes 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.



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

Table 12: 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.
Export	Export report.
Add VRRP	Insert a VRRP interface on a VLAN.
Synchronize VLAN name	Synchronize the VLAN name.
Search field	Search by Device, sysName, Ports, or Select All. Type text to search and click **Enter**.

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 13: 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 97.

Creating and configuring Avaya Spanning Tree Groups

This section describes how to create and modify Avaya STGs. This section also provides information about Avaya STG membership.

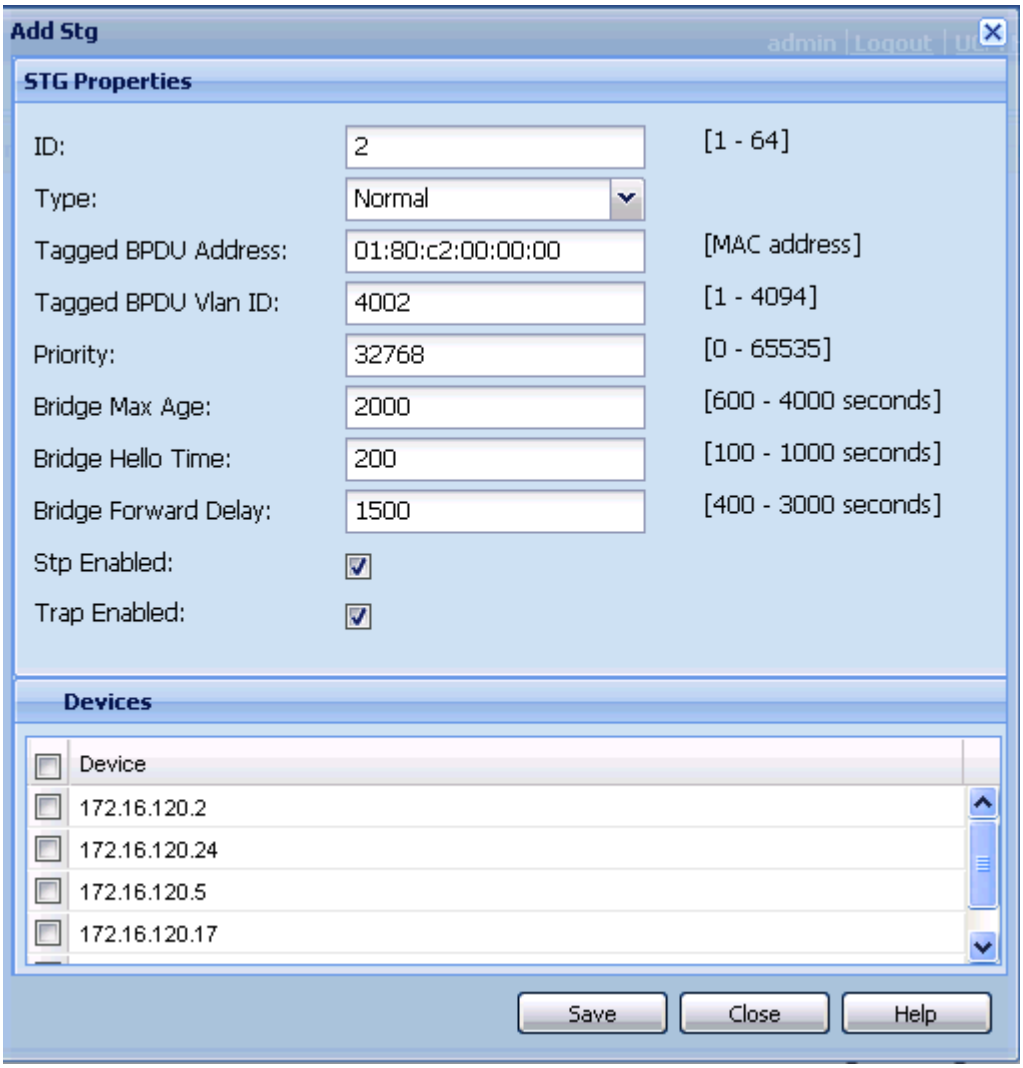
Creating an Avaya Spanning Tree Group

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

Procedure steps

1. From the Navigation pane, expand **Network** and then select **Avaya STGs**.
2. Select **STG**.
3. Click **Add**.

The Add STG dialog box displays.



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

Add STG dialog box fields

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

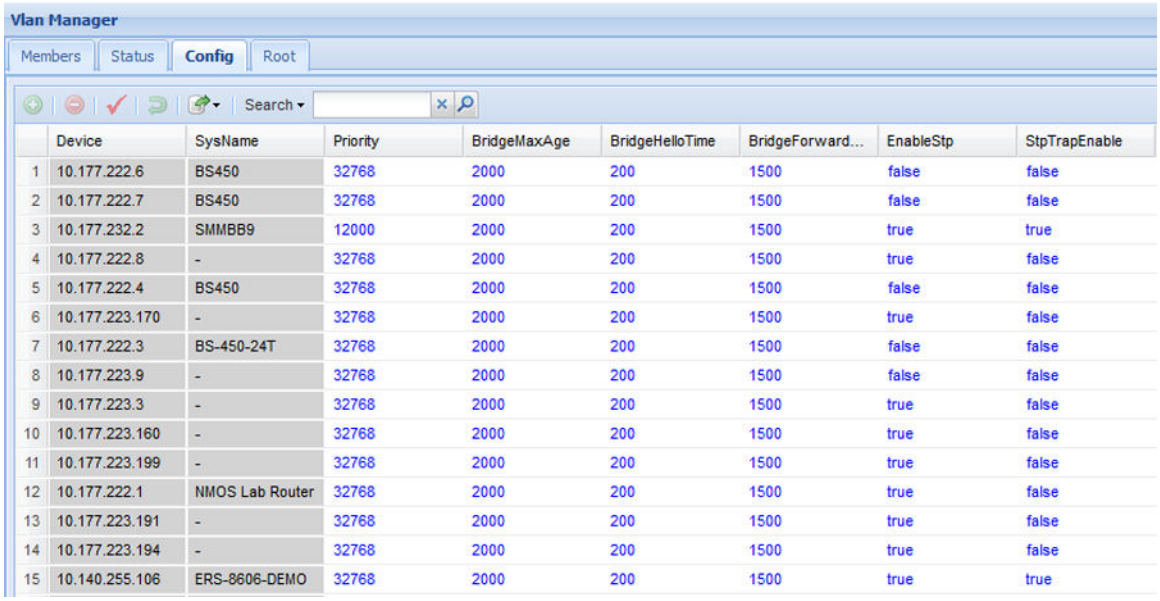
Table 14: Add STG dialog box items

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.

Field	Description
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. **Important:** 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

In the Navigation pane, open an Avaya STG and select **Config** to view and configure Avaya STG parameters.



	Device	SysName	Priority	BridgeMaxAge	BridgeHelloTime	BridgeForward...	EnableStp	StpTrapEnable
1	10.177.222.6	BS450	32768	2000	200	1500	false	false
2	10.177.222.7	BS450	32768	2000	200	1500	false	false
3	10.177.232.2	SMMBB9	12000	2000	200	1500	true	true
4	10.177.222.8	-	32768	2000	200	1500	true	false
5	10.177.222.4	BS450	32768	2000	200	1500	false	false
6	10.177.223.170	-	32768	2000	200	1500	true	false
7	10.177.222.3	BS-450-24T	32768	2000	200	1500	false	false
8	10.177.223.9	-	32768	2000	200	1500	false	false
9	10.177.223.3	-	32768	2000	200	1500	true	false
10	10.177.223.160	-	32768	2000	200	1500	true	false
11	10.177.223.199	-	32768	2000	200	1500	true	false
12	10.177.222.1	NMOS Lab Router	32768	2000	200	1500	true	false
13	10.177.223.191	-	32768	2000	200	1500	true	false
14	10.177.223.194	-	32768	2000	200	1500	true	false
15	10.140.255.106	ERS-8606-DEMO	32768	2000	200	1500	true	true

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).
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
- spbm-switchedUni 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

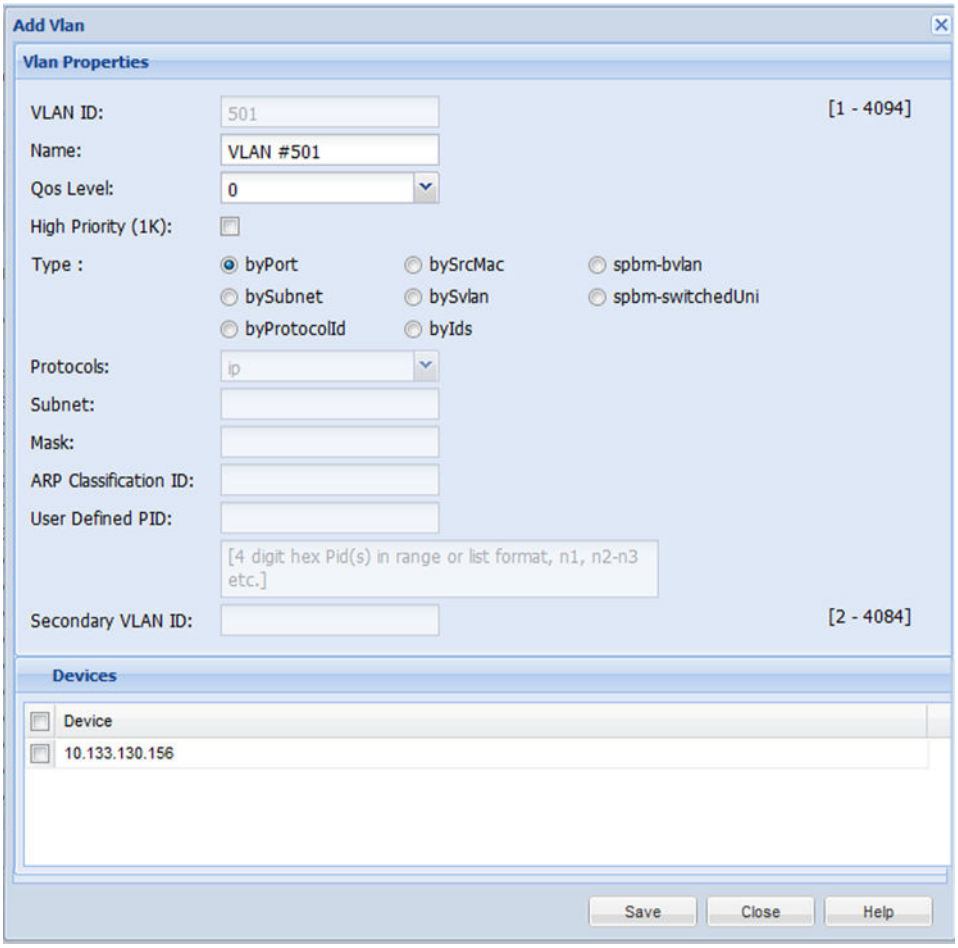
Perform the following procedure to create a port based VLAN.

Procedure steps

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

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

   The Add Vlan window displays.



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 (option). If a name is not entered for the VLAN, a default name 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 are 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 VLAN table displays in the General tab in the contents pane.
3. Select a device in the contents pane.
4. Click **Add** to insert a subnet based VLAN.

   The Add Vlan window displays. For an example of the Add Vlan window, see Creating a port based VLAN on page 73 .
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 a name is not entered for the VLAN, a default name 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 Add Vlan window 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 are 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 pane, expand **Network** folder, and then select **Avaya STGs** folder.
2. Select **STG**.

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

   The Add Vlan window displays. For an example of the Add Vlan window, see Creating a port based VLAN on page 73
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 a name is not entered for the VLAN, a default name 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 Add Vlan window that apply to a protocol Id based VLAN are activated.
10. In the **Protocol** field, select the required protocol from the 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 are 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 VLAN table displays in the General tab in the contents pane.
3. Select a device in the Content pane.
4. Click **Add** to insert a source MAC address based VLAN.

   The Add Vlan window displays. For an example of the Add Vlan window, see Creating a port based VLAN on page 73 .
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 a name is not entered for the VLAN, a default name 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 Add Vlan window 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 are 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 pane, expand **Network** folder, and then select **Avaya STGs** folder.
2. Select **STG**.

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

   The Add Vlan window displays. For an example of the Add Vlan window, see Creating a port based VLAN on page 73 .
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 a name is not entered for the VLAN, a default name 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 Add Vlan window 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 are 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 VLAN table displays in the General tab in the contents pane.
3. Select a device in the Content pane.
4. Click **Add** to insert an ID based VLAN.

   The Add Vlan window displays. For an example of the Add Vlan window, see Creating a port based VLAN on page 73 .
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 a name is not entered for the VLAN, a default name 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 **bylds** type option.

   Other items in the Add Vlan window 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 are absent from the device list.
11. Click **Save** to save all the changes.

Creating an spbm-bvlan

Perform the following procedure to create an spbm-bvlan.

Prerequisites

- ERS 8600/8800 v 7.1 switch, VSP 7000 v 10.2, or VSP 9000 series

- mib attribute rcPlsbGlobalEnable set to true.

Note:

In the case of the VSP 7000 series, the STG/MSTP id is not used for creating a spbm-bvlan. These spbm-bvlans will be displayed under "STG 0" or "msti-0".

Procedure steps

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

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

   The Add Vlan window displays. For an example of the Add Vlan window, see Creating a port based VLAN on page 73 .
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 a name is not entered for the VLAN, a default name 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 Add Vlan window 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 are absent from the device list.
11. Click **Save** to save all the changes.

Creating a spbm-switched Uni Vlan

Switched UNI is supported on VSP 7000 v10.2 and ERS4800 v5.7.

About this task

Perform the following procedure to create a spbm-switched Uni Vlan.

Procedure

1. From the Navigation pane, expand **Network** folder, and then select **Avaya STGs** folder.
2. Select one of the following:
   - STG for Avaya STG instances

- CIST/msti for MSTP instances

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

3. Select a device in the Content pane.
4. To insert an spbm-based VLAN, click **Add**.

   The Add Vlan window displays. See Creating a port based VLAN on page 73
5. In the **VLAN ID** field, type the VLAN ID. The value can be from 1 to 4096 (switched UNI supports 4096 Vlans), as long as it is not already in use.
6. In the **Name** field, type the VLAN name (optional). If a name is not entered for the VLAN, a default name is created.
7. Select the QoS Level and specify whether the VLAN traffic is to be tagged as High Priority (1K).
8. From the **Type** field, select the **spbm-switched Uni** option.

   Other items in the Add Vlan window that apply to a port-based VLAN are activated.
9. Select the VSP 7000 or ERS4800 devices to be configured from the Device pane.

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

   Devices that do not support spbm-switchedUni VLANs are absent from the device list.
10. 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: • by port • by subnet • by protocol • by source MAC Address • by SVLANs

Field	Description
	• by ID • by spbm-bvlan
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.

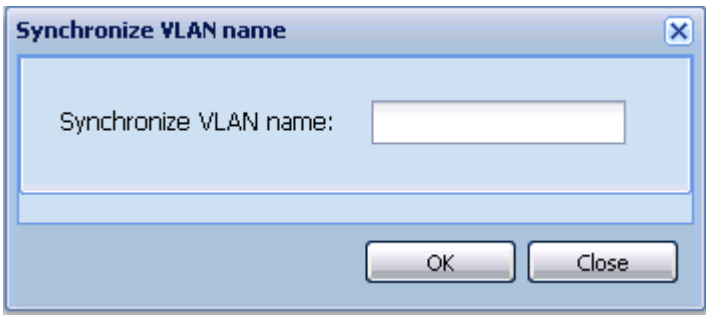
Synchronizing VLAN name

Perform the following procedure to synchronize the VLAN name.

Procedure steps

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

   The Synchronize VLAN name dialog box displays.



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

Managing Rapid Spanning Tree Protocol

The following section describes how to edit Rapid Spanning Tree Protocol (RSTP) instances and provides information about RSTP membership.

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 pane, 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 display in bold.
5. On the VLAN Manager toolbar, click **Apply Changes**.

Creating and configuring VLANs for Rapid Spanning Tree Protocol

This section describes 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 displays.
3. Insert values or select options in the option boxes.
4. Click **Ok**.

Note:

spbm-switchedUni Vlan is not supported under RSTP.

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 displays.
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 displays.
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

This section describes how to add and delete Multiple Spanning Tree Protocol (MSTP) instances and provides information about MSTP membership.

Adding an MSTI in Multiple Spanning Tree

Perform the following procedure to add an MSTI instance.

Procedure steps

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

   The **Add MSTP** dialog box displays.
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 displays.

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 display in bold.
7. On the VLAN Manager toolbar, click **Apply Changes**.

Managing VLANs for MSTP

This section describes how to create and delete VLANs for Multiple Spanning Tree Protocol (MSTP) instances, as well as how to add members to a VLAN group.

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

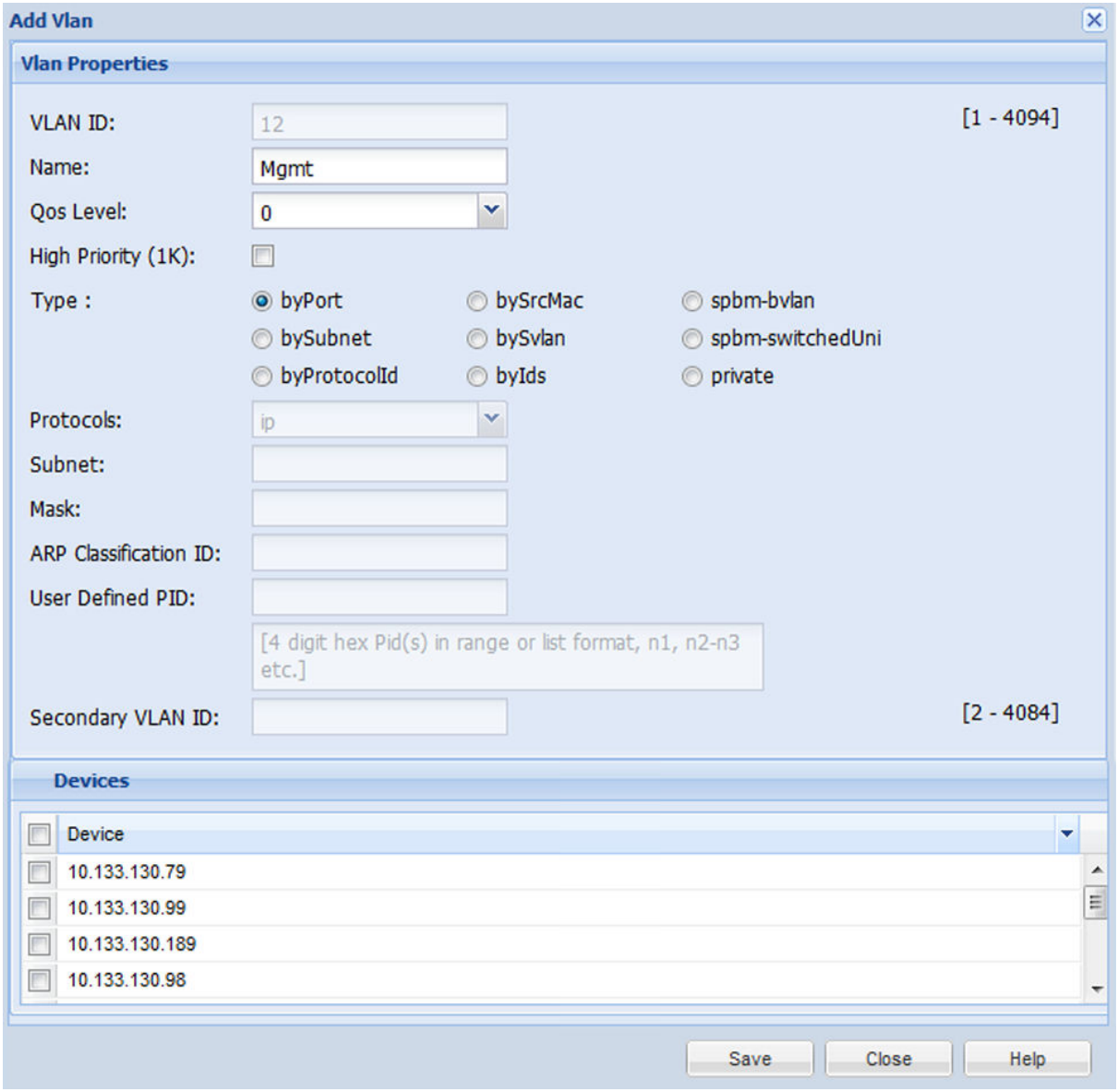
Adding members to a VLAN in Multiple Spanning Tree

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

Procedure steps

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

   The Add Vlan window displays .



3. 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.
4. In the **Name** field, type the VLAN name (optional). If a name is not entered for the VLAN, a default name is created.
5. Select the QoS Level and specify whether the VLAN traffic is to be tagged as High Priority (1K).
6. From the **Type** field, select the **byPort** option.

   Other items in the Add Vlan window that apply to a port-based VLAN are activated.
7. 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 are absent from the device list.

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

Private VLAN

This section provides an overview of Private VLANs.

Mark private Vlan ports

Before a port is added to a private vlan it must be marked or identified as isolated, promiscuous, or trunk. By default, a port is set to none.

A port that is either promiscuous or isolated can only have private VLANs on that port.

Note:

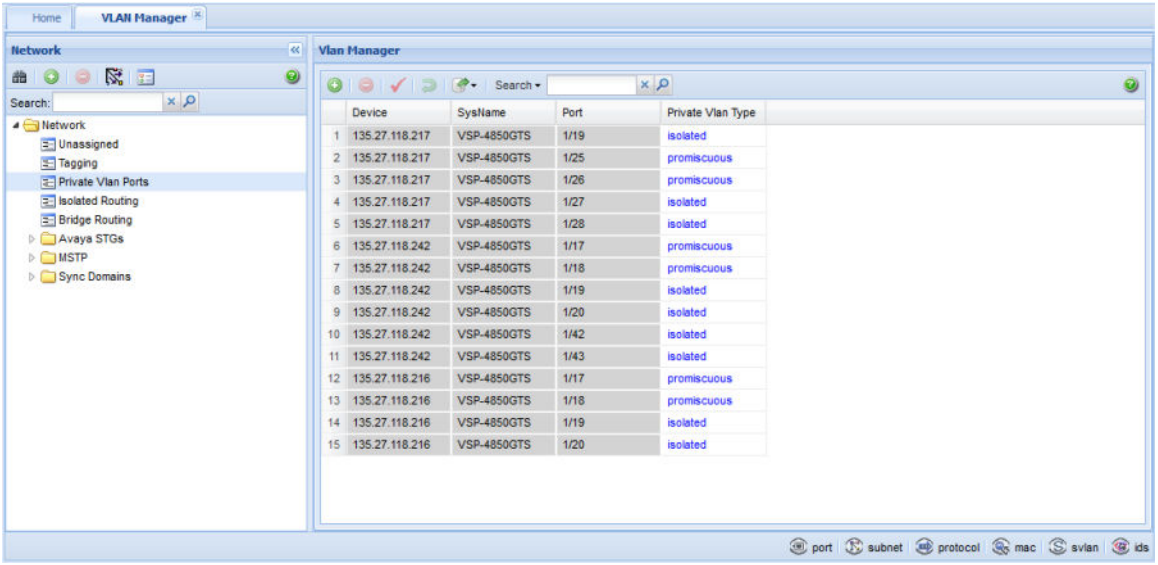
When the user configures the private VLAN type of a port to trunk, the port is tagged automatically.

Marking private VLAN ports

Procedure steps

1. From the Navigation pane, select **Private VLAN Port**.
2. Select the Private VLAN Port.

Only the Private VLAN capable devices and Promiscuous, Isolated, and Trunk ports display.



If you configure Private VLAN Port as Trunk, the port is tagged automatically

Add private VLANs in Multiple Spanning Tree

A private VLAN consists of two VLANs, the primary VLAN and the secondary VLAN. The user must specify the two VLANs so that they can be associated. All the ports in the private VLAN must be marked as isolated, promiscuous, or trunk. Trunk ports must have VLAN encapsulation enabled. A port can be a single port or can be a member of an MLT.

A port that is of private VLAN type trunk must be tagged. Isolated and promiscuous private VLAN ports can be either tagged or untagged. The primary and secondary VLAN values on multiple devices should be configured to be the same.

Adding a Private VLAN in Multiple Spanning Tree

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

Procedure steps

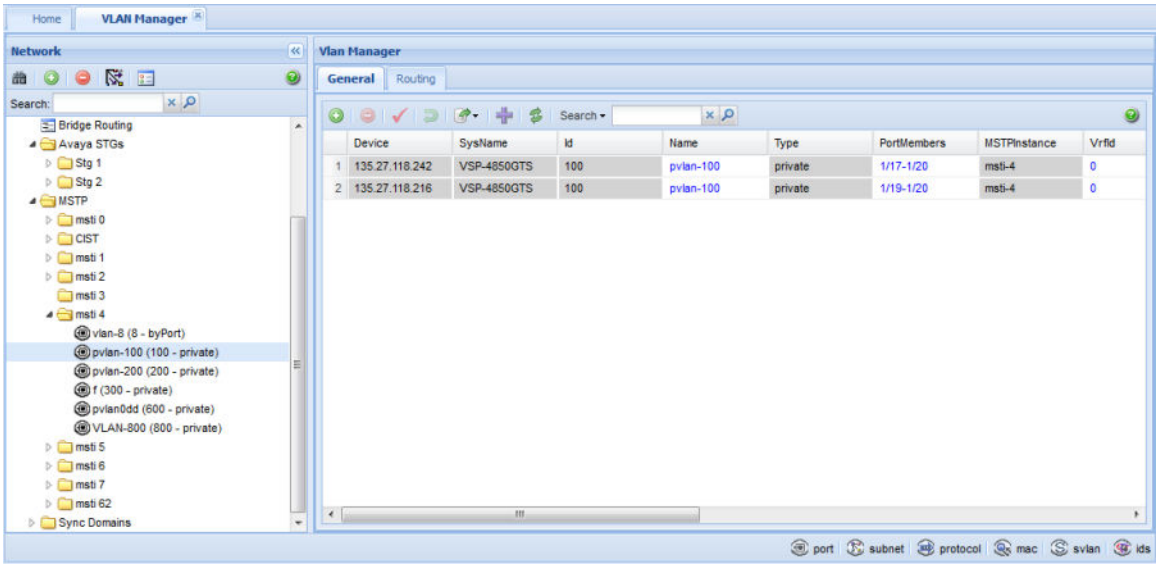
1. From the Navigation pane, select the **MSTP** folder.
2. Select the **CIST** folder or an **MSTI** folder.
3. On the VLAN Manager toolbar, click **Add**.

   The Add Vlan window displays. For an example of the Add Vlan window, see Adding members to a VLAN in Multiple Spanning Tree on page 86.
4. Select **private**.
5. Insert the values or select options in the option boxes.

   Note:

   The Secondary VLAN ID must be a different value than the primary VLAN ID.
6. Click **Save**.

After the private VLAN is created successfully, a VLAN tree node displays beneath the respective MSTI/RSTP instance node.



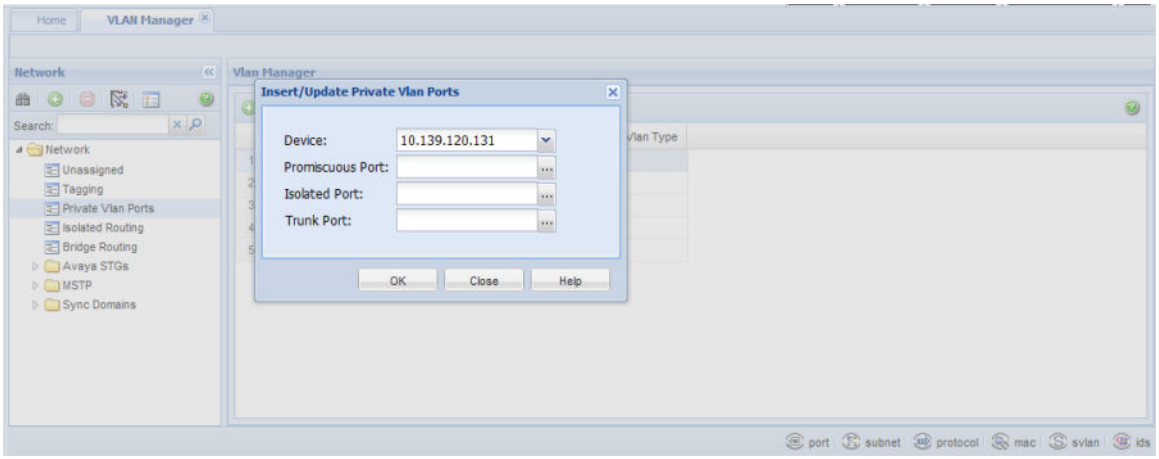
Add Private VLAN Ports

Perform the following procedure to add a Private VLAN port type.

Procedure steps

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

   The **Private VLAN Port** dialog box displays.



3. Insert the values.
4. Click **OK**.

Deleting a Private VLAN in Multiple Spanning Tree

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

Procedure steps

1. In the Navigation pane, under the **CIST** or **MSTI** folder, select the Private 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.

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 101.

Port membership types

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

Table 15: 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 101.
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 101.
Private Vlan ports	A port that can be configured as isolated, promiscuous, or trunk for private VLAN. For more information, see Marking private VLAN ports on page 88.
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 102.
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 104.

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

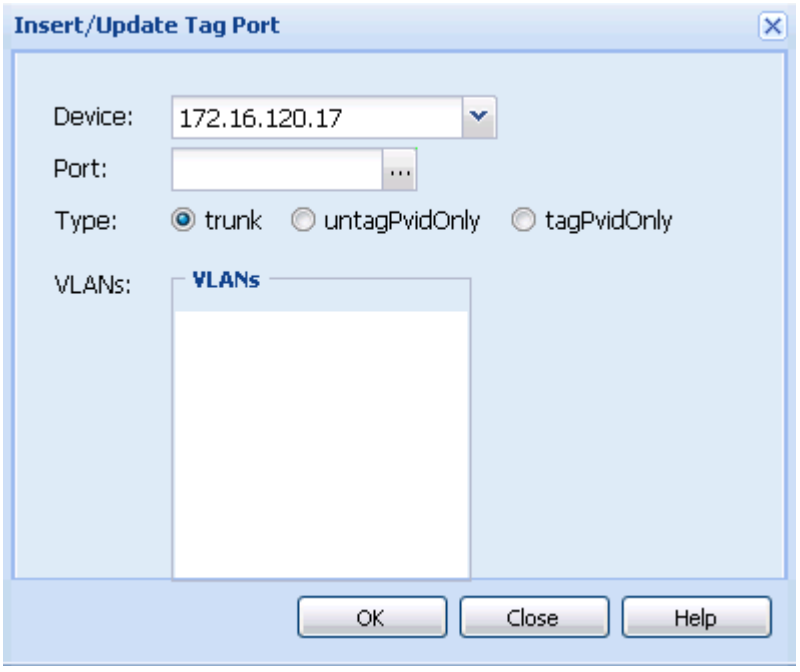
Perform the following procedure to add tagged ports.

Procedure steps

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

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

   The Insert/Update Tag Port dialog box displays.



3. Select the **Device** address you want to add.
4. Click **Port**. The ports for the selected device display.
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 displays when the addition is complete.
9. Click **OK**. The Operation Result dialog box closes and the added port is visible in the contents pane.

Note:

Adding tagged ports is not supported for Switched UNI type VLAN.

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.

Enabling OSPF on a VLAN interface

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

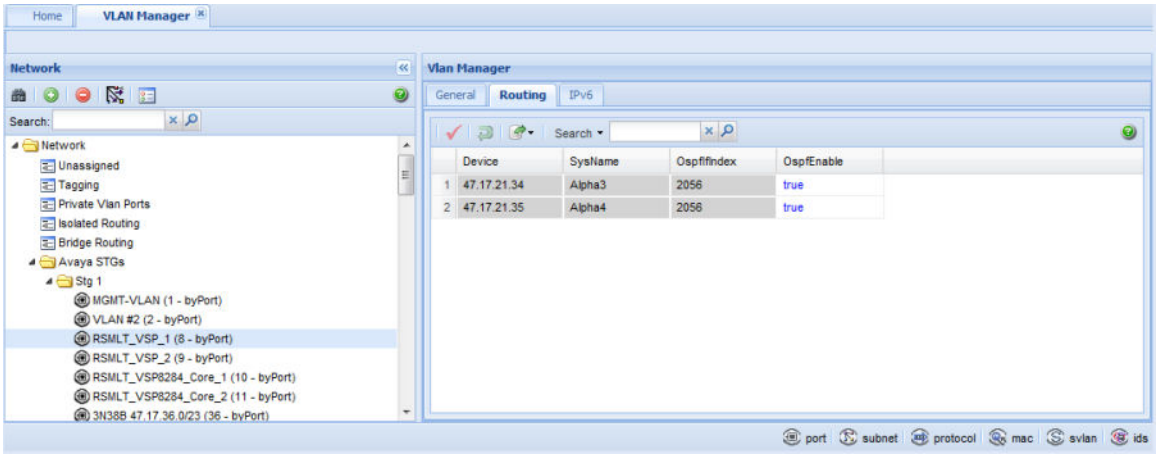
Perform the following procedure to enable OSPF routing on a VLAN interface.

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 displays 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

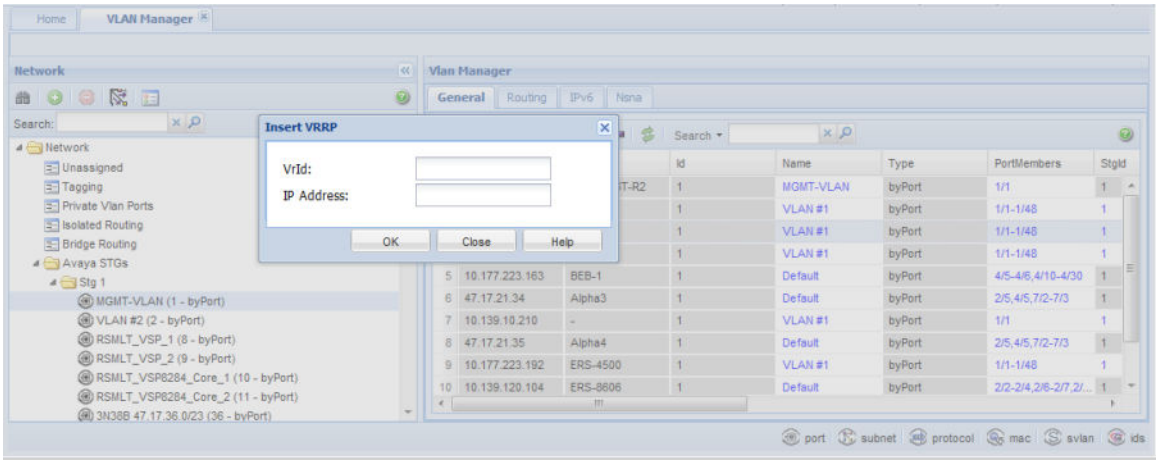
You can use VLAN Manager to insert a VRRP routing interface for a VLAN. Before inserting the VRRP interface, ensure the VLAN has an assigned IP address for routing. Perform the following procedure to insert a VRRP interface on a VLAN.

Procedure steps

1. In the Navigation pane, select a VLAN.

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

   The Insert VRRP dialog box displays.



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 displays in Routing Manager under the VRRP Interfaces folder.

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.

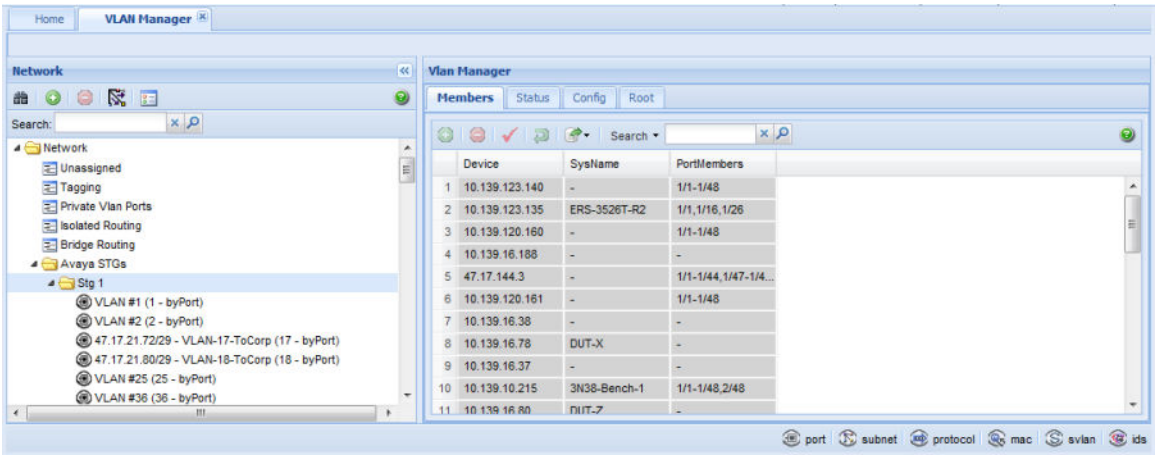
Viewing STG information

This section provided information about viewing STG information.

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.

From the Navigation pane, open the folder for the STG you want to view.



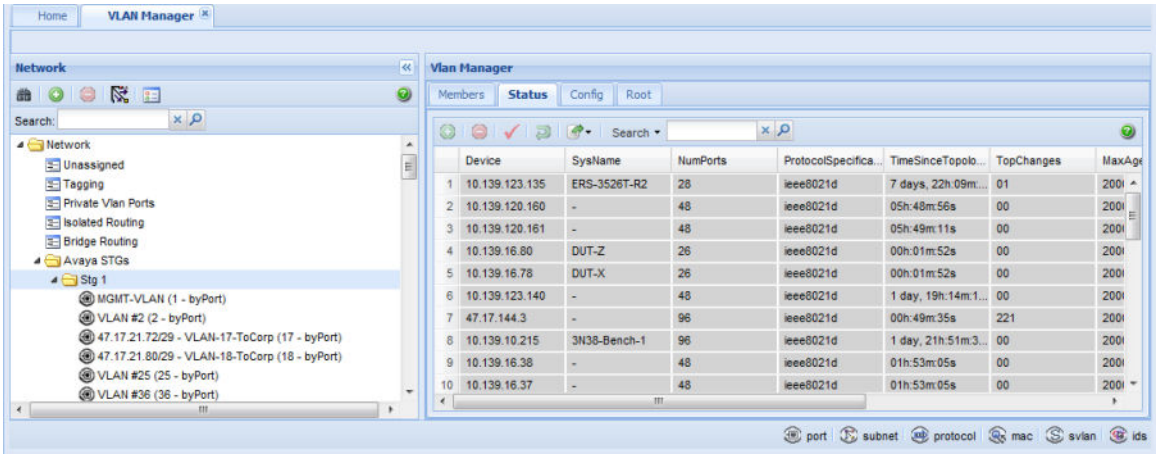
Viewing STG status

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

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

   The Status table displays in contents pane.



Job aid

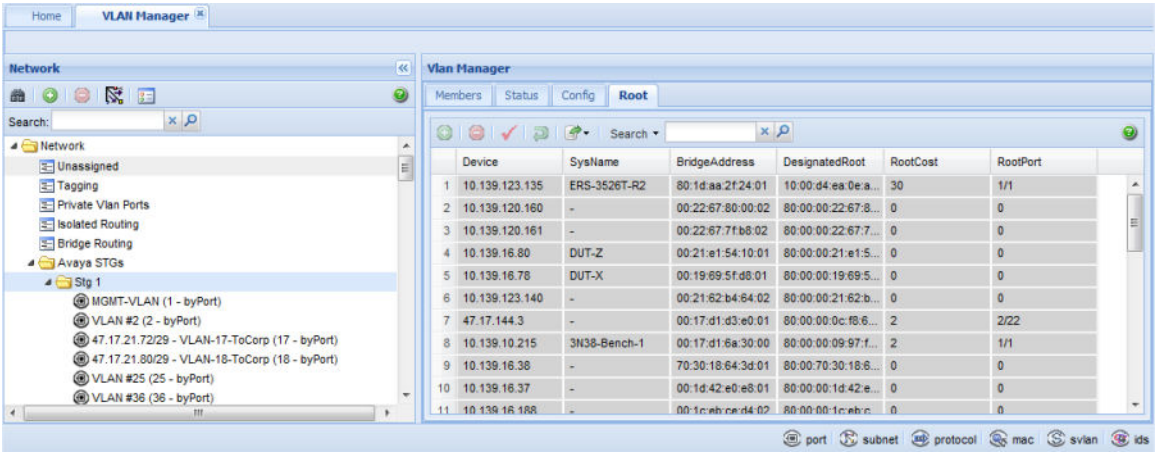
The following table describes the fields in the Status table.

Field	Description
Device	IP address of the bridge.
NumPorts	Number of ports controlled by this bridging entity.
SysName	
Protocol Specification	An indication of which version of the Spanning Tree Protocol (STP) is operating. The IEEE 802.1d implementsations 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).
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.

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.
SysName	System name.
Bridge Address	MAC address used by this bridge when it must be identified in a unique fashion.
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 viewing VLAN information.

VLAN icons

The VLAN icons in the Navigation pane, represent the VLANs that are part of an STG. The following figure Figure 1: VLAN Icon elements on page 98 shows elements of VLAN icons.

Figure 1: VLAN Icon elements

Parts of VLAN icon

The following table Table 16: Parts of a VLAN icon on page 98 describes the elements of a VLAN icon.

Table 16: Parts of a VLAN icon

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

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/8xxx/4xxx
- 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

1. 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 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.

Field	Description
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: • Passport (legacy) 1050/1100/1150/1200/1250 switch: 257 to 512 • Ethernet Routing Switch 8000 Series: 2049 to 4096 • Virtual Services Platform 9xxx: 2049 to 4096 **Important:** 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.

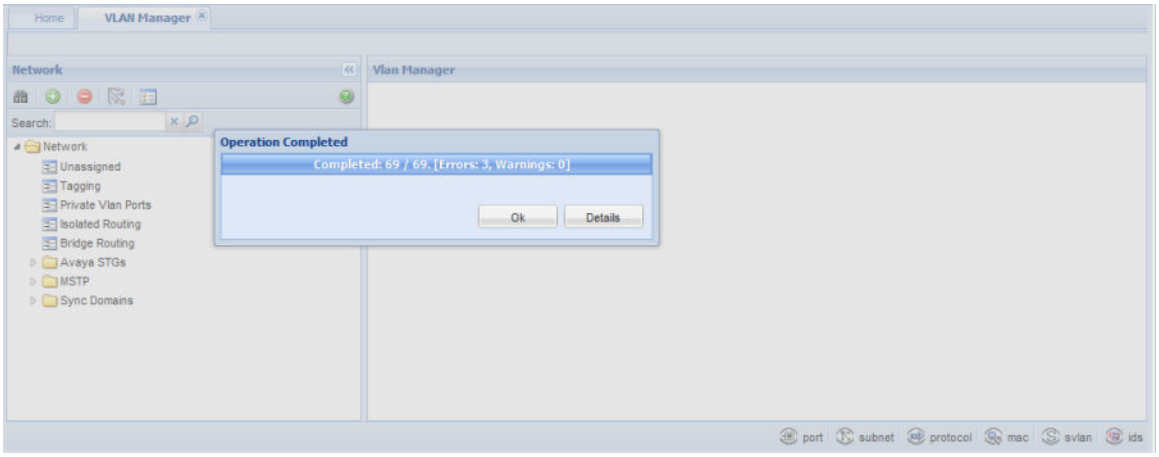
Updating VLAN discovery information

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 displays when the discovery is complete.



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

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.

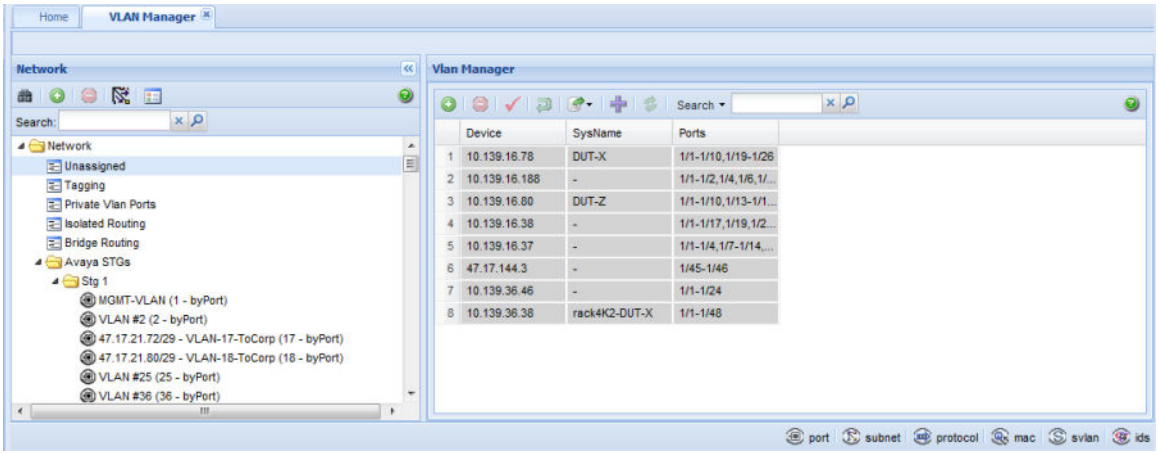
Viewing the unassigned ports

Perform the following procedure to view the unassigned ports.

Procedure steps

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

   The Unassigned Ports table displays 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.

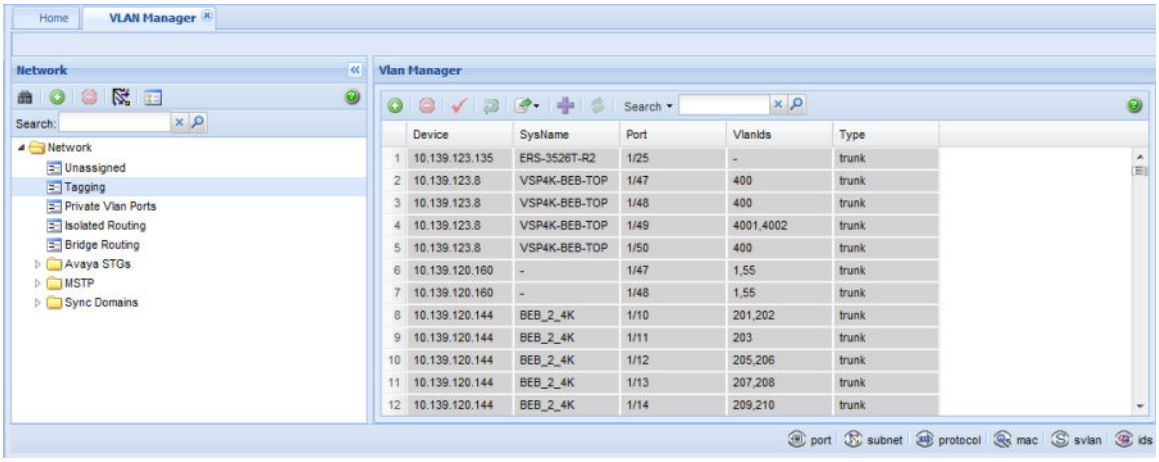
Viewing tagged ports

Perform the following procedure to view tagged ports.

Procedure steps

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

   The Tagging Ports table displays 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.
SysName	System name.
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

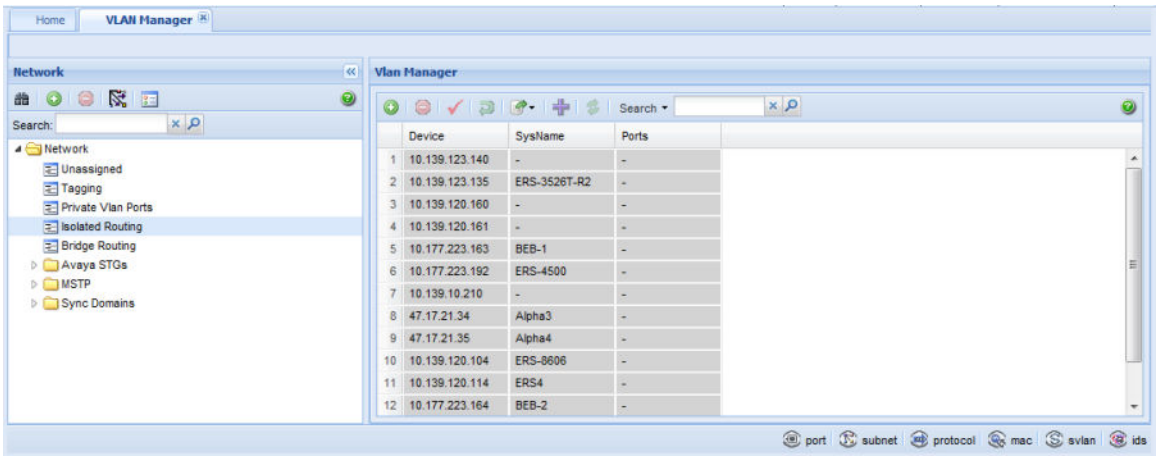
Viewing isolated router ports

Perform the following procedure to view isolated router ports.

Procedure steps

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

   The Isolated Routing Ports table displays 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.
SysName	System name.
Ports	Ports that route only IP packets.

Viewing Private VLAN ports

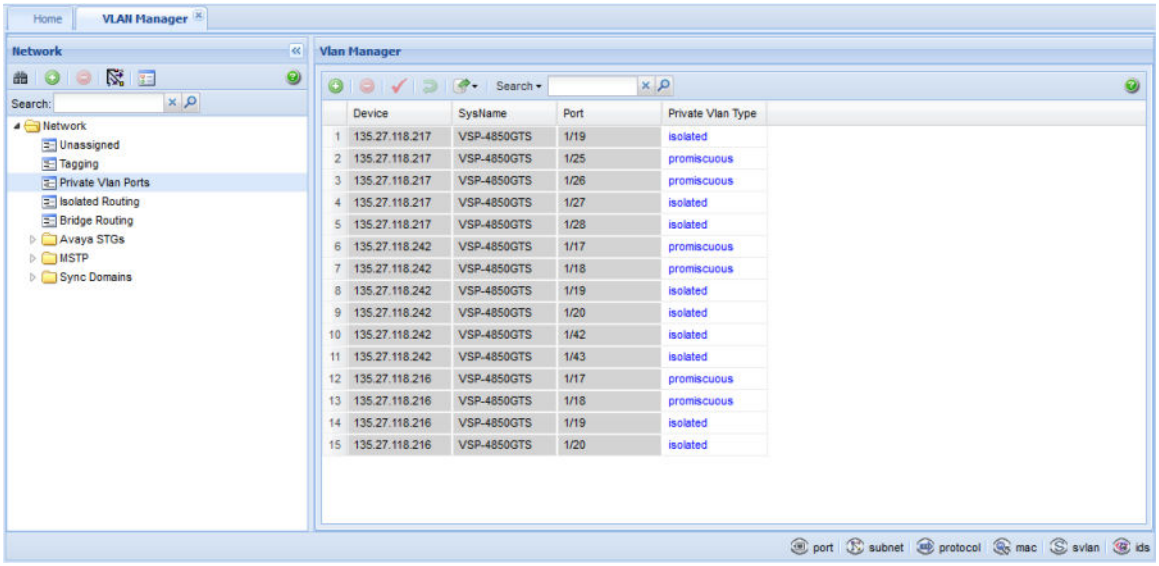
About this task

Perform the following procedure to view Private VLAN ports

Procedure

In the Navigation pane, select **Private VLAN ports**.

The Private VLAN ports table displays in the contents pane.



Job aid

The following table describes the fields in the Private VLAN ports table.

Field	Descriptions
Device	IP address, system name, or host name of the device.
SysName	System name.
Port	Ports that route only IP packets.
Private VLAN Type	Private VLAN capable devices configured as Promiscuous, Isolated, and Trunk ports.

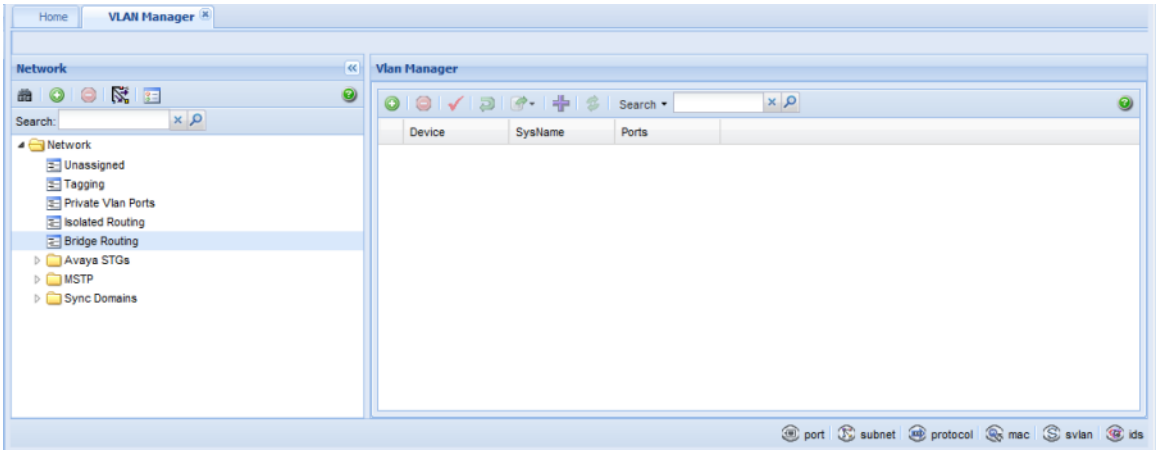
Viewing bridge routing ports

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

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

   The Bridge Routing Ports table displays in the contents pane.



Job aid

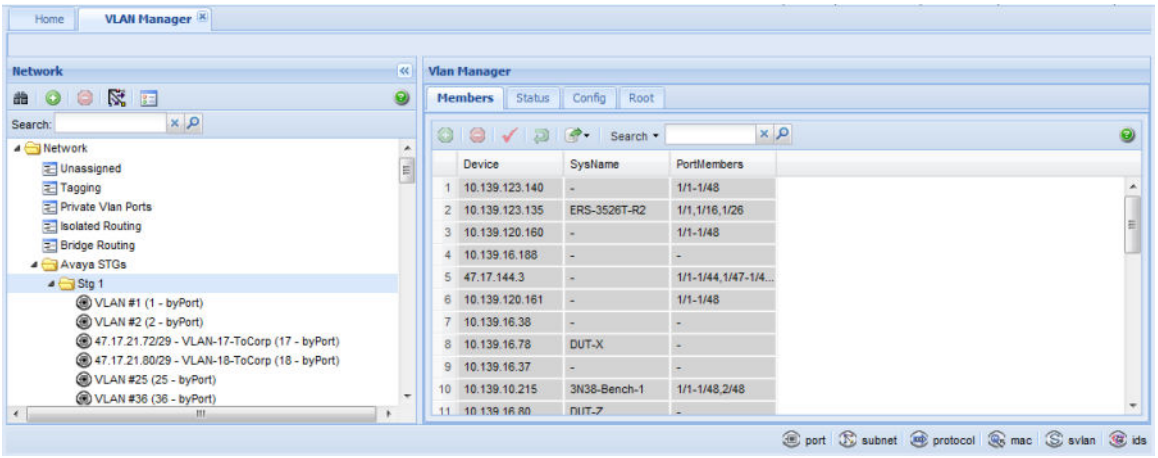
The following table describes the fields in the Bridge Routing Ports table.

Field	Descriptions
Device	IP address, system name, or host name of the device.
SysName	System name.
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.

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.
SysName	System name.
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 pane, select the **MSTP** folder.
2. Select the **CIST** folder or an **MSTI** folder.
3. Select a VLAN.

   The Members table displays 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.

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 displays in the VLAN Manager contents pane.

2. On the VLAN Manager menu bar, click **Highlight on topology**.

   The highlighted topology view displays 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 displays in the VLAN Manager contents pane.

2. On the VLAN Manager menu bar, click **Highlight 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 displays in the contents pane.

2. On the VLAN Manager menu bar, click **Highlight on topology**.

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

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 on page 107
  - Sync Domain interface on page 107
  - Server node VLAN interface on page 109
  - IP Address and Net Mask interfaces on page 111
- Domain synchronization procedures on page 112
  - Creating a sync domain on page 112
  - Adding a VLAN to a sync domain server node on page 113
  - Modifying a sync domain on page 114
  - Modifying a sync domain server node VLAN on page 114
  - Deleting a sync domain on page 115
  - Deleting a server node VLAN on page 115

Domain synchronization interfaces

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

- Sync Domain interface on page 107

  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 109

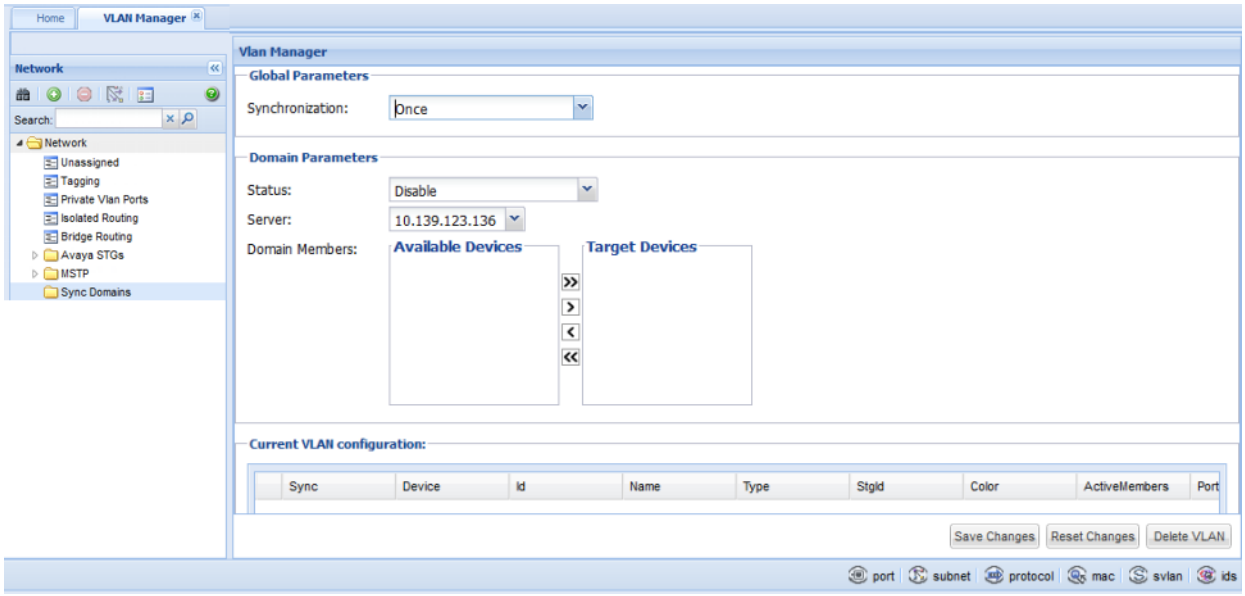
  Use the VLAN interface to add a new VLAN or private VLAN to the server node.

- IP Address and Net Mask interfaces on page 111

  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 following figure shows the Sync Domain interface which you use to define a new sync domain or modify an existing sync domain.



The following table describes the elements of the interface.

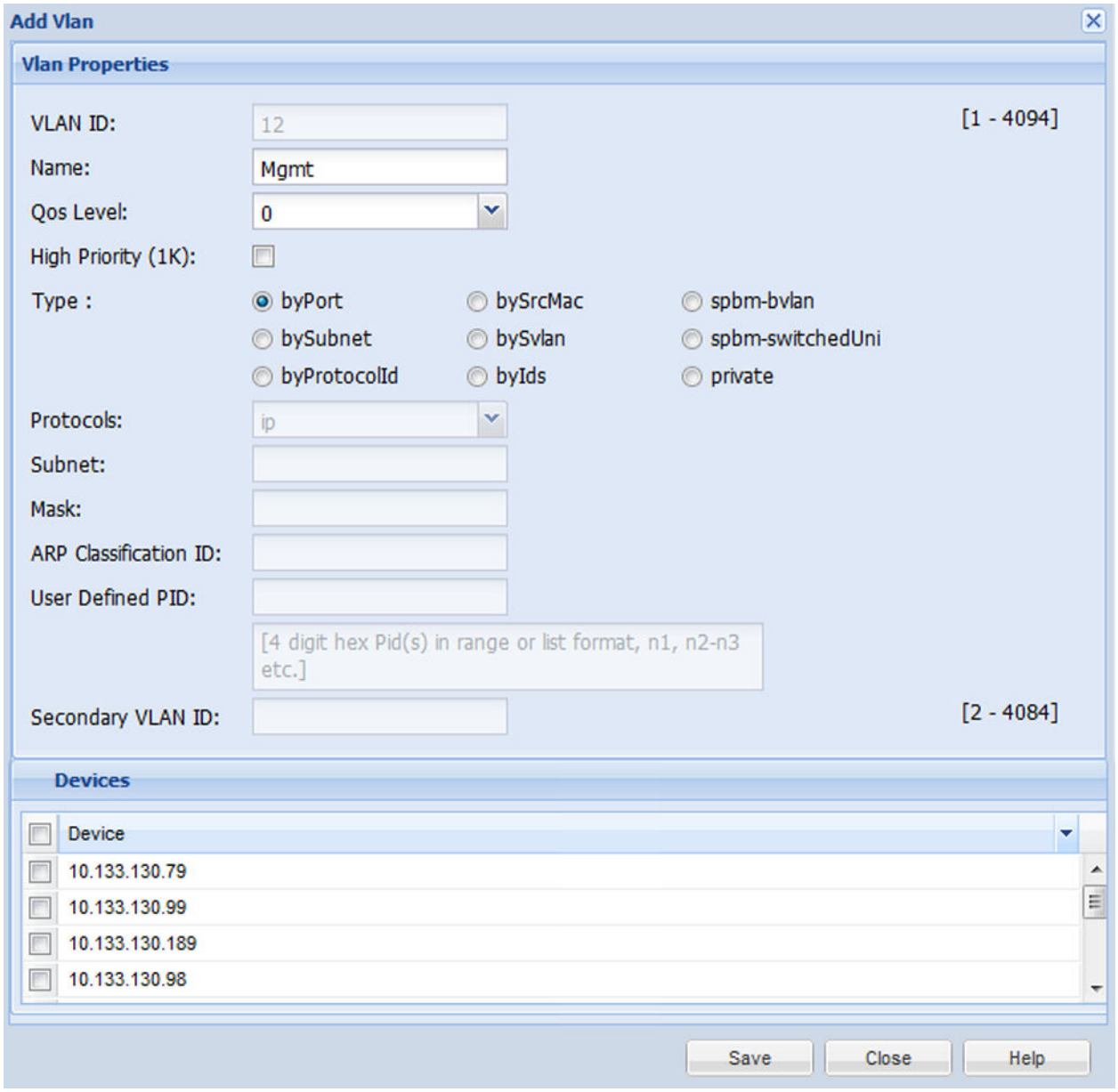
Table 17: Sync Domain interface elements

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: • Once Synchronization occurs when you save the domain by clicking **Save Changes**. • Configuration change in VM 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 devices from a list of available devices. The list is generated by filtering the devices

Field	Description
	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. 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 111.
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 111.
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.

Server node VLAN interface

The following figure shows the VLAN interface which you use to add a new VLAN to the server node.



The following table describes the elements of the interface.

Table 18: VLAN interface elements

Element	Description
VLAN ID	This is the primary identity of the VLAN. VLAN Manager fills this with the next available number but you can change it. The primary VLAN Id ranges from 1 to 4084.
Name	Enter a name for the VLAN.
QOS Level	Select from levels 0 through 7.
High Priority (1K)	Choose to activate this or leave unselected.

Element	Description
Type	Choose private to configure a private VLAN.
Subnet, Mask, ARP-Classi-fication-Id, UsrDefined PId	One or more of these fields may be enabled, depending on the ProtocolId.
IP Address	Enter the IP address of the VLAN.
Net Mask	Enter the network mask of the VLAN.
Secondary VLAN	Enter the Secondary VLAN ID. This value should be different than the primary VLAN ID.
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	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 17: Sync Domain interface elements on page 108 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.PAdress 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.

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 113.

Prerequisites

- Familiarity with the Sync Domain interface is required for this procedure. See Sync Domain interface on page 107 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 109 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 114.

Prerequisites

- Familiarity with Creating a sync domain on page 112 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 111 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.

Chapter 7: Create and manage MultiLink Trunks

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.

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 19: 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
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.

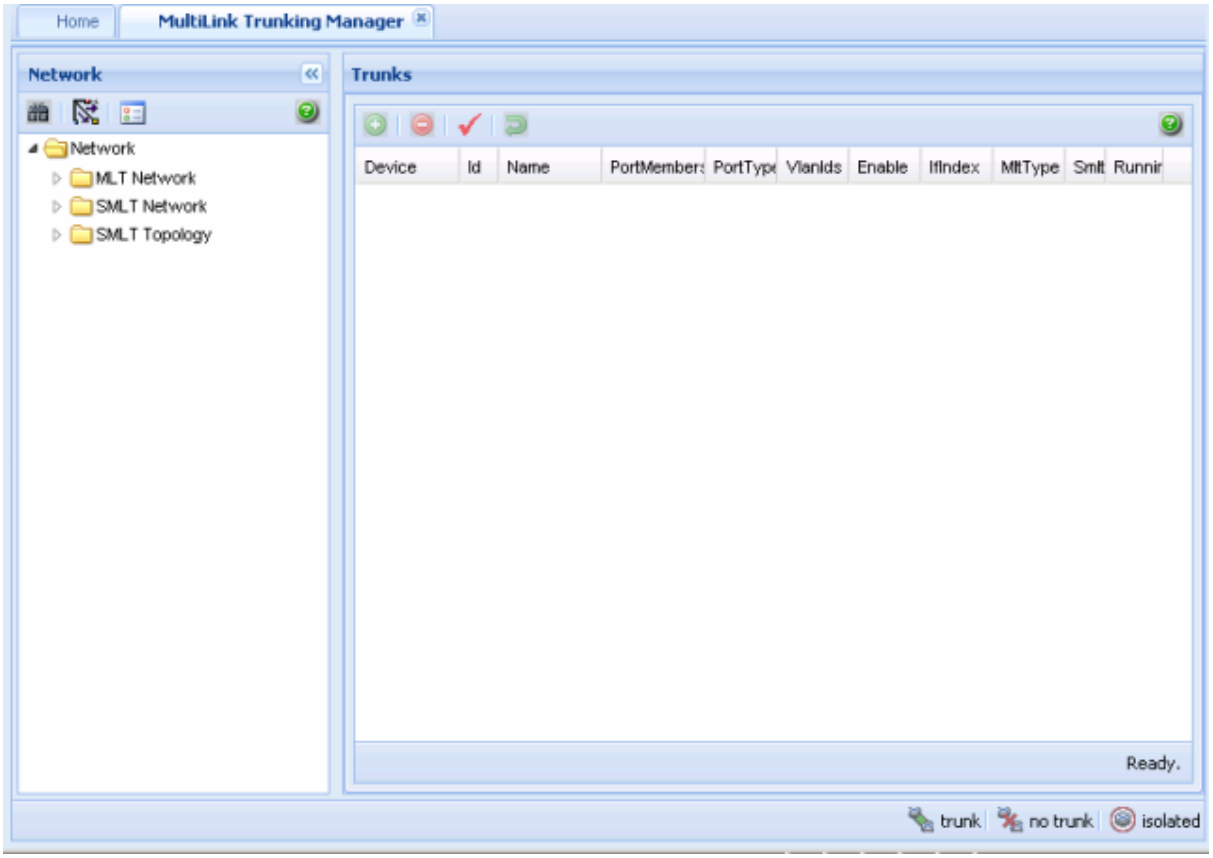
Procedure steps

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.

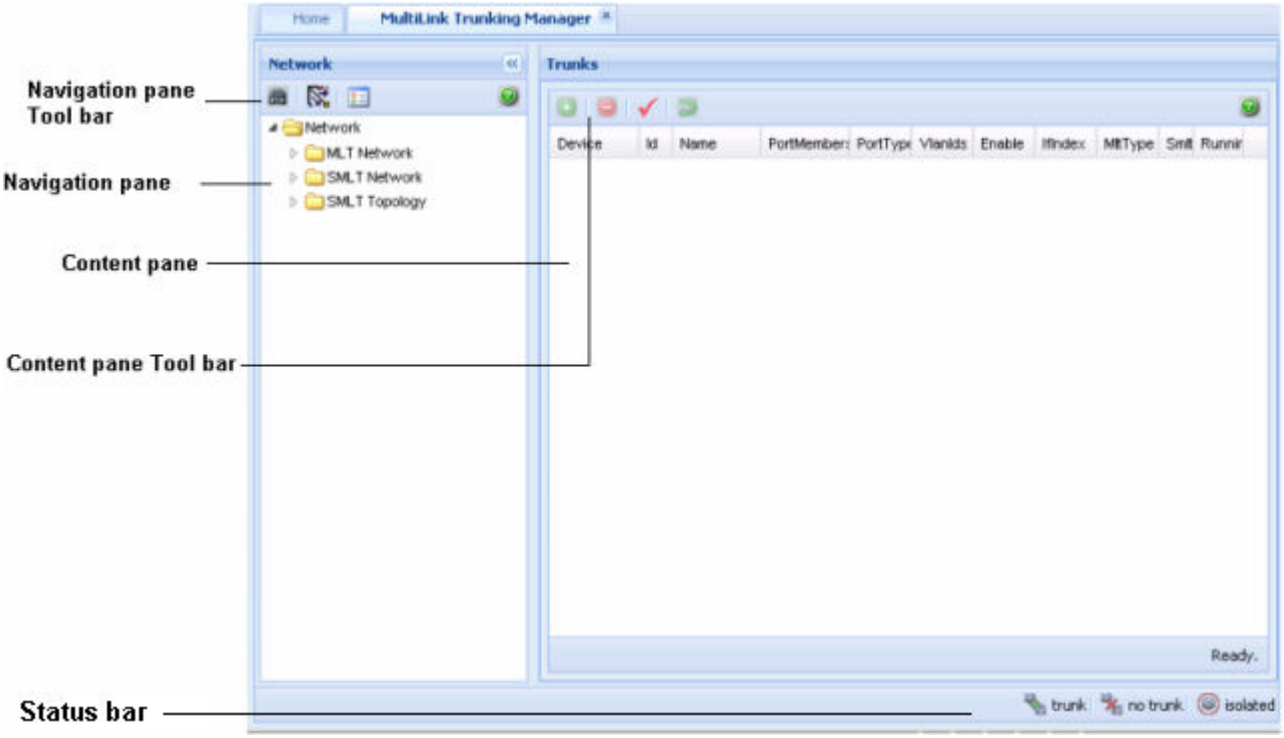


Figure 2: MultiLink Trunking Manager window

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

Table 20: 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.

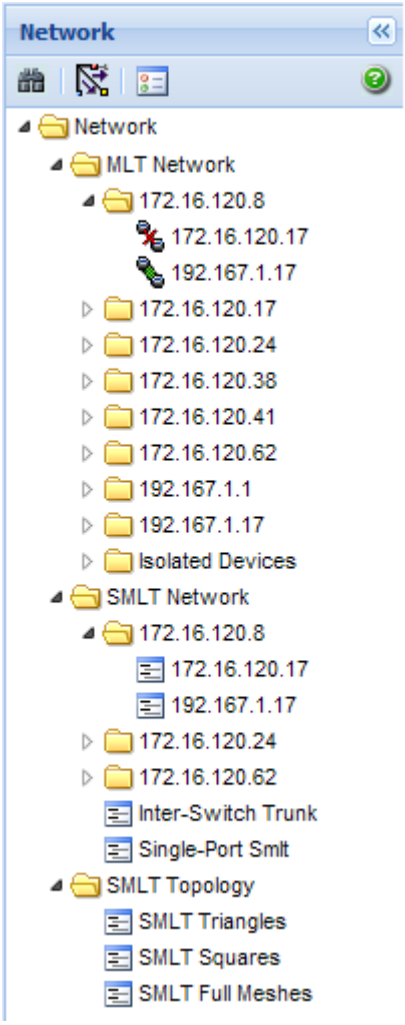


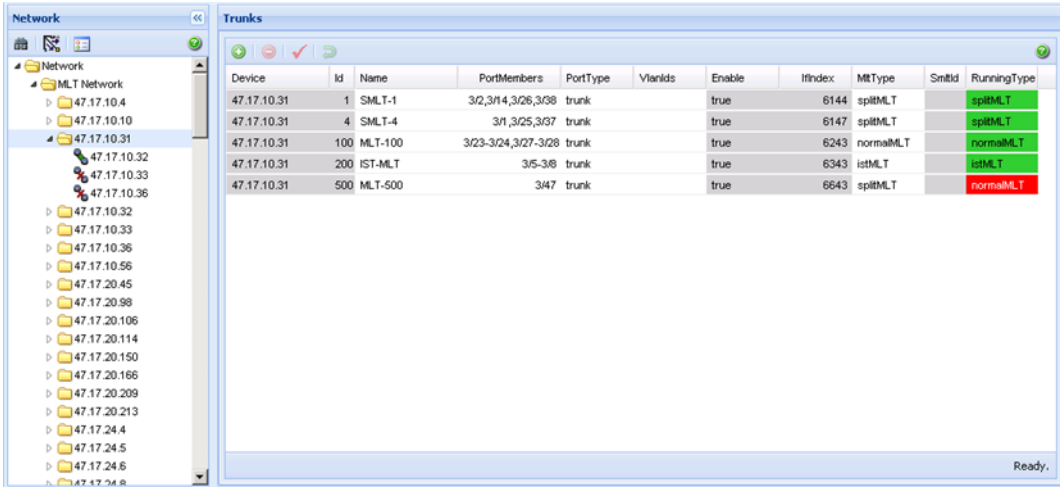
Figure 3: MultiLink Trunking Manager navigation pane

The Network folder has the following resources available in it.

- MLT Network folder on page 121
- SMLT Network folder on page 122
- SMLT Topology folder on page 124

MLT Network folder

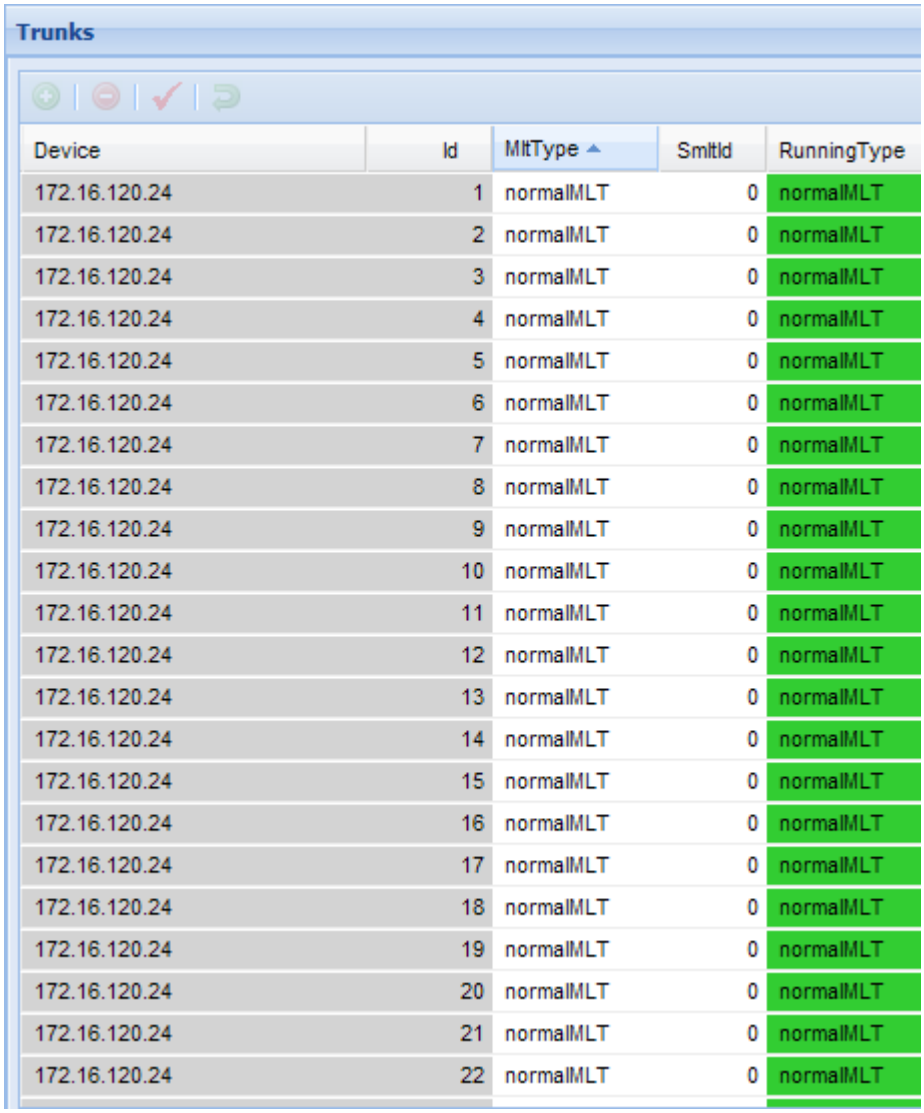
The MLT Network folder displays all the configured trunks of the devices. When you click on the nodes on the navigation pane inside the MLT Network folder, the contents pane displays all the configured tasks of the device. When you click on the child nodes which is connected to the parent devices, only 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.



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 4: SMLT Network

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

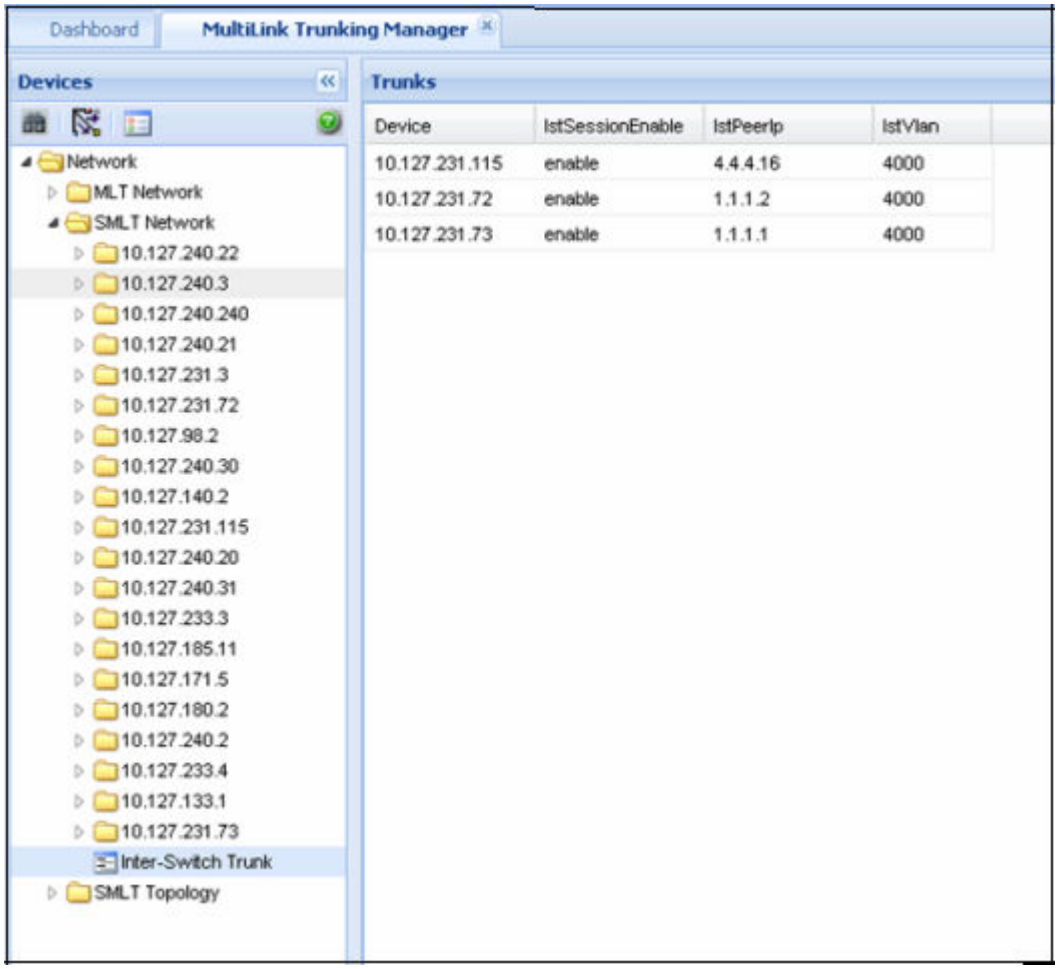


Figure 5: SMLT Network IST

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.

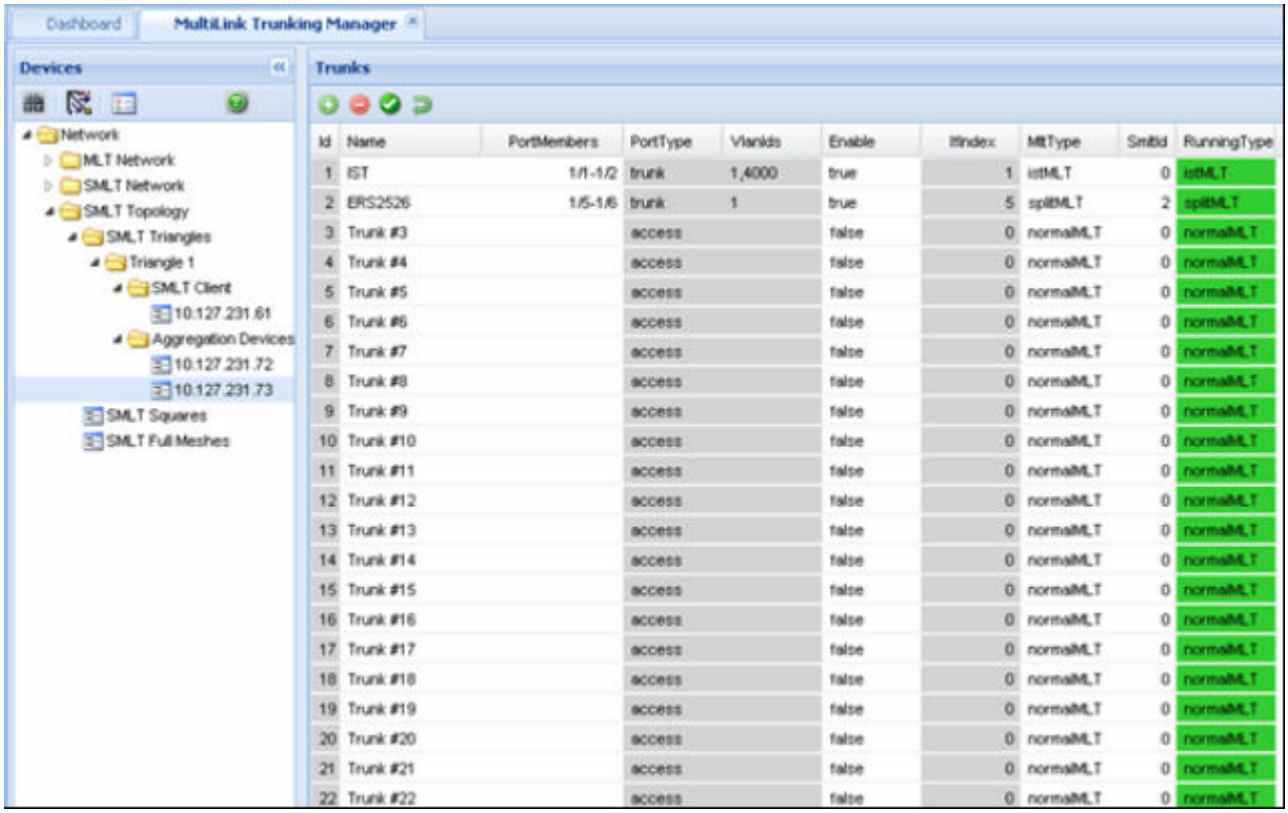


Figure 6: SMLT Triangle

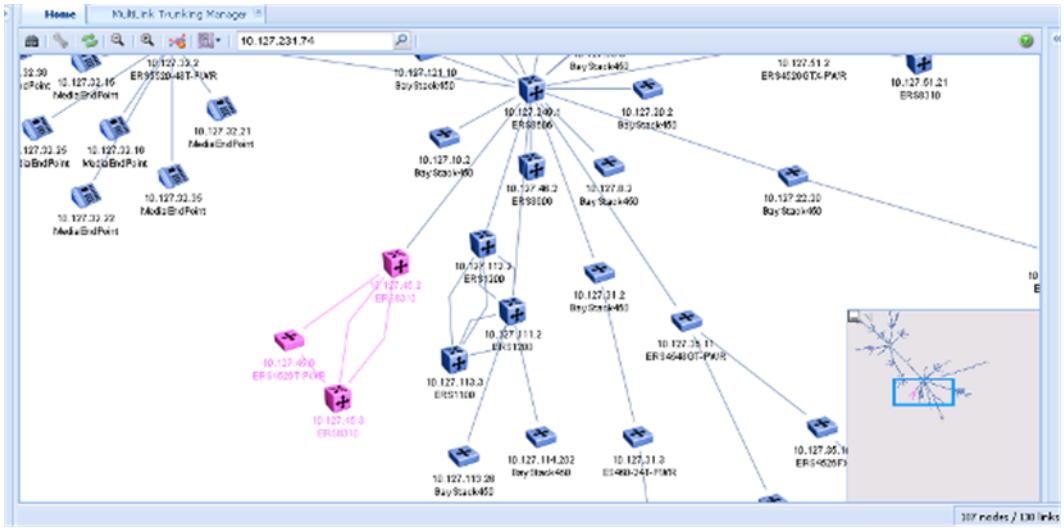


Figure 7: SMLT Triangle Topology

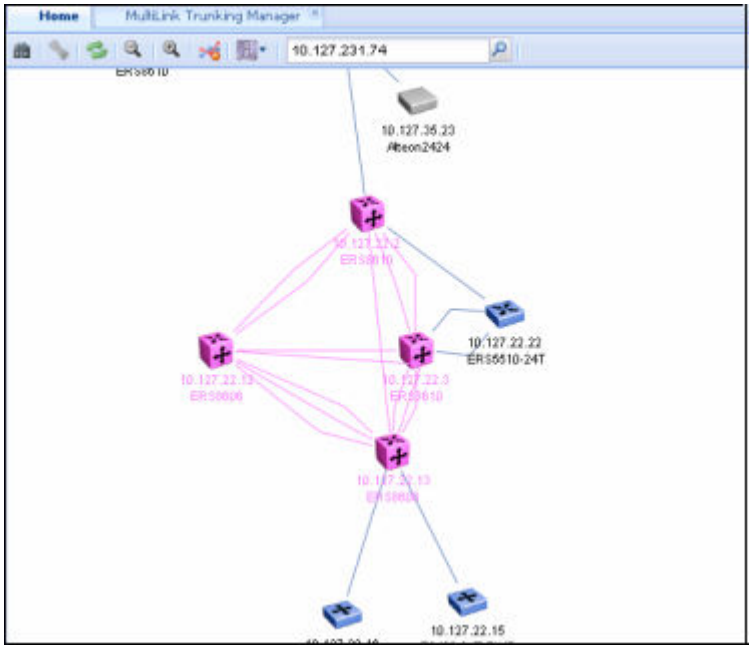


Figure 8: SMLT Full mesh Topology

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 21: 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.

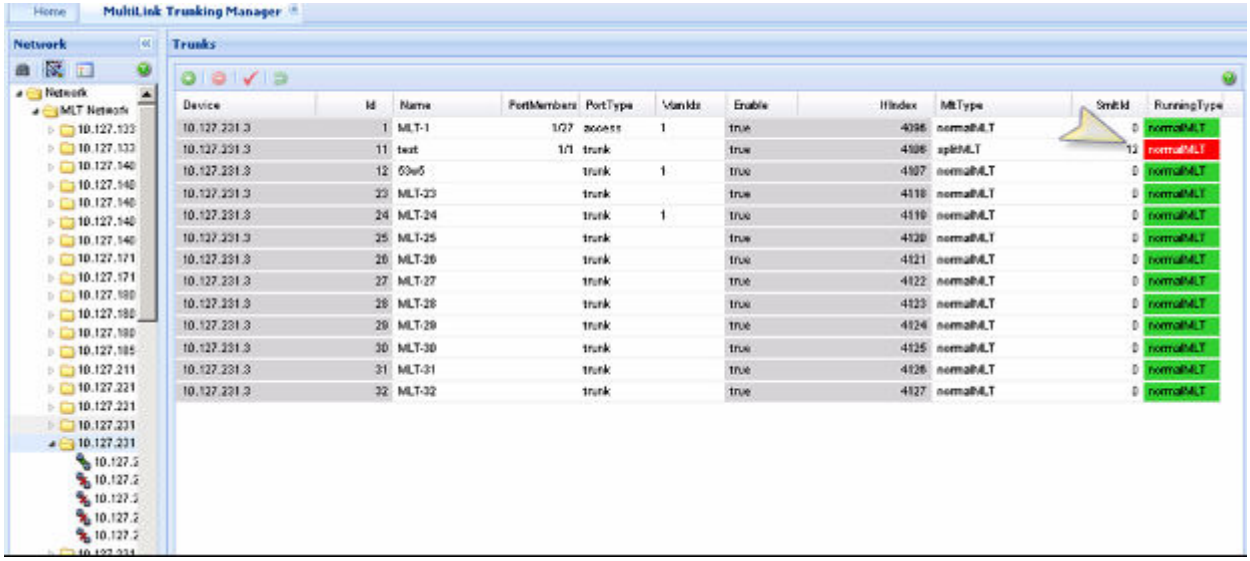


Figure 9: MultiLink Trunking Manager contents pane

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 22: 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 on ERS 1424/16xx, ERS 8000, VSP 9xxx, and VSP 4000 3.1 devices on page 128.

Tools	Toolbar button	Description
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, VSP 9xxx, or VSP 4000 on page 135.
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 sections describe common operations you can perform using MultiLink Trunking Manager.

Creating MLTs on ERS 1424/16xx, ERS 8000, VSP 9xxx, and VSP 4000 3.1 devices

To create an MLT on Ethernet Routing Switch 1424/16xx, Ethernet Routing Switch 8000, VSP 9xxx and VSP 4000 3.1 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 129.

  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 129

- Creating an MLT with one device for ERS 1424/16xx on page 130
- Creating an MLT with one device for VSP 4000 v 3.0.x on page 132

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:

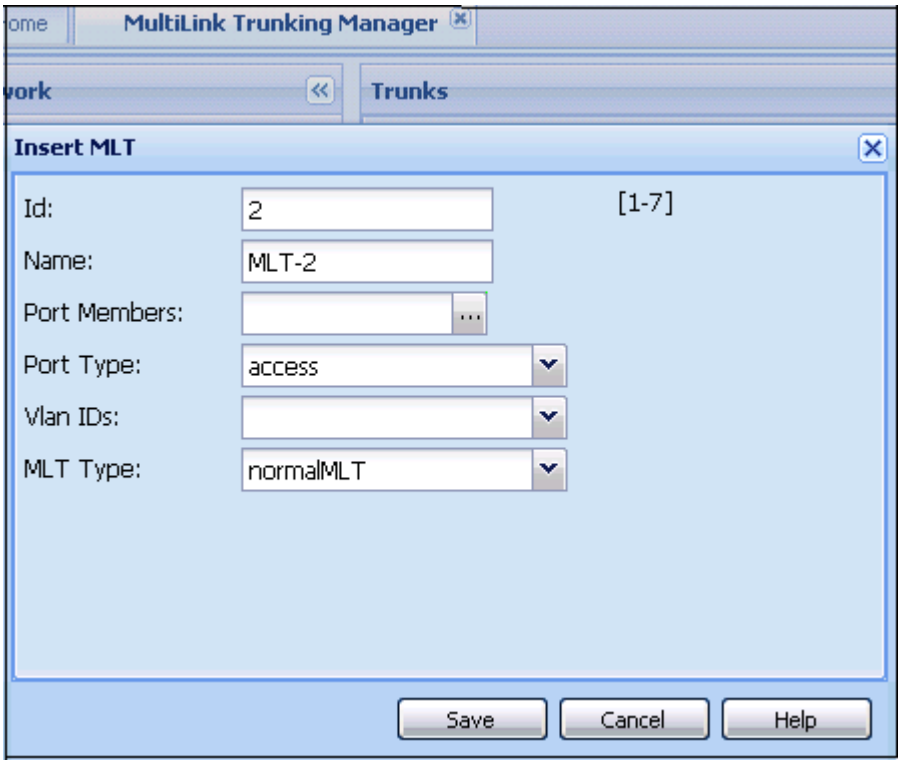
Procedure steps

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 142.
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 23: Insert MLT dialog box items for ERS 8000 or VSP 9xxx

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: • Access • Trunk The default is Access.
Vlan IDs	VLAN IDs found on the device.
MLT type	One of the following types of MLT links: • normalMLT- Use for normal MLT that do not use SMLT features. • istMLT- Use for IST (inter-switch trunk) links between peer devices in SMLT configurations. • 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 142.

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 24: 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: • Access • Trunk The default is Access.
Vlan IDs	VLAN IDs found on the device.
MLT type	One of the following types of MLT links: • normalMLT- Use for normal MLT that do not use SMLT features. • istMLT- Use for IST (inter-switch trunk) links between peer devices in SMLT configurations. • splitMLT- Use for SMLT links between peer devices and non-peer devices in SMLT configurations.

Item	Description
Ports	Ports in the MLT. The maximum number of ports for one trunk is four.

Creating an MLT with one device for VSP 4000 v 3.0.x

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 VSP 4000 3.0.x device selected.

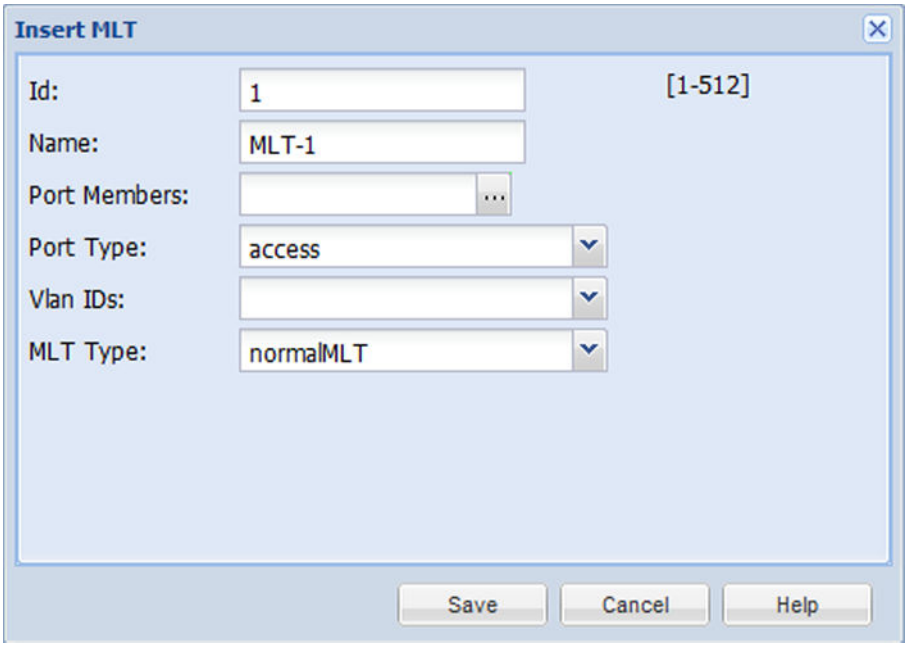
Procedure steps

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

   The Device table displays in the contents pane.

2. On the Content Pane Toolbar, click **Add**.

   The Insert MLT dialog box displays.



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 **Vlan IDs** field, select the VLAN IDs that belong to the MLT port.
8. Select the **PVLAN port type**.

9. 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 142.

10. Click **Save**.

Validations

- When Trunk is selected as the private VLAN port type the MLT is tagged automatically.
- When Isolated is selected as the private VLAN port type and there are other non-private VLANs using that MLT the following message displays: All non-private VLANs using this interface will be removed once this mlt becomes isolated. Do you wish to continue? Y/N .

Insert MLT dialog box for VPS 4000 3.0.x

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

Table 25: Insert MLT dialog box for VPS 4000 3.0.x

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.
Vlan IDs	VLAN IDs found on the device.
PVLAN Port type	Selection is available for a Private VLAN-capable device only. • Trunk • Isolated • Promiscuous • None
Port Type	One of the following types of MLT: • Access • Trunk The default is Access.
MLT type	One of the following types of MLT links: • normalMLT- Use for normal MLT that do not use SMLT features. • istMLT- Use for IST (inter-switch trunk) links between peer devices in SMLT configurations. • splitMLT- Use for SMLT links between peer devices and non-peer devices in SMLT configurations.

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 displays in the contents pane.

2. In the table, double-click the **PortMembers** field.

   The PortMembers dialog box displays.

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 129.

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 displays in the contents pane.

2. In the table, double-click the **PortMembers** field.

   The PortMembers dialog box displays.

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, VSP 9xxx, or VSP 4000

Perform the following procedure to delete an MLT from an Ethernet Routing Switch 1424/16xx or 8000, VSP 9xxx, or VSP 4000.

Procedure steps

1. In the navigation pane, select a device.

   The MLT table displays 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 displays 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**.

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

1. 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.
MltType	One of the following types of MLT links: • normalMLT—used for normal MLT that do not use SMLT features. • istMLT—used for IST (Inter-Switch Trunk) links between peer devices in SMLT configurations. • 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: • normalMLT • istMLT • 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

1. 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).
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: • 512–519 for Passport (legacy) 1050, 1150, 1200, and 1250 devices • 4096–4127 for Ethernet Routing Switch 8000 family devices
MltType	For SMLT configurations, shows one of the following types of MLT links: • normalMLT—used for normal MLT that do not use SMLT features. • istMLT—used for IST (inter-switch trunk) links between peer devices in SMLT configurations. • 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: • normalMLT • istMLT • 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

1. 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: • 512–519 for Passport (legacy) 1050, 1150, 1200, and 1250 devices • 4096–4127 for Ethernet Routing Switch 8000 family devices
MltType	For SMLT configurations, shows one of the following types of MLT links: • normalMLT—used for normal MLT that do not use SMLT features. • istMLT—used for IST (inter-switch trunk) links between peer devices in SMLT configurations. • 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: • normalMLT • istMLT • 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

1. 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 140.

Perform the following procedure to view SMLT.

Procedure steps

1. 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: • normalMLT–Use for normal MLT that do not use SMLT features. • istMLT– Use for IST (inter-switch trunk) links between peer devices in SMLT configurations.

Field	Description
	• 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: • normalMLT • istMLT • splitMLT

Viewing single port SMLTs

Perform the following to view single-port SMLT.

Procedure steps

1. 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. • A read-only field with a value of 1 to 512 indicates the port's single port SMLT ID assignment. • 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: • normalMLT • istMLT • splitMLT
VlanIDs	VLAN IDs for the single-port SMLT.

Updating information in the MultiLink Trunking Manager

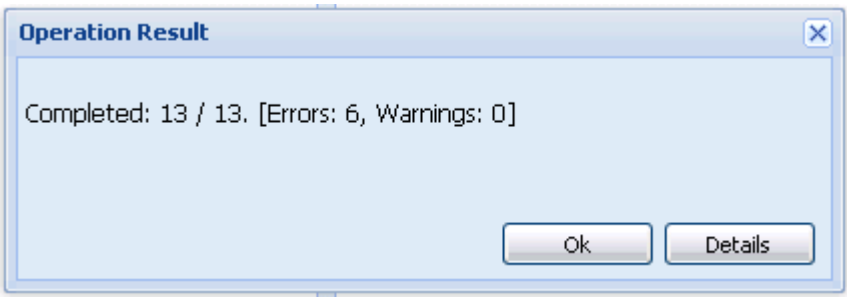
You can discover the devices in the MultiLink Trunking Manager window with MultiLink trunk information polled from the network devices. You can use this feature to load any updated information that took effect since you opened MultiLink Trunking Manager.

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.

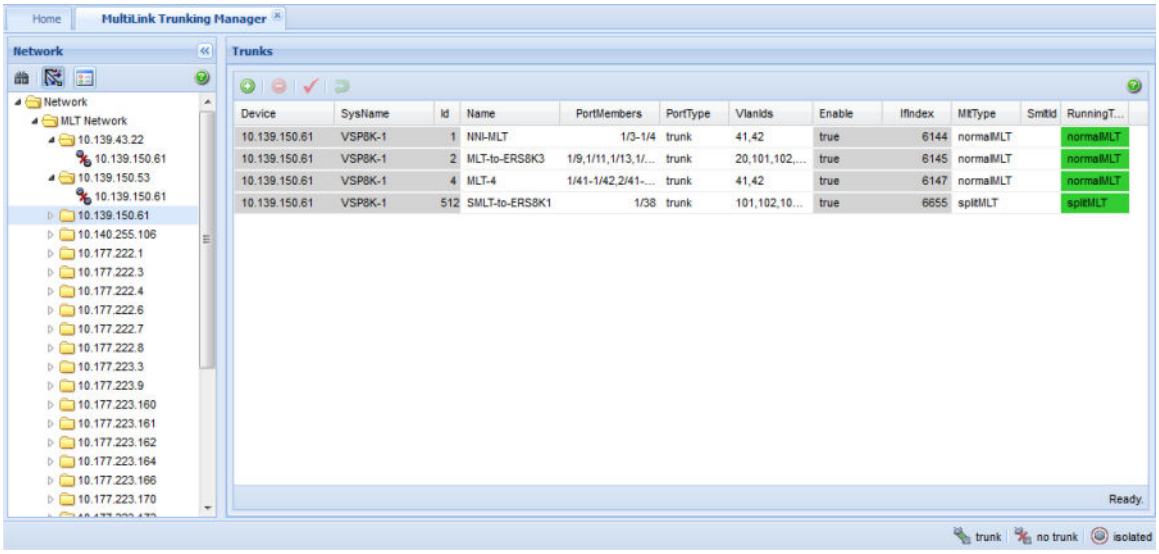
Procedure steps

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

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

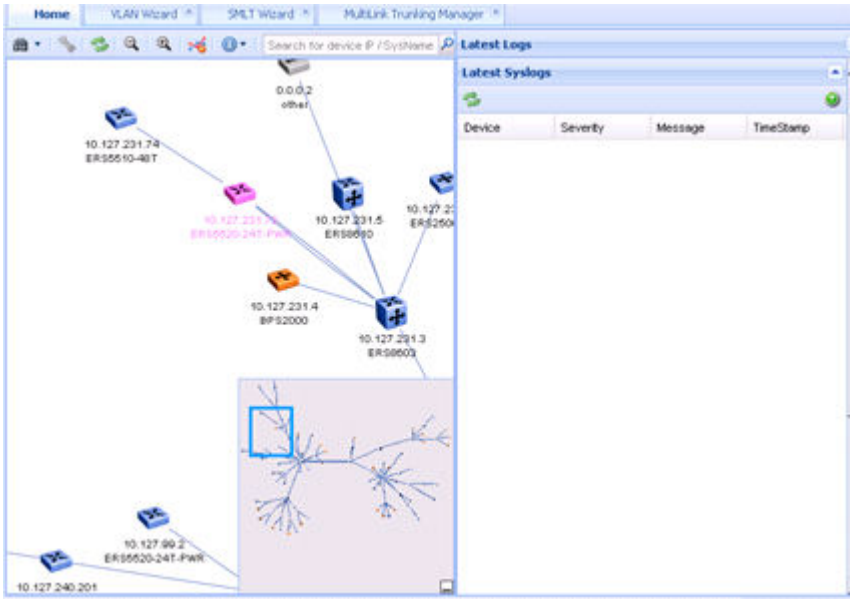
2. From the MultiLink Trunking Manager menu bar, choose **Highlight On topology**.

   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.



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 143.
- 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 144.
- 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 145.
- On the two peer devices, you configure the IST peers. For more information, see Configuring IST peers on page 145.

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 144.
- You configure a normalMLT link on the non-peer device. For more information, see Configuring SMLT links on non peer devices on page 145.

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 130
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 143, 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. • A read-only field with a value of 1 to 512 indicates the port single port SMLT ID assignment. • 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**.

Chapter 8: Configure security on your network devices

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

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

Note:

VSP 8000 does not support Password SNMP.

Important:

This functionality is not to be confused with the Device and Server Credentials offered through SMGR-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 26: 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 5xxx/4xxx/35xx
	Ethernet Routing Switch 16xx 2.0 or later (WEB only)
	Virtual Services Platform 9xxx/8xxx/4xxx
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/8xxx/4xxx
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 48xx
	Ethernet Routing Switch 45xx
	Ethernet Routing Switch 25xx/35xx
	Ethernet Routing Switch 8xxx 3.3 and up (8300 all)
	Ethernet Routing Switch 16xx 2.0 or later
	Virtual Services Platform 7024
	Virtual Services Platform 9xxx/8xxx/4xxx
	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
	Ethernet Routing Switch 55xx, 56xx 4.0.0 and up
	Ethernet Switch 425/420/325 3.0 and up
	Ethernet Routing Switch 48xx

Type of access	Device type
	Ethernet Routing Switch 45xx/35xx/25xx
	Virtual Services Platform 9xxx/8xxx/7xxx/4xxx
TACACS	Wireless Controller 8xxx
	Ethernet Routing Switch 8600 5.1 and up
	Ethernet Routing Switch 45xx/5xxx
	Ethernet Routing Switch 8300 2.2 and up
	Virtual Services Platform 9xxx/8xxx/7xxx/4xxx

Starting Security Manager

Perform the following procedure to start Security Manager.

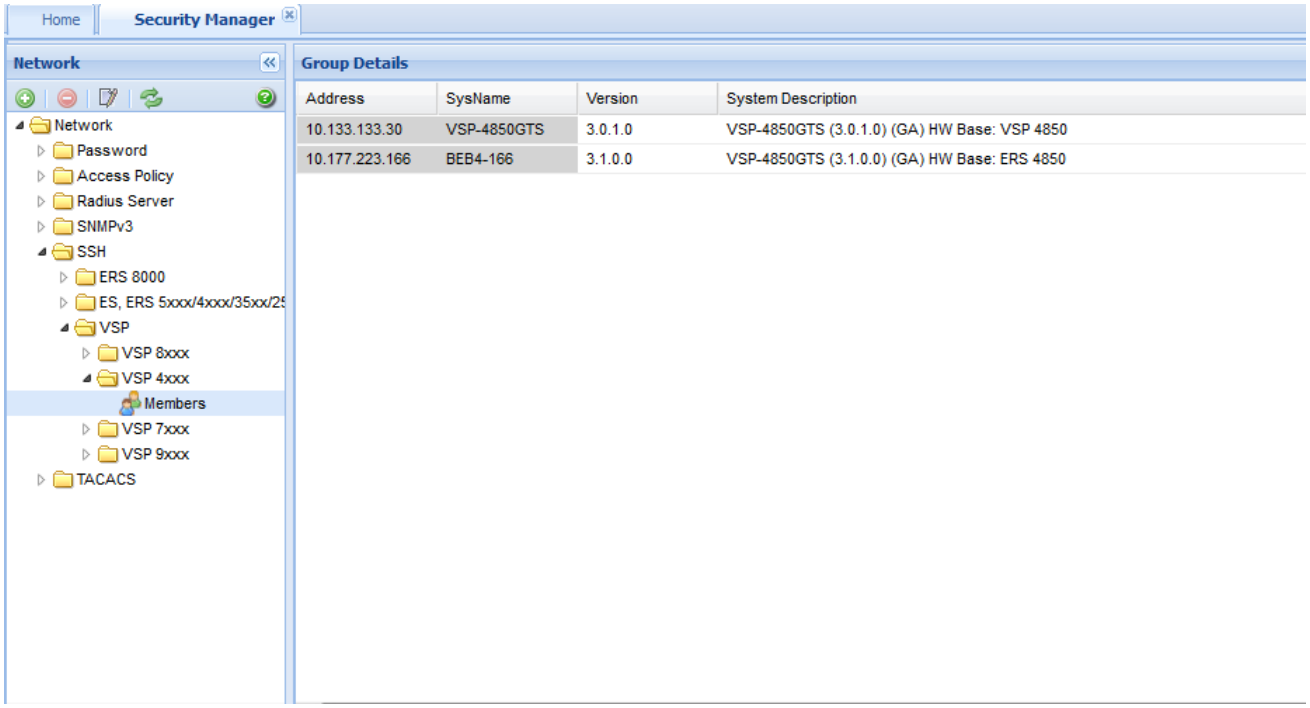
Procedure steps

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.



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

Table 27: 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 150.
Navigation pane	Allows you to navigate security settings for the current network devices. For more information, see Navigation pane on page 151.
Contents pane	Displays elements of the folder or element selected on the navigation pane. For more information, see Contents pane on page 152.

Toolbar and Contents pane buttons

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

Table 28: Security Manager Menu bar commands and toolbar buttons

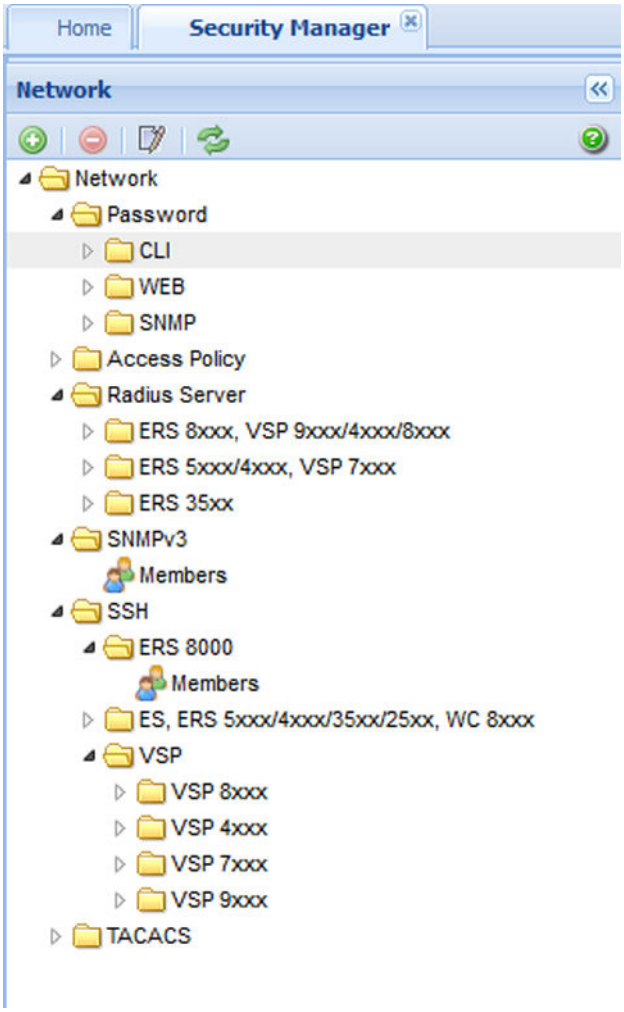
Command	Tool bar button	Description
Add		Creates a new security group that contains devices of the current domain type (CLI, WEB, SNMP, Access Policy, Radius Server, SSH, TACACS).
Delete		Removes the selected security group from Security manager.

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 155.
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.



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

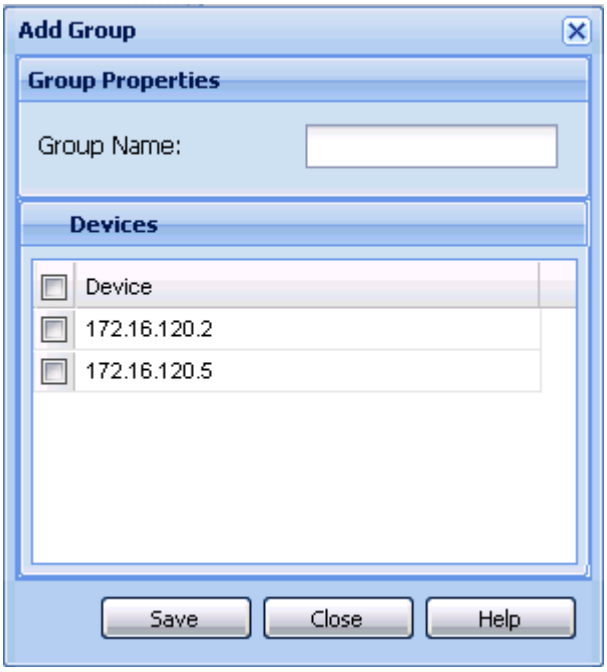
Perform the following procedure to create a security group.

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.

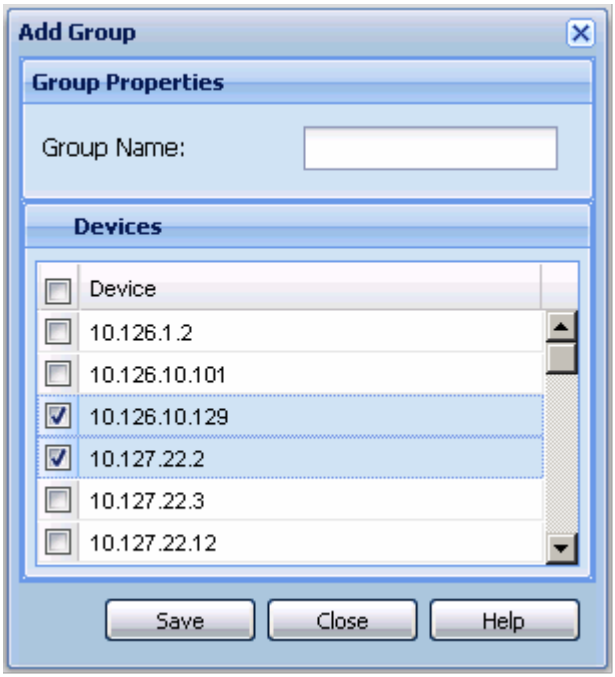
Adding new devices to a security group

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 displays.



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 the device 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 displays 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

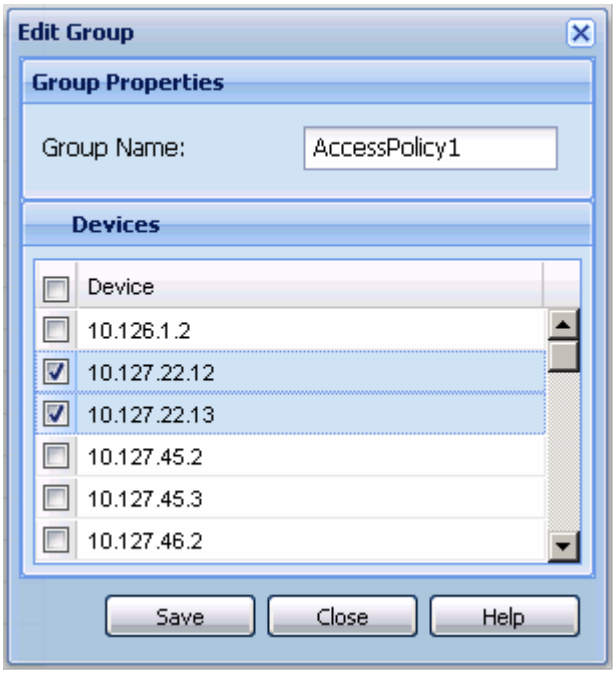
1. In the Navigation pane, browse and select one of the following application folders:
   - Access Policy
   - Radius Server
   - SNMPv3
   - SSH

- 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 displays.



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.

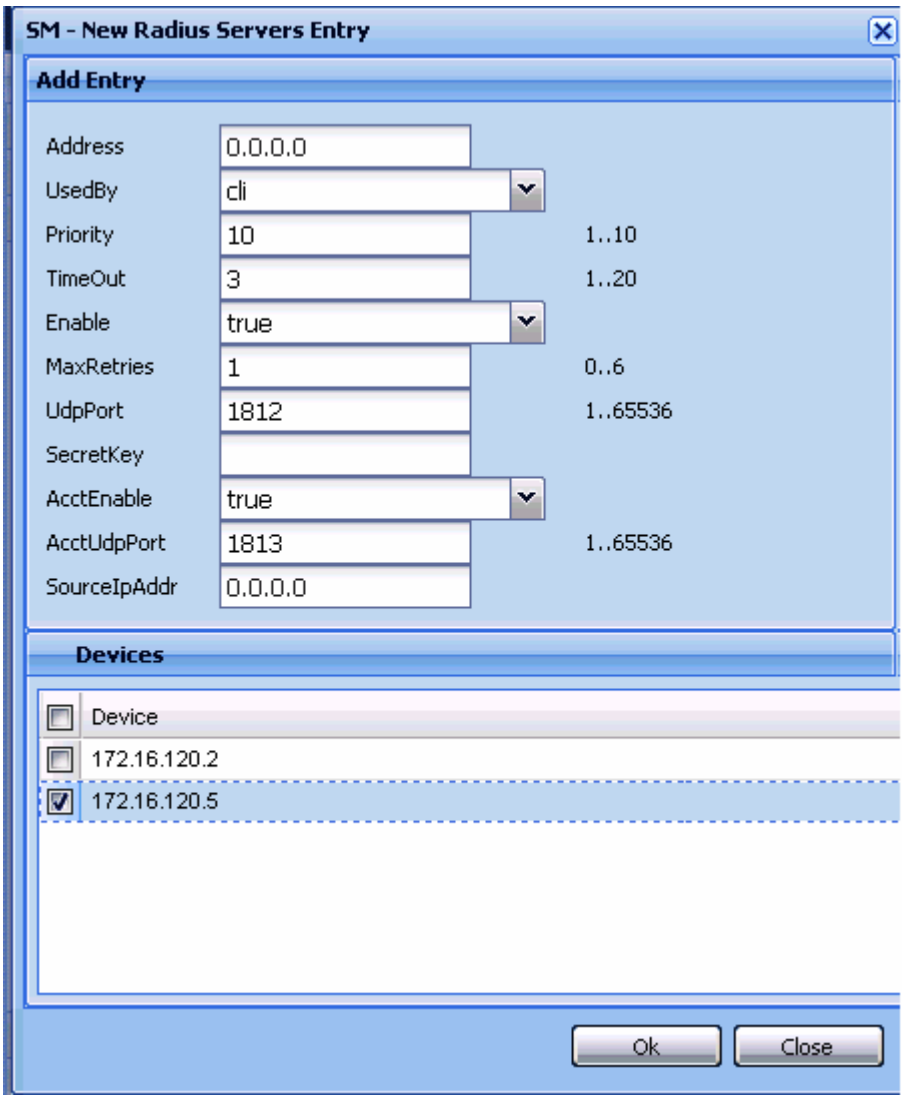
Adding RADIUS servers

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.
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. 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. The default value is 1813.
SourceIpAddr	Configures the source IP address for RADIUS packets.

The following table describes the Radius Servers tab.

Table 29: 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. **Important:** The UDP port value set for the client must be the same as the value set for the RADIUS server.
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.

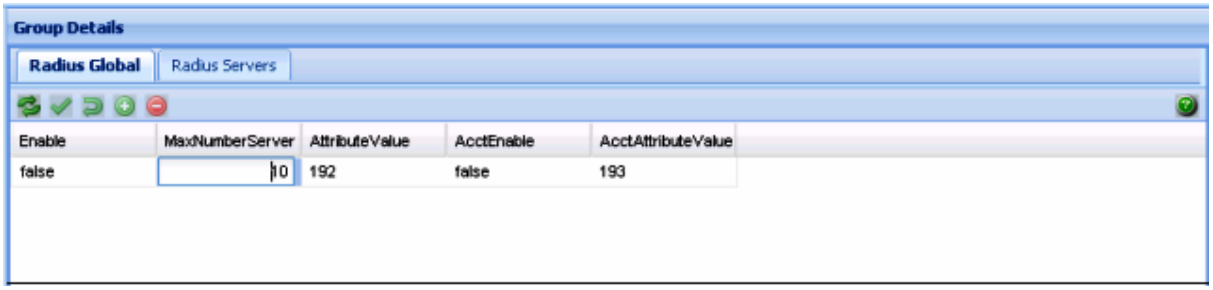
Part	Description
SourceIpAddr	Configures the source IP address for RADIUS packets.

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.
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.

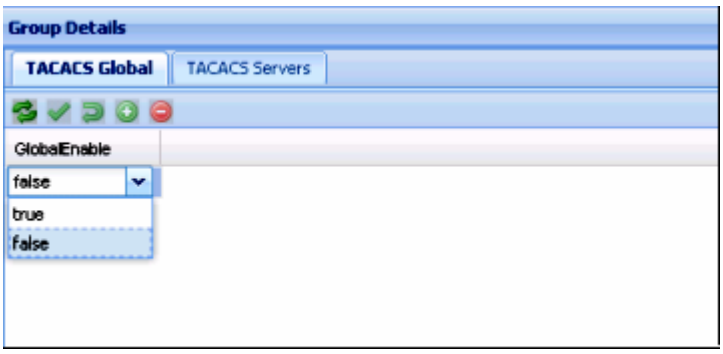
Enabling or disabling TACACS Global

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

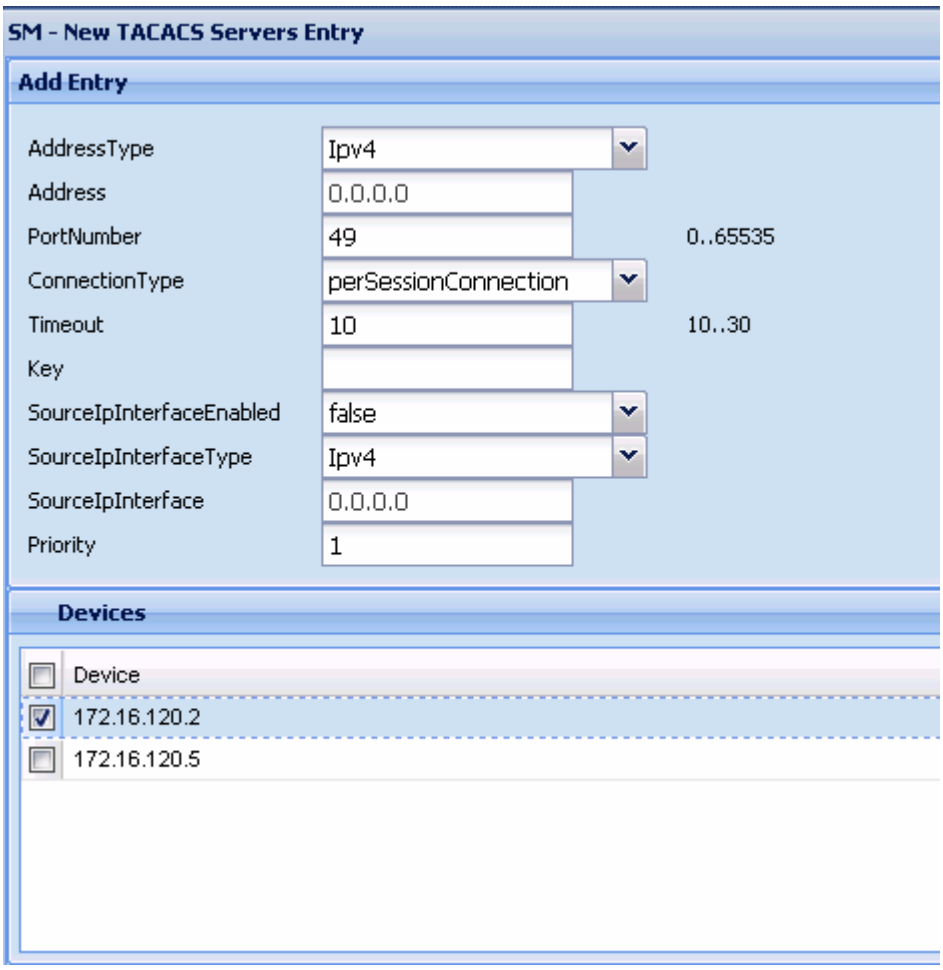
You can add TACACS servers using the Security Manager.

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 30: 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

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

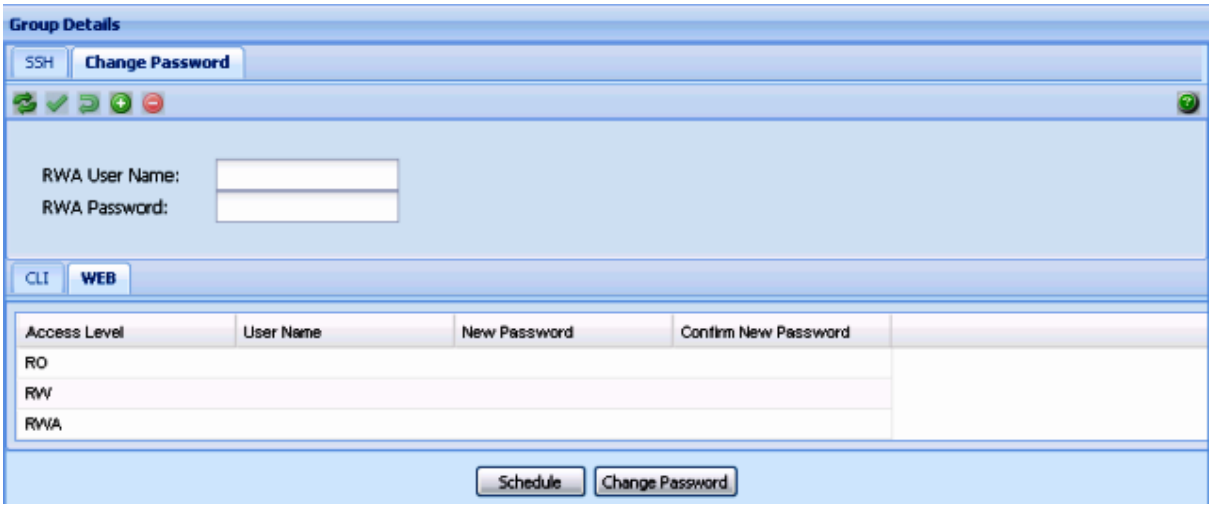
In Security Manager, you can use Secure Shell (SSH) to configure the CLI user name and password for all the devices in a security group. You can also use SSH to configure the SNMP communities for the security group on ERS 55xx/35xx/45xx/25xx, Ethernet Switch devices, and VSP 9xxx devices. Using an SSH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

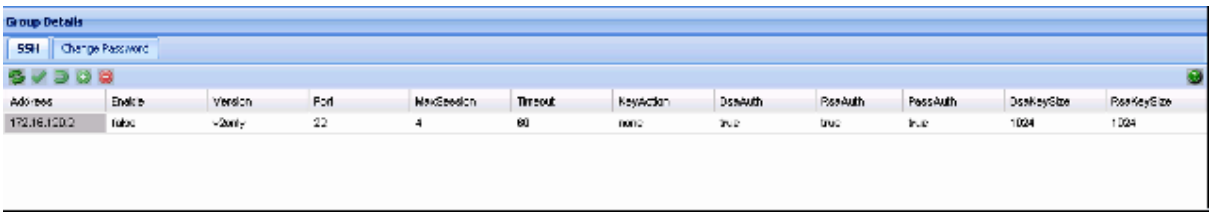
Configuring SSH properties for ERS 8000 and VSP 9xxx security groups and devices

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. 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.

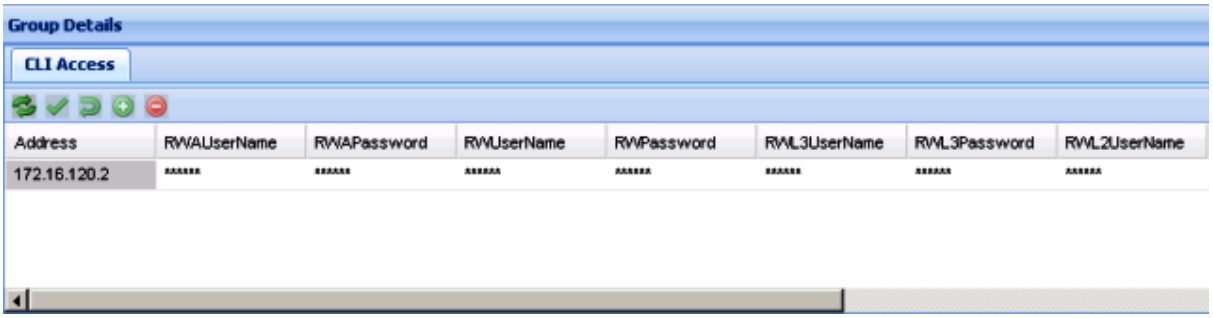


Figure 10: CLI Access tab

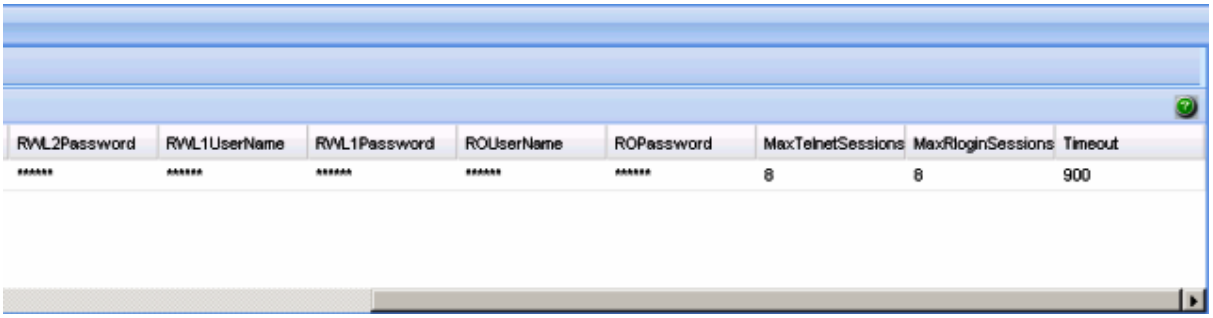


Figure 11: CLI Access tab (contd.)

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.
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.

Part	Description
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

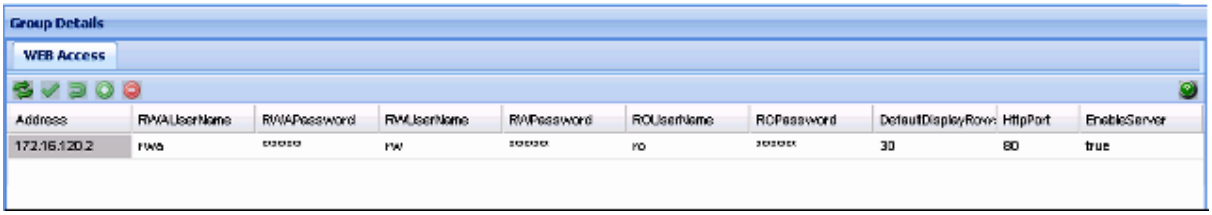
You can use Security Manager to manage access to the Web interfaces for all devices in the security group.

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.

Part	Description
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.

Part	Description
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 SMGR-CS.

After you have configured the SNMP v3 credentials on the device, and in the SMGR-CS 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 172 and Adding a USM user on page 173
- add the user to the VACM group; see Configuring VACM group members on page 175
- assign access levels to the USM group; see Configuring VACM group access on page 174
- create a VACM MIB view; see Configuring the VACM MIB view on page 176

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 31: 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 32: 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 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.

Part	Description
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 33: 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.
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: noAuthNoPriv authNoPriv 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.

Part	Description
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 34: 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 35: 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.

Part	Description
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 36: 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 vacmViewTreeFami lySubtree 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 37: 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 vacmViewTreeFami lySubtree 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 38: 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 39: 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 40: 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.
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 snmpTargetPara msTable 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 41: Job aid

Part	Description
Name	The unique identifier to index this table.
TDomain	The transport type of the address in the snmpTargetAddr TAddressobject.

Part	Description
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 snmpTargetPara msTable 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 42: 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: • noAuthNoPriv • authNoPriv • 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 43: 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: • noAuthNoPriv • authNoPriv • 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 44: 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: • trap • 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 45: 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: • trap • 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 46: 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 47: 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.

Part	Description
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 48: 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.

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 49: 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 185
- Enabling or disabling access policies for devices in a security group on page 187
- Enabling or disabling individual access policies on page 188
- Deleting access policies on page 189

Adding access policies

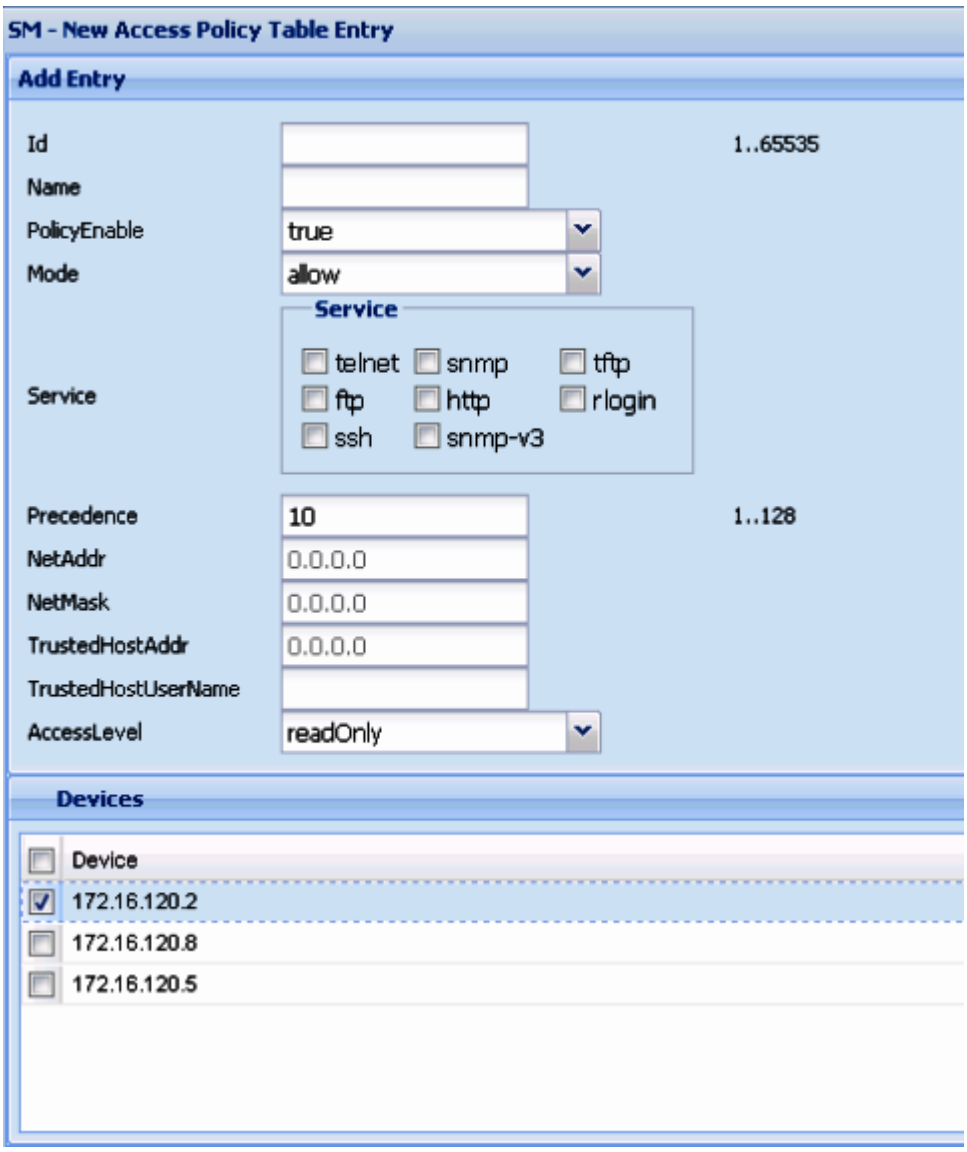
You can control access to Passport and Accelar devices in the security group with access policies. The access policy specifies the hosts or networks that can access the switch through various services.

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.

Part	Description
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.
TrustedHost Addr	Specifies the trusted IP address of the host performing rlogin or rsh into the device. Applies only to rlogin and rsh. **Important:** You cannot use wildcard entries.
TrustedHost UserName	Specifies the user name assigned to the trusted host. Applies only to rlogin and rsh. **Important:** 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.

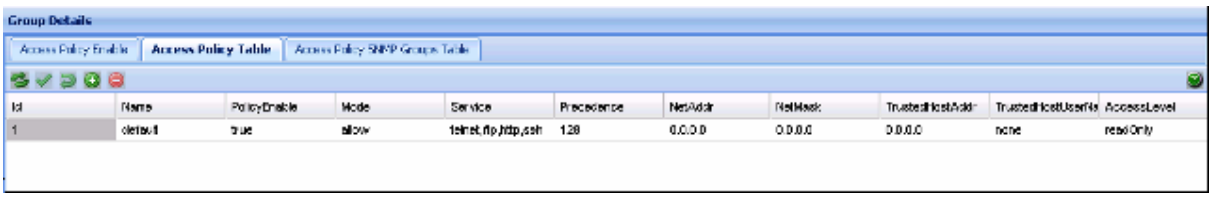
Part	Description
AccessPolicyEnable	Enables or disables access policies for the security group. The available settings are true and false.

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	Activates or deactivates the access policy. See Enabling or disabling individual access policies on page 188 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. **Important:** You cannot use wildcard entries.
TrustedHostUser Name	Specifies the user name assigned to the trusted host. Applies only to rlogin and rsh. **Important:** 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 9: 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

Note:

VSP 8000 does not support IPV6 Routing, IPV6 OSPF, and IPV6 VRRP.

For information about which devices support the protocols in the preceding list, see Supported devices for Routing Manager on page 197.

Starting Routing Manager

Perform the following procedure to start the Routing Manager.

Procedure steps

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

Job aid

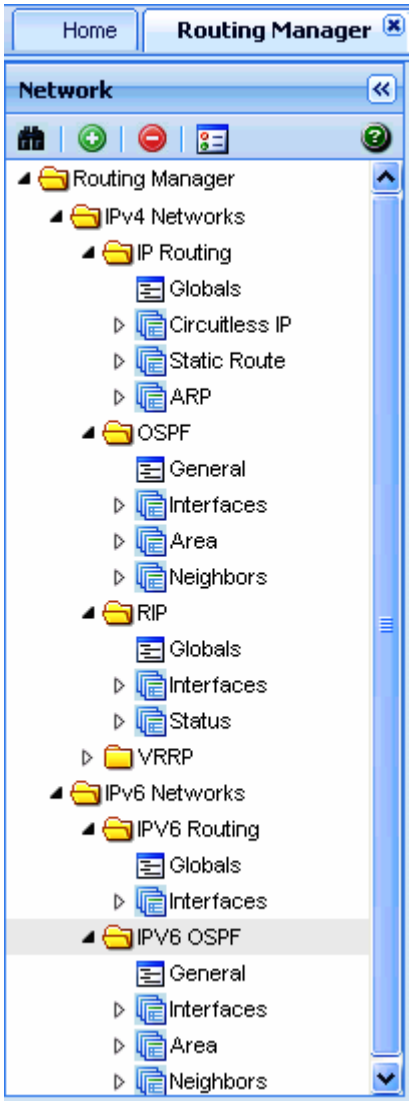
The following table describes the parts of the Routing Manager tool bar.

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.



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

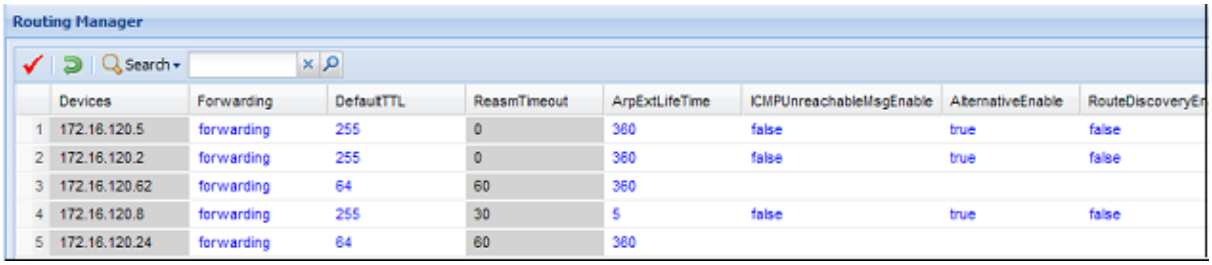
Contents pane

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

1. 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.

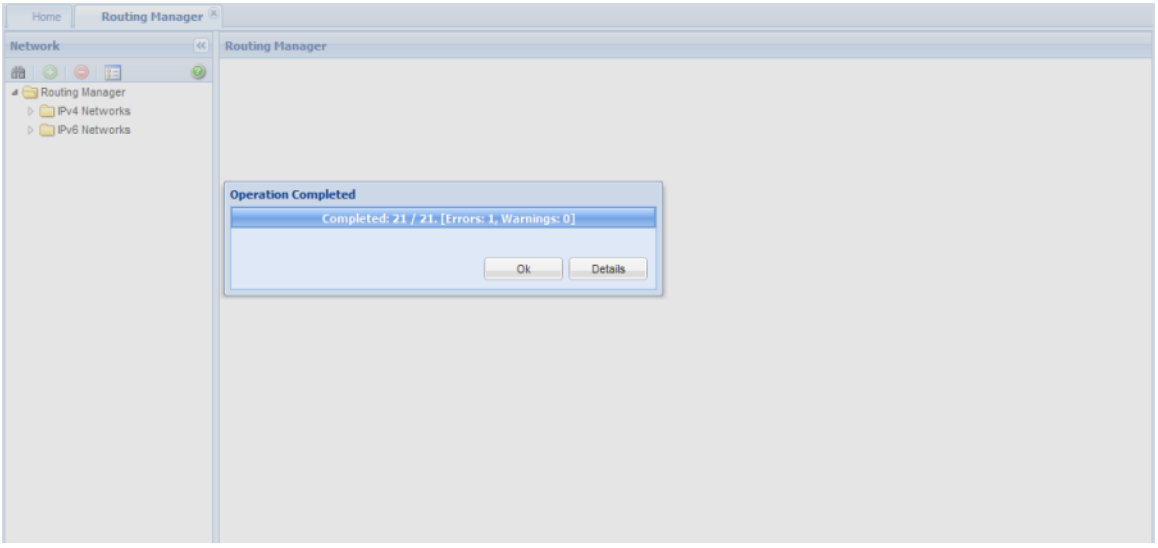
Procedure steps

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.

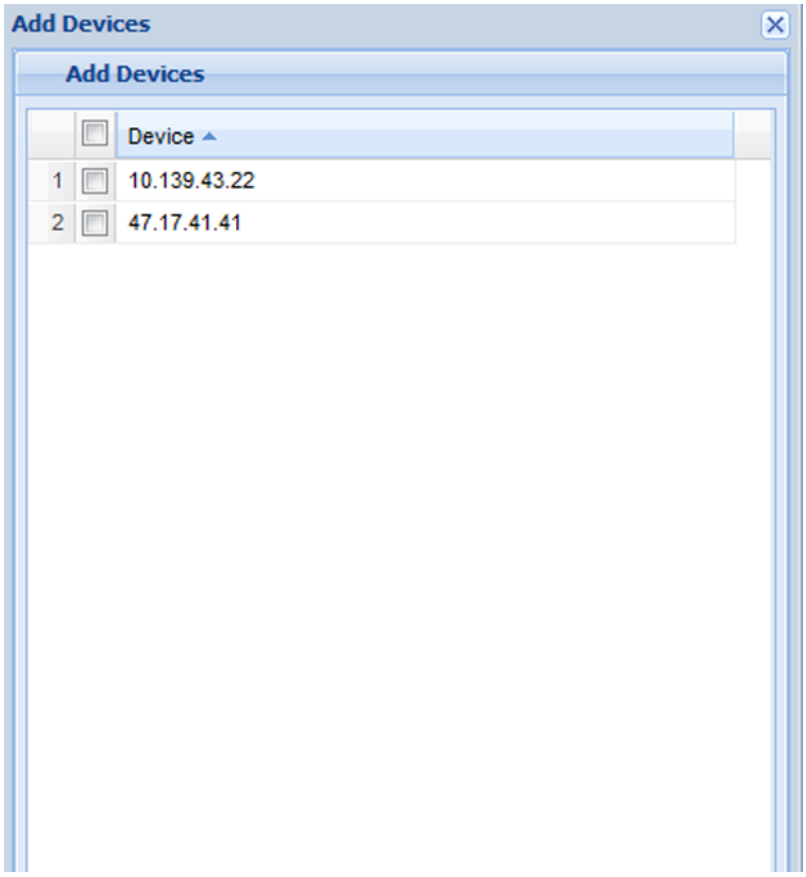


Adding devices

Click **Add Devices** in the toolbar. The available devices for the selected tree node display in the Add Devices window. The available devices can be:

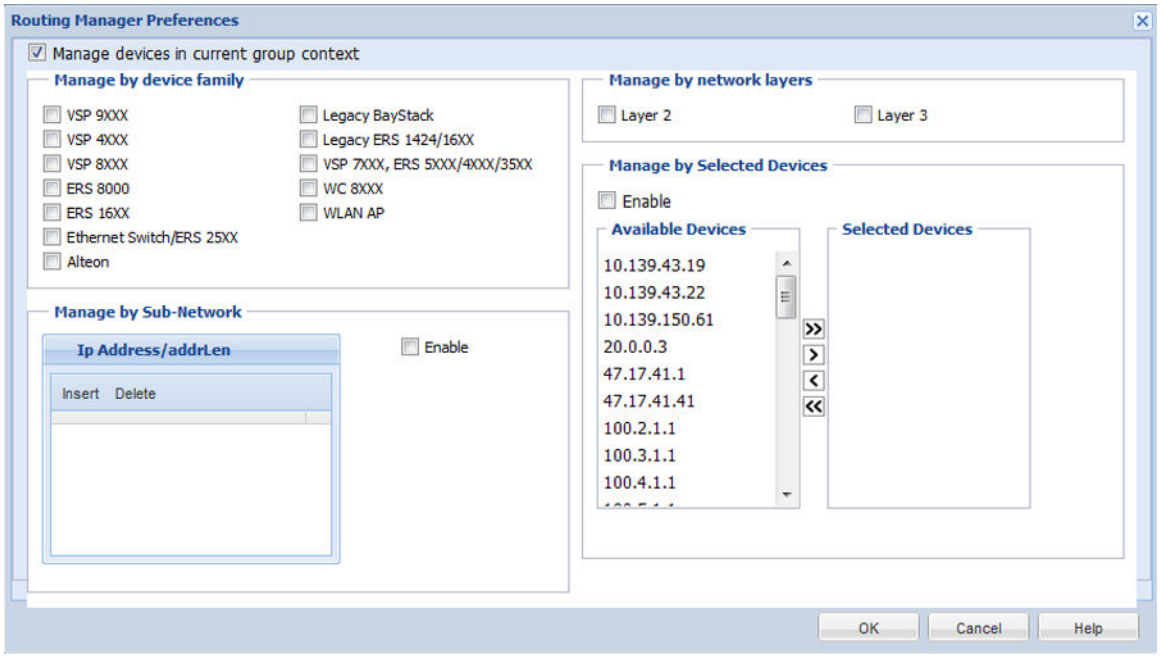
- Devices that have support for the specific protocol (such as, IP Routing/Circuitless).
- Devices that were previously removed from the tree for the specific protocol.

Select the desired devices to add them to the left side tree.



Preferences

Click **Preferences** in the toolbar to display the Routing Manager Preferences window. You can select specific set of assigned devices to be used in the Routing Manager discovery process based on several criteria.



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 197.

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 35xx, ERS 4xxx, ERS 5xxx, devices.

Features		Supported devices			
		ERS 35xx	ERS 4xxx	ERS 5xxx	ERS 16xx
IPv4 Routing	Circuitless IP	not supported	not supported	v6.2.7 and up	v2.0 and up
	Static Route	v5.1.1 and up	v5.5 and up	v4.0 and up	v2.1 and up
	ARP	v5.1.1 and up	v5.5 and up	v3.0 and up	v2.1 and up
OSPF	Interfaces	not supported	v5.5	v5.0 and up	v2.1 and up
	Area	not supported	v5.5	v5.0 and up	v2.1 and up
	Neighbors	not supported	v5.5	v5.0 and up	v2.1 and up
RIP	Interfaces	v5.2	v5.5	v5.0 and up	v2.1 and up
	Status	v5.2	v5.5	v5.0 and up	v2.1 and up
VRRP	Interfaces	not supported	v5.5	v5.0 and up	v2.1 and up
IPv6 Routing	Interfaces	v5.1.1 and up	v5.6.3 and up	v6.2.7 and up	not supported
IPv6 OSPF	Interfaces	not supported	v5.6.3 and up	not supported	not supported
	Area	not supported	v5.6.3 and up	not supported	not supported
	Neighbors	not supported	v5.6.3 and up	not supported	not supported
IPv6 VRRP	Interface	not supported	v5.6.3 and up	not supported	not supported

The following table provides a feature/device matrix for the Routing Manager for VSP 7xxx, VSP 9xxx, and VSP 8xxx, and WC devices.

Features		Supported devices			
		VSP 7xxx	VSP 9xxx	VSP 8xxx	WC 8xxx
IPv4 Routing	Circuitless IP	v10.2 and up	v3.0.0, v4.0	v4.0	not supported
	Static Route	v10.2 and up	v3.0.0, v4.0	v4.0	v1.0.0

Features		Supported devices			
		VSP 7xxx	VSP 9xxx	VSP 8xxx	WC 8xxx
	ARP	v10.2 and up	v3.0.0, v4.0	v4.0	v1.0.0
OSPF	Interfaces	v10.2 and up	v3.0.0, v4.0	v4.0	not supported
	Area	v10.2 and up	v3.0.0, v4.0	v4.0	not supported
	Neighbors	v10.2 and up	v3.0.0, v4.0	v4.0	not supported
RIP	Interfaces	v10.2 and up	v3.0.0, v4.0	v4.0	not supported
	Status	v10.2 and up	v3.0.0, v4.0	v4.0	not supported
VRRP	Interfaces	v10.1 and up	v3.0.0, v4.0	v4.0	not supported
IPv6 Routing	Interfaces	v10.3 and up	v3.0.0, v4.0	not supported	not supported
IPv6 OSPF	Interfaces	v10.3 and up	v4.0	not supported	not supported
	Area	v10.3 and up	v4.0	not supported	not supported
	Neighbors	v10.3 and up	v4.0	not supported	not supported
IPv6 VRRP	Interface	v10.3 and up	v4.0	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 on page 200
- Configuring circuitless IP on page 202
- Configuring IPv4 routing Static Route on page 202
- Configuring IPv4 routing ARP on page 203

Configuring IPv4 routing Globals

Perform the following procedure to configure the IPv4 routing global properties.

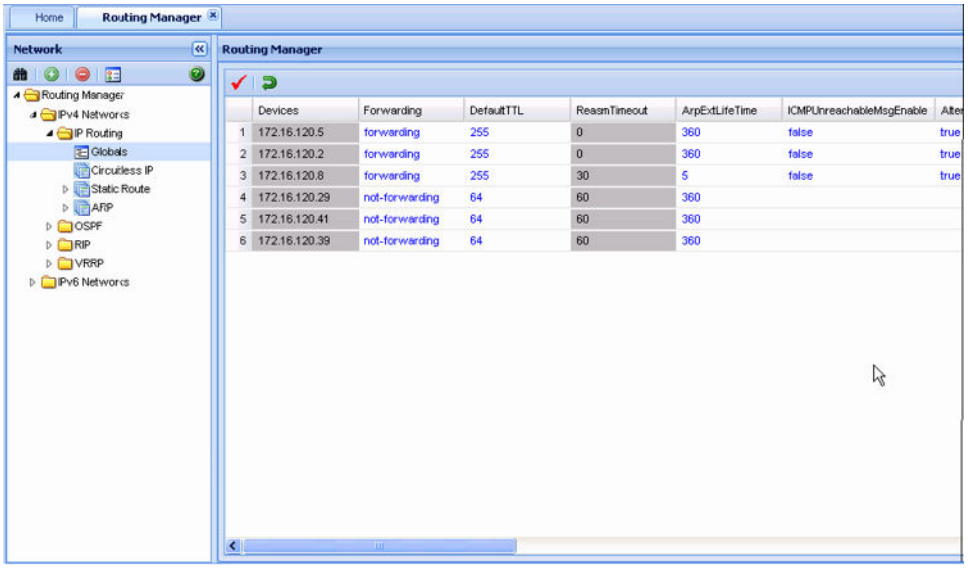
Procedure steps

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.

Field	Description
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.
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. • When the switch is in R mode, the interval is 1 to 8. • When the switch is not in R mode, the interval is 1 to 4. • The default value is 1. 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: • Brouter interfaces are identified by the slot or port number of the brouter port. • 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: • local—a locally configured ARP entry • static—a statically configured ARP entry • dynamic—a learned ARP entry

Configuring OSPF

For a list of devices that support OSPF, see Supported devices for Routing Manager on page 197.

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). **Important:** 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.
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).

Field	Description
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

Field	Description
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. **Important:** 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 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. • none—No authentication required. • simple password—All OSPF updates received by the interface must contain the authentication key specified in the interface AuthKey field. • 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. **Important:** 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.

Field	Description
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.
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 50: 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: • none—no authentication required. • simple password—all OSPF updates received by the interface must contain the authentication key specified in the interface AuthKey field. • 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. **Important:** The link state database (LSDB) is inconsistent if the settings is default area for VLAN.
Advertise WhenDown	Indicates when the interface advertises. **Important:** 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. The OSPF priority for the interface during the election process for the designated route: • designated router—interface with the highest priority number • backup designated router—interface with the second highest priority **Important:** 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 51: 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.

Field	Description
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.

Field	Description
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

For a list of devices that support RIP, see Supported devices for Routing Manager on page 197.

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): • DoNotSend—no RIP updates sent on this interface • ripVersion1—RIP updates compliant with RFC 1058 • rip1Compatible—broadcast RIP2 updates using RFC 1058 route subsumption rules • ripVersion2—multicasting RIP2 updates
Receive	Indicates which versions of RIP updates are accepted: • rip1 • rip2 • rip1OrRip2 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

1. 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.

Field	Description
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.
ProxyAnnounceFlag	Enables or disables proxy announcements on this interface.

Configuring VRRP

For a list of devices that support VRRP, see Supported devices for Routing Manager on page 197.

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): • Enabled—SNMP traps are sent • 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
Interface	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: • initialize—waiting for a startup event • backup—monitoring availability and state of the master router • 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: • preemption—preempt the timer • none—allow the timer to keep working

Field	Description
HoldDown Timer	The time interval (in seconds) a router is delayed for the following conditions: • 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. • 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). • 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	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. • up: during BackupMaster state • 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.

For a list of devices that support IPv6 routing, see Supported devices for Routing Manager on page 197.

Configuring IPv6 routing

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.
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	Enables or disables the fast advertisement interval. When disabled, the regular advertisement interval is used. The default is disabled.
FasterAdvInterval	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.

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.

Field	Description
MulticastAdminStatus	The admin status for multicast for this interface.

Configuring IPv6 OSPF

For a list of devices that support IPv6 OSPF, see Supported devices for Routing Manager on page 197.

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). **Important:** 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.
RxNewLsas	A read-only field displaying the number of new LSAs received. This number does not include new instantiations of self-originated LSAs.

Field	Description
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: • intraAreaMulticast—forwards to directly attached areas (called intra-area multicast routing) • interAreaMulticast—forwards between OSPFv3 areas (called inter-area multicast routing) • 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: • none (default) • plannedOnly • plannedAndUnplanned
RestartStatus	A read-only field indicating the current status of OSPF hitless restart. Options include: • notRestarting (default) • plannedRestart • 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.

Field	Description
RestartExit Reason	A read-only field indicating the outcome of the last attempt at a hitless restart. Options include: • none: indicates no restart was attempted • inProgress: indicates a restart attempt is currently underway • completed: indicates a completed restart • timedout: indicates a timed out restart • 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. **Important:** 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.

Field	Description
HelloInterval	Length of time, in seconds, between Hello packets. This value must be the same for all routers attached to a common network. **Important:** 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: • down • loopback • waiting • pointToPoint • designatedRouter • backupDesignatedRouter • 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.

Field	Description
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: • always

Field	Description
	• candidate (default)
NssaTranslator State	Indicates if and how an NSSA border router translates NSSA type-7 LSAs into type-5 LSAs. Options include: • enabled indicates the NSSA border router translator role is set to always. • elected indicates a candidate NSSA border router is translating type-7 LSAs into type-5. • 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: • rcOspfv3Metric indicates the OSPF metric • comparableCost indicates an external type 1 • 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.
AddressType	A read-only field indicating the address type of rcOspfv3NbrAddress. Only IPv6 addresses without zone index are expected. Options include: • unknown • ipv6

Field	Description
	• ipv6z • 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: • down • attempt • init • twoWay • exchangeStart • exchange • loading • 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: • notHelping • helping
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: • none: indicates no restart was attempted (default) • inProgress: indicates a restart attempt is currently underway • completed: indicates a completed restart • timedout: indicates a timed-out restart

Field	Description
	• topologyChanged: indicates a cancelled restart due to the topology change

Configuring IPv6 VRRP

Configuring IPv6 VRRP Globals

Perform the following procedure to configure IPv6 VRRP Global properties.

Procedure

1. From the COM navigation tree, expand **Managers**, and click **Routing Manager**.
2. From the Routing Manager Network navigation tree, select **Routing Manager** > **IPv6 Networks** > **IPV6 VRRP** > **Globals**, and select a node.

   The Globals table displays in the contents pane.
3. To modify any of the configurable IPv6 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 IPv6 VRRP Globals table.

Field	Description
Devices	Identifies the device.
SysName	Identifies the system name of 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): • Enabled—SNMP traps are sent • Disabled—no traps are sent

Configuring IPv6 VRRP Interfaces

Perform the following procedure to configure the IPv6 VRRP interface properties.

Procedure

1. From the COM navigation tree, expand **Managers**, and click **Routing Manager**.
2. From the Routing Manager Network navigation tree, select **Routing Manager** > **IPv6 Networks** > **IPV6 VRRP** > **Interfaces**, and select a node.
3. To modify any of the configurable IPV6 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 IPv6 VRRP Interfaces table.

Field	Description
Interface	Interface of the VRRP router.
InetAddrType	Specifies the address type for the VRRP interface. In this case, IPv6.
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).
PrimaryIpAddr	Specifies the link-local address assigned to the VRRP.
VirtualMacAddr	The MAC address of the virtual router interface.
State	The state of the virtual router interface: • initialize—waiting for a startup event • backup—monitoring availability and state of the master router • 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.
AdvInterval	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.
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.
UpTime	The time elapsed since the entry was created.
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.
CriticalIpAddrEnabled	Sets the IP interface on the local router to enable or disable the backup.
BackUpMaster	Indicates if the VRRP backup master is enabled or disabled. This option is not recommended for non Split-MLT ports.

Field	Description
BackUpMasterState	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. • up: during BackupMaster state • down: during the original state
FasterAdvIntervalEnabled	Enables or disables the fast advertisement interval. When disabled, the regular advertisement interval is used. The default is disabled.
FasterAdvInterval	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.
AcceptMode	Controls whether a master router accepts packets addressed to the IPv6 address of the address owner as its own if it is not the IPv6 address owner. The default value is disable.
Action	Using the following action list to manually override the delay timer and force preemption: • preemption—preempt the timer • none—allow the timer to keep working
HoldDownTimer	The time interval (in seconds) a router is delayed for the following conditions: • 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. • 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). • The VRRP holddown timer applies to the VRRP BackupMaster feature.
HoldDownTimeRemaining	The remaining time (in seconds) before preemption.

Chapter 10: Configuration of Virtual Routing and forwarding

Virtual Routing Manager is a feature that you can use to configure and manage virtual routing and forwarding on the following devices:

- ERS 8600 v5.0 and above
- ERS 8300 v4.1 and above
- ERS 8800 all versions
- ERS 5xxx v6.3 and above
- VSP 9xxx v3.0
- VSP 4xxx all versions
- VSP 8xxx all versions

You can use Virtual Routing Manager configure Virtual Routing and Forwarding (VRF) for each device, as well as manage VRF configurations across multiple devices.

The 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 devices 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, such as 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/4xxx/8xxx devices 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.

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.

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.

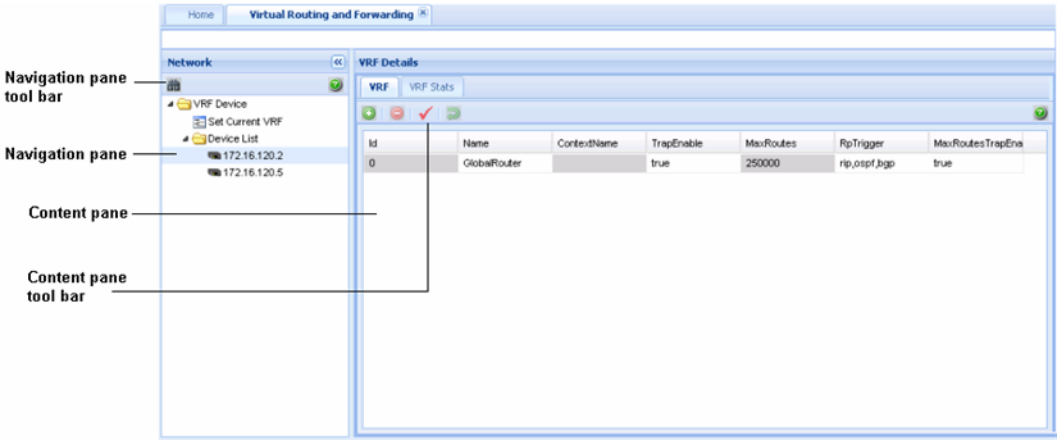
2. Click **Ok** to view the Virtual Routing and Forwarding window.

   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 52: 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.
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.

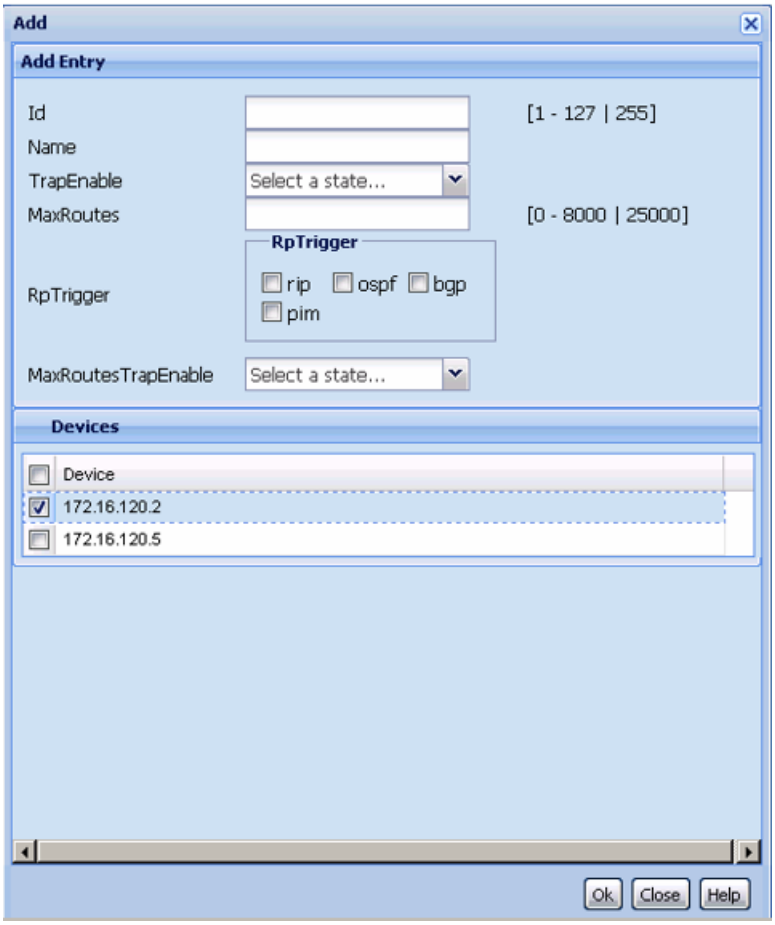
Procedure steps

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 displays in the contents pane.

2. In the **Contents** toolbar, click **Create Entry**.

   The Add Entry dialog box displays.



Note:

VSP 4850 v3.0 and VSP 8284XSQ v4.0 do not support RpTrigger.

3. Configure 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**.

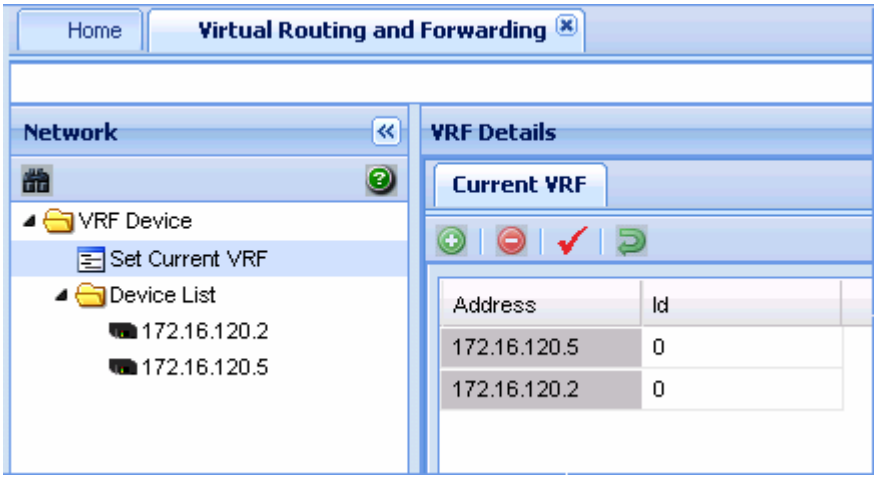
Setting VRF content for devices

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.

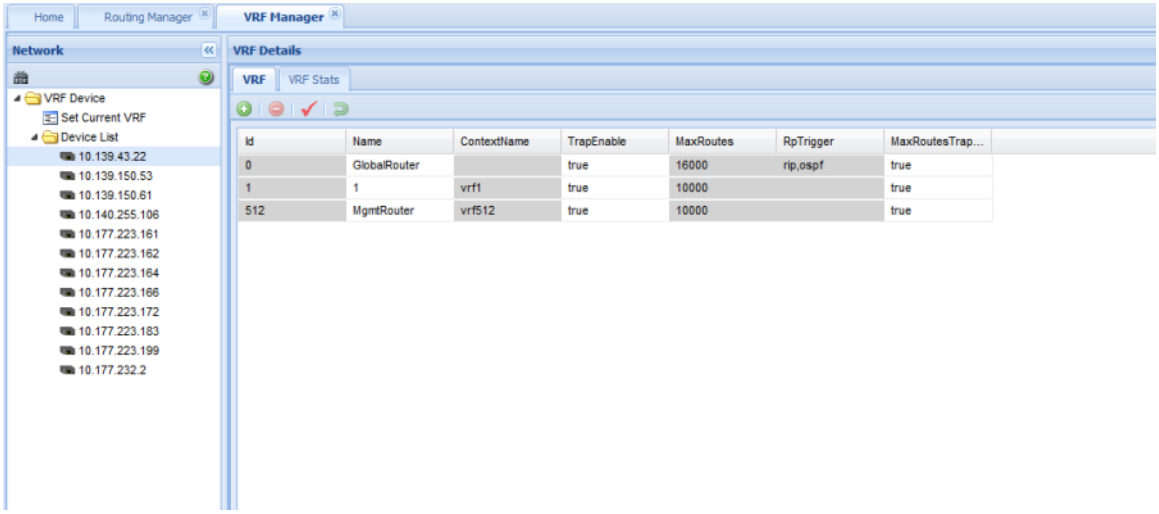
Viewing all the VRFs and its statistics configured for a specific device

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

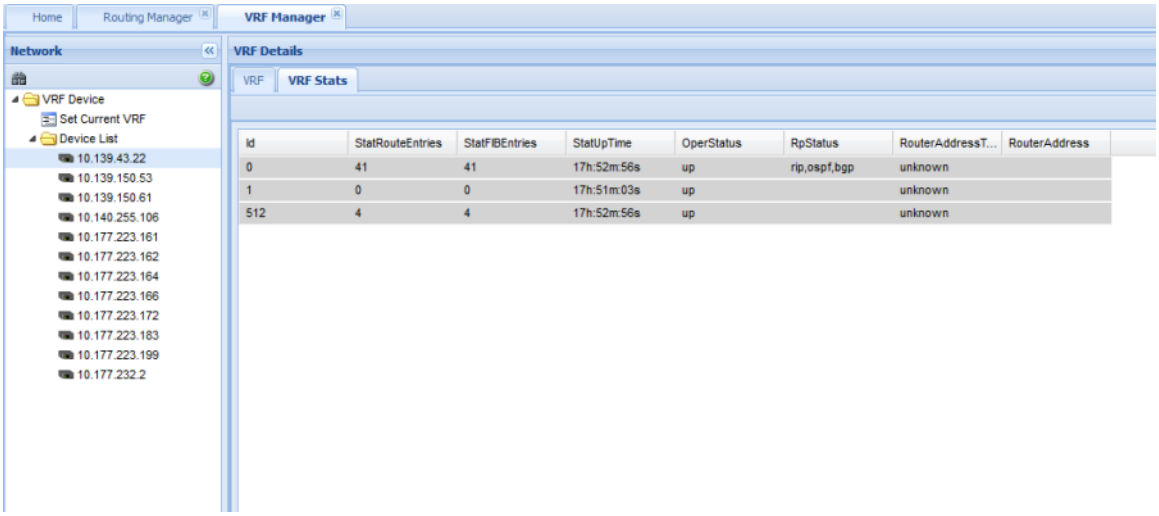
1. In the Navigation pane of Virtual Routing and Forwarding window, expand the **Device List** folder, and select a device from the navigation tree.

   The VRF information displays in the contents pane.



2. To see the VRF statistics in the contents pane, click the **VRF Stats** tab.

   The VRF statistics information displays 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: Management of Multicast devices

With the Avaya Configuration and Orchestration Manager (COM) Multicast Manager you can manage Avaya devices that support multicast. The Multicast manager displays multicast configurations across a network of devices. You can edit the Multicast Manager and highlight multicast information on the topology map; however, to fully configure the multicast network, you must use EDM or JDM.

The Multicast Manager displays the following multicast protocols supported on the devices discovered in the network topology:

- IGMP and IGMP Snoop
- DVMRP
- PIM-SM
- MSDP
- Multicast Route
- Policy

The Multicast Manager requires COM 3.1 and one or more of the following Avaya devices:

- VSP 7000/9000
- VSP 4000 v 3.1 and above
- Ethernet Routing Switch 8600/8800
- Ethernet Routing Switch 48xx/55xx/35xx/45xx/25xx
- Ethernet Routing Switch 1424/16xx
- Ethernet Switch
- Legacy BayStack devices

Related Links

[About Multicast Manager](#) on page 237
[Starting Multicast Manager](#) on page 237
[Actions](#) on page 238
[Navigation tree structure](#) on page 241
[Using tables to change device configuration](#) on page 241
[IGMP and IGMP Snoop](#) on page 241

DVMRP protocol folder on page 261
PIM SM protocol folder on page 268
MSDP Protocol folder on page 276
Multicast Route protocol folder on page 282
Policy folder on page 287
Highlight multicast data in the topology map on page 294

About Multicast Manager

After you launch the Multicast Manager for the first time, the Multicast Manager performs a discovery of devices, and shows the progress of the discovery. As with all Configuration and Orchestration Manager (COM) managers, you can filter the devices through the Manager Preferences button at the top left of the Multicast Manager tab near the Discovery button. You can use the Discovery button to perform subsequent discoveries.

The Multicast Manager user interface (UI) is composed of two parts presented side by side.

- The Multicast Manager Navigation Tree—displays furthest to the left. Expand or collapse the nodes (by clicking on the node handles that appear in front of the node), and then select the node.
- The Multicast Manager Content Panel—displays to the right of the Multicast Manager navigation tree. After you select a node in the Multicast Manager navigation tree, information about the node displays in the Multicast Manager content pane.

Note:

VSP 8000 does not support Multicast Manager functionality.

Related Links

Management of Multicast devices on page 236

Starting Multicast Manager

About this task

Perform the following procedure to launch the Multicast Manager.

Procedure

1. From the COM navigation panel, expand **Managers**.
2. Click **Multicast Manager**.

   The Multicast Manager user interface (UI) appears in separate COM tab.

Related Links

Management of Multicast devices on page 236

Actions

With the Multicast Manager, you can perform manager actions and table actions.

Manager actions

You can perform the following actions in the Multicast Manager context.

- Discover—rediscover device information.
- Add—add devices from the navigation tree (device related tree nodes only).
- Remove Device—removes devices from the navigation tree (device related tree nodes only).
- Highlight on Topology—highlights the device on the topology map.
- Preferences—manage user preferences.
- Help—launch help information.

Table actions

You can perform the following actions in the Multicast Manager single table context; not all operations are available for all tables.

- Add—add a new table row.
- Delete—remove a table row.
- Save—send user changes to the device.

Related Links

Management of Multicast devices on page 236
Performing A Multicast Discovery on page 238
Adding a device in the Multicast Manager on page 239
Deleting a device from the Multicast Manager on page 239
Editing Protocol tables in the Multicast Manager on page 240
Selecting preferences for the Multicast Manager on page 240

Performing A Multicast Discovery

Perform the following procedure to discover devices in the Multicast Manager.

Procedure

1. From the Multicast Manager menu bar, click **Discover Multicast**.

   The Multicast discovery progress bar appears.
2. To view details of the discovery, click **Details**.
3. After the discovery is complete, click **OK**.

Related Links

Actions on page 238

Adding a device in the Multicast Manager

Perform the following procedure to add a device in the Multicast Manager.

Note:

The Add button is available only if you select a major functionality from the Multicast Manager navigation tree.

About this task

The devices that appear on the Availability Device list are available for the following reasons:

- There are devices discovered in the COM application.
- There are devices that are discovered after performing a discovery in the Multicast Manager.
- There are devices that can participate in a protocol if the devices have the proper functionality.

If a device is not capable of a protocol functionality, the device does not appear in the Availability Device list. If the Availability Device list is empty, there are no devices with the proper functionality for the protocol.

Procedure

1. From the Multicast Manager navigation tree, select a location for the device.
2. From the Multicast Manager menu bar, click **Add Devices**.

   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 device, and then click the left-pointing arrow.
4. Click **Select**.

Related Links

Actions on page 238

Deleting a device from the Multicast Manager

Perform the following procedure to remove a device from the Multicast Manager navigation tree.

Procedure

1. From the Multicast Manager navigation tree, select a device.

2. From the Multicast Manager menu bar, click **Delete**.

Related Links

Actions on page 238

Editing Protocol tables in the Multicast Manager

Perform the following procedure to edit Protocol tables in the Multicast Manager

Procedure

1. From the Multicast Manager Navigation Tree, select the appropriate folders and select a device.
2. In the Multicast Data Panel, select a tab.
3. In the table, select a cell with a white background and change the value.
4. Click **Apply Changes**.

Related Links

Actions on page 238

Selecting preferences for the Multicast Manager

Perform the following procedure to manage user preferences.

Procedure

1. From the Multicast Manager menu bar, click **Preferences**.

   The Multicast Manager Preferences window appears.
2. Select or clear the check box to enable or disable the associated filters to manage devices in current group context. The available options to configure Multicast Manager preferences are:
   - Manage by device family—allows you to choose the supported device families: VSP 7XXX, VSP 9XXX, ERS 8000, ERS 16XX, Ethernet Switch/ERS 25XX, Alteon, Legacy BayStack, Legacy ERS 1424/16XX, ERS 55XX/56XX/45XX/35XX, WC 8XXX, and WLAN AP.
   - 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 and click the right-pointing arrow to move the devices to the Selected Devices list.
3. Click **OK**.

Related Links

Actions on page 238

Navigation tree structure

The Multicast Manager displays information about multicast protocols in the navigation and contents panes. The navigation pane provides a hierarchy of protocols and resources that you use to navigate to a specific node. After you select the node, COM provides detailed information about the node through tabs and tables in the contents pane.

The following list outlines the major folders in the navigation tree.

- IGMP and IGMP Snoop protocol
- DVMRP protocol
- PIM SM protocol
- MSDP protocol
- Multicast Route protocol
- Policy

The following sections describe the major folders and the content within the folders.

Related Links

Management of Multicast devices on page 236

Using tables to change device configuration

The Multicast Manager data for a device appears in tables in the contents pane. After you navigate through a tree and select a device or route node, a table appears in the contents pane with cells containing data specific to the device or route node. Each tab above the table represents a different table.

If a cell has a white background, you can configure the cell by changing the data in the cell. However, if you change the data in the cell, you change the configuration of the device.

Related Links

Management of Multicast devices on page 236

IGMP and IGMP Snoop

You configure IGMP and IGMP Snooping using the Device Manager. You can configure all devices supported by Avaya Configuration and Orchestration Manager (COM) for IGMP Snooping. The

IGMP and IGMP Snoop protocol folder contains subfolders for devices that have various IGMP and IGMP Snoop protocol features enabled. To view more information in the contents pane, click a device icon. If there are no devices in the folder, the contents pane does not show information or column headers.

The following table describes the parts of the IGMP and IGMP Snoop protocol folder.

Table 53: Parts of the IGMP and IGMP Snoop folder

Parts	Description
Globals folder	Displays the fast leave mode and the state of traps and logs.
Devices folder	Displays switches that have either DVMRP or PIM enabled globally.
IGAP folder	Displays the state of IGAP parameters for the selected device.
Snoop folder	Displays devices that have either Snoop or proxy snoop enabled on one or more of the devices interfaces.
Stream Limit folder	Displays the state of Stream Limit parameters for the selected device.
SSM folder	Displays the state of Source Specific Multicast (SSM) parameters for the selected device.
Fast Leave folder	Displays devices that have one or more interfaces with Fast Leave enabled.
MRDISC folder	Displays devices that have Multicast Route Discovery enabled.
Access List folder	Displays the Static Members and Group Access folders.

Related Links

Management of Multicast devices on page 236
IGMP and IGMP Snoop Globals folder on page 243
IGMP and IGMP Snoop Devices folder on page 243
IGMP and IGMP Snoop IGAP folder on page 249
IGMP and IGMP Snoop Snoop folder on page 251
IGMP and IGMP Snoop Stream Limit folder on page 253
IGMP and IGMP Snoop SSM folder on page 254
IGMP and IGMP Snoop Fast Leave folder on page 256
IGMP and IGMP Snoop MRDISC folder on page 257
IGMP and IGMP Snoop Access List folder on page 257

IGMP and IGMP Snoop Globals folder

With the Globals folder you can view and configure the fast leave mode and the state of logs and traps.

The following table describes the parts of the IGMP and IGMP Snoop Globals folder.

Table 54: Parts of the IGMP and IGMP Snoop Globals folder

Parts	Description
Devices	IP address of the device.
FastLeaveMode	Controls all IGMP fast leave enabled interfaces. Fast leave mode applies to fast leave enabled IGMP interfaces, not to IGAP interfaces. The modes are: • multipleUser—Removes the IGMP member who sent the Leave message from the group. Traffic is not stopped if there are other receivers on the interface port. This is the default. • oneUser—Removes all group members on a fast leave enabled interface port upon receiving the first Leave message from a member. This behavior is the same as the conventional fast leave process.
GenerateTrap	Enables or disables traps.
GenerateLog	Enables or disables logs.

Related Links

IGMP and IGMP Snoop on page 241

IGMP and IGMP Snoop Devices folder

The Devices folder contains switches that have either DVMRP or PIM enabled globally.

The following table describes the parts of the Devices folder.

Table 55: Parts of the IGMP and IGMP Snoop Devices folder

Parts	Description
Interface tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and above, and ERS 1424/16xx devices	Displays information about ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and above, and ERS 1424/16xx IGMP interfaces.
Cache tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and above, and ERS 1424/16xx devices	Displays information about ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and above, and ERS 1424/16xx multicast groups.

Parts	Description
Groups tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and above, and ERS 8300 devices	Displays information about ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and above, and ERS 8300 multicast groups.
Senders tab for ERS 8600/8800, VSP 9000, VSP 4000 v3.1 and above, and ERS 8300 devices	Displays information about ERS 8600/8800, VSP 9000, VSP 4000 v3.1 and above, and ERS 8300 multicast senders.

Related Links

IGMP and IGMP Snoop on page 241
Interface tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000, and ERS 1424/16xx devices on page 244
Cache tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000, and ERS 1424/16xx devices on page 245
Groups tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000, and ERS 8300 devices on page 246
Senders tab for ERS 8600/8800, VSP 9000, VSP 4000, and ERS 8300 devices on page 247
IGMPv3 Cache tab for VSP 9000 devices on page 248
Router Source List tab for VSP 9000 devices on page 249

Interface tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000, and ERS 1424/16xx devices

The Interface tab of the IGMP and IGMP Snoop Devices folder displays information about the IGMP interfaces used.

The following table describes the parts of the Interface tab. An asterisk indicates a field that applies to ERS 8600/8800 and VSP 7000, VSP 9000, VSP 4000 v3.1 and above devices only. Otherwise, the field applies to ERS 8600 and ERS 1424/16xx devices.

Table 56: Parts of the IGMP and IGMP Snoop Devices folder Interface tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v 3.1 and above, and ERS 1424/16xx devices

Part	Description
Interface	Interface on which IGMP is enabled.
Status	Indicates if the device is Active or Not In Service.
Version	Version of IGMP that is configured on the interface. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN.
OperVersion*	Version of IGMP that is running on this interface.
Query Interval	Frequency with which IGMP Host-Query packets are transmitted on this interface.
Querier	Address of the IGMP querier on the IP subnet to which the interface is attached.

Part	Description
QueryMaxResponse Time	Maximum query response time advertised on the interface.
WrongVersionQueries	Number of queries received whose IGMP versions do not match the IGMP version of this interface.
Joins	Number of times a group membership has been added on this interface; that is, the number of times an entry for this interface has been added to the cache table. This number indicates the amount of IGMP activity over time.
Robustness	Variable that allows tuning for the expected packet loss on a subnet.
LastMembQueryIntrvl	Max Response Time in Group-Specific Queries sent in response to Leave Group messages. Also, the amount of time between Group-Specific Query messages.
OtherQuerierPresent Timeout Not applicable for VSP 7000.	Length of time taken by Multicast router to determine if there is any other router to be the querier. If the local router is the querier, the value is 0.
FlushAction For VSP 7000, the attribute name is ExtnFlushAction.	Flushes the sender or the group member or the router.
RouterAlertEnable For VSP 7000, the attribute name is ExtnRouterAlertEnable.	This parameter, when enabled, instructs the router to process packets addressed to it indirectly. Set the parameter according to the version of IGMP currently in use to maximize the network performance. The parameters are: • IGMPv1—Disable • IGMPv2—Enable • IGMPv3—Enable
SsmEnable Not applicable for VSP 7000 devices.	Enables SSM.

Related Links

IGMP and IGMP Snoop Devices folder on page 243

Cache tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000, and ERS 1424/16xx devices

The Cache tab displays the following information about multicast groups.

- The interfaces that receive the multicast groups.
- The last host that sent a report for the multicast groups.
- The expected expiry time for the multicast groups.

The following table describes the parts of the IGMP and IGMP Snoop Devices folder Cache tab. An asterisk indicates a field that applies to ERS 1424/16xx devices only. Otherwise, the field applies to ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and up, and ERS 1424/16xx devices.

Table 57: IGMP and IGMP Snoop Devices folder Cache tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000, and ERS 1424/16xx devices

Part	Description
Address	The IP Multicast group address for which the entry contains information.
IfIndex	The interface from which the corresponding multicast group address is heard.
UpTime For VSP 7000, the attribute name is ExtnType.	The time elapsed since the entry was created.
Self*	Sets whether to advertise local routes to neighbors.
LastReporter	The IP address of the source of the last membership report received for an IP Multicast group address on an interface. If no membership report is received, then the object has the value 0.0.0.0.
ExpiryTime	The amount of time, in seconds, remaining before this entry is aged out.
Status*	The IGMP row status. If an interface has an IP address and DVMRP or PIM-SM is enabled, the status appears as active. Otherwise, it is shown as notInService.
Version1HostTimer	The time remaining until the local router assumes that there are no longer any IGMP version 1 members on the IP subnet attached to the interface. After hearing any IGMPv1 membership report, the value is reset to the group membership timer. After the time remaining is nonzero, the local router dismisses any IGMPv2 Leave messages for a group that the local router receives on an interface.

Related Links

IGMP and IGMP Snoop Devices folder on page 243

Groups tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000, and ERS 8300 devices

The following table describes the parts of the IGMP and IGMP Snoop Devices folder Groups tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and up, and ERS 8300 devices.

Table 58: Parts of the IGMP and IGMP Snoop Devices folder Groups tab for ERS 8600/8800, VSP 7000, VSP 9000, , VSP 4000 v3.1 and up, and ERS 8300 devices

Part	Description
IpAddress	Multicast group Address (Class D) that members can join. A group address can be the same for many incoming ports.
IfIndex	A unique value that identifies a physical interface or a logical interface (VLAN) that receives Group reports from various sources.
Members	IP address of a member that has issued a group report for this group.
InPort	A unique value to identify a router interface or a logical interface (VLAN) that has received Group reports from various members.
Expiration	Time left before the group report expires on this port. COM updates this variable after receiving a group report.

Related Links

IGMP and IGMP Snoop Devices folder on page 243

Senders tab for ERS 8600/8800, VSP 9000, VSP 4000, and ERS 8300 devices

The following table describes the parts of the IGMP and IGMP Snoop Devices folder Senders tab for ERS 8600/8800, VSP 9000, VSP 4000 v3.1 and up, and ERS 8300 devices.

Table 59: Parts of the IGMP and IGMP Snoop Devices folder Senders tab for ERS 8600/8800, VSP 9000, VSP 4000 v3.1 and up, and ERS 8300 devices

Part	Description
GrpAddr	Enter the Multicast group address of the multicast stream. Within the indicated valid range (224.0.1.0 to 239.255.255.255), the following are invalid addresses: 244.0.0.x and the corresponding 31 multicast addresses that map to the IP MAC addresses. If you select an invalid addresses, you receive an invalid message.
IfIndex	The interface on which the IGMP entry is enabled.
MemberAddr	The IP address of a host that contains information about the entry.
TPort	Identifies the T Port.

Related Links

IGMP and IGMP Snoop Devices folder on page 243

IGMPv3 Cache tab for VSP 9000 devices

The following table describes the parts of the IGMP and IGMP Snoop Devices folder IGMPv3 Cache tab for VSP 9000 devices.

Table 60: Parts of the IGMP and IGMP Snoop Devices folder IGMPv3 Cache tab for VSP 9000 devices

Part	Description
GroupAddress	Multicast group Address (Class D) that members can join. A group address can be the same for many incoming ports.
IfIndex	A unique value that identifies a physical interface or a logical interface (VLAN) that receives Group reports from various sources.
InPort	An unique value to identify a physical interface or a logical interface (VLAN), which has received Group reports from various sources.
ModeExpiryTimer	This value is applicable only to IGMPv3-compatible nodes and represents the time remaining before the interface EXCLUDE state expires and the interface state transitions to INCLUDE mode. This value can never be greater than rcIgmpNewGroupExpiration.
Version1HostTimer	The time remaining until the local router assumes that there are no longer any IGMP version 1 members on the IP subnet attached to this interface. This entry only applies to IGMPv1 hosts. After hearing any IGMPv1 Report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv2 Leave messages for this group that it receives on this interface.
Version2HostTimer	The time remaining until the local router assumes that there are no longer any IGMP version 2 members on the IP subnet attached to this interface. After hearing any IGMPv2 Membership Report, this value is reset to the group membership timer. Assuming no IGMPv1 hosts have been detected, the local router does not ignore any IGMPv2 Leave messages for this group that it receives on this interface.
SourceFilterMode	The current group state, applicable to IGMPv3-compatible nodes. The value indicates whether the state is INCLUDE or EXCLUDE.

Related Links

IGMP and IGMP Snoop Devices folder on page 243

Router Source List tab for VSP 9000 devices

The following table describes the parts of the IGMP and IGMP Snoop Devices folder Router Source List tab for VSP 9000 devices.

Table 61: Parts of the IGMP and IGMP Snoop Devices folder Router Source List tab for VSP 9000 devices

Part	Description
GroupAddress	Multicast group Address (Class D) that members can join. A group address can be the same for many incoming ports.
IfIndex	A unique value that identifies a physical interface or a logical interface (VLAN) that receives Group reports from various sources.
InPort	A unique value to identify a physical interface or a logical interface (VLAN), that has received Group reports from various sources.
HostAddress	The host address to which the entry corresponds.
MemberAddress	The IP Address of a member that sends a source specific report requesting to join the source.
Expire	Indicates the relevance of the SrcList entry. A non-zero value indicates an INCLUDE state value, and a zero value indicates an EXCLUDE state value.
Mode	The current member state, applicable to IGMPv3-compatible nodes. The value indicates whether the state is INCLUDE or EXCLUDE.
MemberExpire	Indicates the time until the member for this sourceexpires.

Related Links

IGMP and IGMP Snoop Devices folder on page 243

IGMP and IGMP Snoop IGAP folder

IGAP is an authentication and accounting protocol that extends the functionality of the Internet Group Management Protocol (IGMPv2) by providing user authentication.

Related Links

IGMP and IGMP Snoop on page 241
IGAP tab on page 250
IGAP Groups on page 250
IGAP Counters on page 251

IGAP tab

The following table describes the parts of the IGAP tab in the IGMP and IGMP Snoop, IGAP folder.

Table 62: Parts of the IGAP tab

Part	Details
IfIndex	The slot and port number or the VLAN ID for the interface.
IgapEnable	Enables or disables IGAP.
AccntEnable	Enables or disables IGAP Accounting.
AuthEnable	Enables or disables IGAP Authentication.

Related Links

IGMP and IGMP Snoop IGAP folder on page 249

IGAP Groups

The following table describes the parts of the IGAP Groups from the IGMP and IGMP Snoop, IGAP folder.

Table 63: Parts of the IGAP Groups

Part	Details
IpAddress	The IP address of the IGAP group.
Members	The IP address of the IGAP group member.
IfIndex	The VLAN name that uniquely identifies the interface.
InPort	The ingress port of the IGAP report.
Expiration	Specifies how much time is left (in seconds) before the Group Report for the interface expires. This timer restarts after the RADIUS server receives a new group report.
Member State	The state of the IGAP group member. The states are: • Auth—indicates that the member is authenticated by a RADIUS server. • Acct—indicates that a RADIUS server successfully started accounting for the member session.
Session Time	The accounting time, in seconds, for the duration of the multicast session for the IGAP group member.
UserID	The UserID of the VLAN interface

Related Links

IGMP and IGMP Snoop IGAP folder on page 249

IGAP Counters

The following table describes the parts of the IGAP Counters tab from the IGMP and IGMP Snoop, IGAP folder.

Table 64: Parts of the IGAP Counters tab

Part	Details
IfIndex	The VLAN name that uniquely identifies the interface.
Auth Success	The number of authentication success messages received from the RADIUS server on this interface.
AuthReject	The number of authentication fail messages received from the RADIUS server on this interface.
Resp Timeout	The number of times that the Authentication Timer times out. The timer controls the waiting time between sending an Authentication request and receiving an Authentication response.
PapJoinReq	The number of Password Authentication Protocol (PAP) Join requests received for members of this interface.
BasicQuery	The number of Basic Query messages sent by the ERS 8600/8800 or VSP 9000 on an IGAP-enabled interface.
BasicLeave	The number of Basic Leave messages received by this interface.

Related Links

IGMP and IGMP Snoop IGAP folder on page 249

IGMP and IGMP Snoop Snoop folder

The Snoop folder of the IGMP and IGMP Snoop protocol folder contains devices that have either Snoop, or proxy snoop enabled on one or more device interfaces.

The following section describes the parts of the IGMP and IGMP Snoop, Snoop folder.

Related Links

IGMP and IGMP Snoop on page 241
IGMP Snoop folder on page 251
IGMP Snoop Router Ports folder on page 252

IGMP Snoop folder

The following table describes the parts of the IGMP Snoop folder.

Table 65: Parts of the IGMP Snoop folder

Part	Description
rcVlanId For VSP 7000, the attribute name is IfIndex.	The VLAN ID for the VLAN.
SnoopEnable	Enables or disables IGMP snooping. IGMP snooping works only when a multicast router exists in the VLAN. The values are True to enable, and False to disable.
SnoopReportProxyEnable For VSP 7000, the attribute name is ProxySnoopEnable.	Indicates if the IGMP report proxy feature is enabled. If this feature is enabled, reports are forwarded from hosts to the multicast router once per group per query interval, or when there is new group information. If this feature is disabled, all reports from different hosts are forwarded to multicast routers, and more than one group report may be forwarded for the same multicast group per query interval. The default is enabled.
SnoopActiveQuerier For VSP 7000, the attribute name is SnoopActiveMRouterPorts.	The IP address of a multicast querier router.
SnoopQuerierPort For VSP 7000, the attribute name is SnoopMRouterPort.	The port on which the multicast querier router is heard.
SnoopMRouter Expiration	Time remaining before the multicast router is aged out. If the switch does not receive any queries before the time expires, the switch flushes out all group memberships known to the VLAN. The Query Max Response Interval, obtained from the queries received, is used as the timer resolution.

Related Links

IGMP and IGMP Snoop Snoop folder on page 251

IGMP Snoop Router Ports folder

The following table describes the parts of the IGMP Snoop Router Ports folder.

Table 66: Parts of the IGMP Snoop Router Ports folder

Part	Description
SnoopMRouterPorts	Ports that have been configured as multicast router ports. Such ports are directly attached to a multicast router so the multicast data and group reports are forwarded to the router.

Part	Description
	Important: Configure this field only when there are multiple multicast routers that are not directly attached to one another, but are directly attached to the VLAN. If multicast routers have a route between them and this field is configured, a multicast loop forms.

Related Links

IGMP and IGMP Snoop Snoop folder on page 251

IGMP and IGMP Snoop Stream Limit folder

With Multicast stream limitation you can limit the number of multicast groups that can join a VLAN, and set the maximum number of streams independently. You can restrict users from receiving more than a set limit of multicast streams on a given interface, and you can control the overall bandwidth usage.

Related Links

IGMP and IGMP Snoop on page 241
Stream Limit tab on page 253
Stream Limit Members tab on page 254
Adding a device to IGMP and IGMP Snoop Stream Limit on page 254

Stream Limit tab

The following table describes the parts of the Stream Limit tab.

Table 67: Parts of the Stream Limit tab

Part	Details
IfIndex	The slot and port number or the VLAN ID for the interface.
StreamLimit Enable	Enables or disables stream limitation on the interface.
MaxStreams	Sets the maximum number of streams allowed on the interface. The range is from 0 to 65535. The default is 4.
Num Streams	The current number of streams received on the interface. This is a read-only value.

Related Links

IGMP and IGMP Snoop Stream Limit folder on page 253

Stream Limit Members tab

The following table describes the parts of the Stream Limit Members tab.

Table 68: Parts of the Stream Limit Members tab

Part	Details
IfIndex	The VLAN name.
Port	A list showing each slot and port number for the interface that has stream limitation enabled.
MaxStreams	Sets the maximum number of allowed streams for the specific port. The number of allowed streams cannot exceed the maximum number for the interface. The range is from 0 to 65535. The default is 4.
Num Streams	The current number of streams received on this interface. This is a read-only value.

Related Links

IGMP and IGMP Snoop Stream Limit folder on page 253

Adding a device to IGMP and IGMP Snoop Stream Limit

Perform the following procedure to add a device to the IGMP and IGMP Snoop Stream Limit.

Procedure

1. From the Multicast Manager Navigation tree, select **IGMP and IGMP Snoop**, and click **Stream Limit**.
2. From the Multicast Manager toolbar, click **Add Devices**.
3. From the Add Devices list, choose one device, or more than one device.
4. Click **Save**.

Related Links

IGMP and IGMP Snoop Stream Limit folder on page 253

IGMP and IGMP Snoop SSM folder

The Source Specific Multicast (SSM) service model defines a channel identified by a source address and an SSM destination address, known as an (S,G) pair. Avaya Configuration and Orchestration Manager (COM) uses an SFM-capable group management protocol such as IGMPv3 or MLDv2 to describe channel subscriptions, and only requires source-based forwarding trees to implement this model.

Related Links

IGMP and IGMP Snoop on page 241

SSM Global tab on page 255
SSM Channel tab on page 255
Adding a device to IGMP and IGMP Snoop SSM on page 256

SSM Global tab

The following table describes the parts of the IGMP and IGMP Snoop SSM global tab.

Table 69: Parts of the IGMP and IGMP Snoop SSM global tab

Part	Details
Dynamic Learning	The slot and port number or the VLAN ID for the interface.
AdminAction	Sets the admin state, which determines whether or not the switch uses the table entries. The table entries are: • none—Does not set the admin state globally so that you can set it for individual SSM channel table entries. The default value is none. • enableAll—Globally activates all the static entries in the SSM channel table. This setting does not affect the dynamically learned entries. • disableAll—Globally inactivates all the static entries in the SSM channel table. This setting does not affect the dynamically learned entries.
RangeGroup	Sets the IP Multicast group address. The lowest group address is 224.0.1.0 and the highest is 239.255.255.255. The default is 232.0.0.0.
RangeMask	Sets the address mask of the multicast group. The default is 255.0.0.0.

Related Links

IGMP and IGMP Snoop SSM folder on page 254

SSM Channel tab

The following table describes the parts of the IGMP and IGMP Snoop SSM Channel tab.

Table 70: Parts of the IGMP and IGMP Snoop SSM Channel tab

Part	Details
IpMulticast Grp	Any IP Multicast address that is within the SSM range.
IpSource	The IP address of the source that sends traffic to the group.

Part	Details
Learning Mode	Indicates if the entry is statically configured or dynamically-learned from IGMPv3. This a read-only field. The values are Static and Dynamic.
Activity	The current activity of the selected (S,G) entry. True indicates that traffic is flowing to the switch. This is a read-only field for the ERS 8600.
AdminState	The admin state for the selected static entry. This state determines whether or not the switch uses the static entries. Set this field to enable to use the entry, or disable to save for future use. The default value is enable.

Related Links

IGMP and IGMP Snoop SSM folder on page 254

Adding a device to IGMP and IGMP Snoop SSM

Perform the following procedure to add a device to the IGMP and IGMP Snoop SSM.

Procedure

1. From the Multicast Manager Navigation tree, select **IGMP and IGMP Snoop**, and **SSM**.
2. From the Multicast Manager toolbar, click **Add Devices**.
3. From the Add Devices list, choose one device, or more than one device.
4. Click **Save**.

Related Links

IGMP and IGMP Snoop SSM folder on page 254

IGMP and IGMP Snoop Fast Leave folder

The Fast Leave folder of the IGMP and IGMP Snoop protocol folder displays the devices that have one or more interfaces with Fast Leave enabled.

The following table describes the parts of the Fast Leave folder.

Table 71: IGMP and IGMP Snoop Fast Leave folder

Parts	Description
Interface	The interface on which Fast Leave is enabled.
Fast Leave Enable	Indicates whether Fast Leave is enabled.
Fast Leave port members	The set of ports that are enabled for fast leave.

Related Links

IGMP and IGMP Snoop on page 241

IGMP and IGMP Snoop MRDISC folder

The MRDISC, or Multicast Route Discovery, folder of the IGMP and IGMP Snoop protocol folder displays the devices that have MRDISC enabled.

The following table describes the parts of the MRDISC folder.

Table 72: Parts of the IGMP and IGMP Snoop MRDISC folder

Part	Description
Interface	The interface on which IGMP is enabled.
MrdiscEnable	Indicates whether MRDISC is enabled.
Discovered route ports	Lists ports discovered by IGMP Multicast Router Discovery (MRDISC) Protocol.
Max advertise interval	The maximum time allowed between sending router advertisements from the interface, in seconds. The range is between 2 and 180 seconds. The default is 20 seconds.
Min advertise interval	The minimum time allowed between sending unsolicited router advertisements from the interface, in seconds. The value must be more than 3 seconds but no greater than the value assigned to the MaxAdvertiseInterval value.
Max initial advertise interval	Sets the maximum number, in seconds, of multicast advertisement intervals that you can configure on the switch.
Max initial advertisements	Used to set the maximum number of initial multicast advertisements that you can configure on the switch.
Neighbor dead interval	The time interval, in seconds, before the router interface drops traffic after you leave the multicast group.

Related Links

IGMP and IGMP Snoop on page 241

IGMP and IGMP Snoop Access List folder

The Access List folder of the IGMP and IGMP Snoop protocol folder contains the Static Members folder and the Group Access folder.

Related Links

IGMP and IGMP Snoop on page 241
Static Members folder on page 258
Group Access folder on page 259

Static Members folder

The Static Members folder of the IGMP and IGMP Snoop protocol folder displays the devices that have static members configured for any multicast group.

The following table describes the parts of the Static Members folder.

Table 73: Parts of the IGMP and IGMP Snoop Access List Static Members folder

Part	Description
Interface	The interface on which IGMP is enabled.
Group address	Multicast group address of the multicast stream.
Member ports	Ports that redirect the multicast stream for the multicast group. The ports are member ports of the VLAN.
Not allowed to join	Ports that do not receive the multicast stream for the multicast group.

Related Links

IGMP and IGMP Snoop Access List folder on page 257
Adding a device to IGMP static members folder on page 258
Inserting a device in the IGMP Static list on page 258

Adding a device to IGMP static members folder

Perform the following procedure to add a device to the IGMP static members folder.

Procedure

1. From the Multicast Manager Navigation tree, select **IGMP and IBMP Snoop** > **Access list** > **Static Members**.
2. From the Multicast Manager toolbar, click **Add Devices**.
3. From the Add Devices list, choose one device, or more than one device.
4. Click **Save**.

Related Links

Static Members folder on page 258

Inserting a device in the IGMP Static list

Perform the following procedure to insert a device in the IGMP Static list.

Procedure

1. From the Multicast Manager Navigation tree, select **IGMP and IGMP Snoop** > **Access List** > **Static Members**, and select a device.
2. From the Multicast Data Panel toolbar, click **Add Entry with Form**.

3. Enter the following properties:
   - Vlan IDs — Click the down arrow to select a value. This field is required.
   - GrpAddr — This field is required.
   - MemberPorts
   - NotAllowedToJoin
4. Click **Save**.
5. Click **Apply Changes**.

Related Links

Static Members folder on page 258

Group Access folder

The Group Access folder of the IGMP and IGMP Snoop protocol folder displays information about hosts that are either denied transmission, denied reception, or denied both transmission and reception of multicast traffic.

The appearance of the Group Access folder is different for ERS 8600 and ERS 8300 devices.

Related Links

IGMP and IGMP Snoop Access List folder on page 257
Adding a device to IGMP Group access folder on page 259
Inserting a device in the Group access list on page 259
Group Access folder for ERS 8600/8800, and VSP 9000 on page 260
Group Access folder for ERS 8300 on page 261

Adding a device to IGMP Group access folder

Perform the following procedure to add a device to the IGMP Group access folder.

Procedure

1. From the Multicast Manager Navigation tree, select **IGMP and IBMP Snoop** > **Access List** > **Group Access**.
2. From the Multicast Manager toolbar, click **Add Devices**.
3. From the Add Devices list, choose one device, or more than one device.
4. Click **Save**.

Related Links

Group Access folder on page 259

Inserting a device in the Group access list

Perform the following procedure to insert a device in the Group access list.

Procedure

1. 1. From the Multicast Manager Navigation tree, select **IGMP and IGMP Snoop** > **Access List** > **Group Access**, and select a device.
2. From the Multicast Data Panel toolbar, click **Add Entry with Form**.
3. Enter the following properties:
   - Select Interface Type — Click the down arrow and select **use Port** or **Use VLAN**.
   - Vlan IDs — Click the down arrow and select a value.
   - IFIndex — This field is required.
   - PrefixListId — This field is required.
   - HostAddr — This field is required.
   - HostMask — This field is required.
   - PrefixListName
   - Action Mode — Click the down arrow and select one of the following options: denyTX, denyRX, denyBOTH, allowTX, allowRX, allowBOTH.
4. Click **Save**.
5. Click **Apply Changes**.

Related Links

Group Access folder on page 259

Group Access folder for ERS 8600/8800, and VSP 9000

The following table describes the parts of the Group Access folder for ERS 8600/8800, and VSP 9000.

Table 74: Parts of the Group Access folder for ERS 8600/8800, and VSP 9000

Part	Description
Interface	The interface on which the IGMP entry is enabled.
PrefixListId	A numeric string that identifies the prefix list.
HostAddr	The IP address of the host.
HostMask	The subnet mask that determines the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the host network.
PrefixListName	The name of the prefix list.
ActionMode	Specifies whether the host identified by HostAddr should be: • Denied IP multicast transmitted traffic. The value is denyTX.

Part	Description
	• Denied IP multicast received traffic. The value is denyRX. • Denied both IP multicast transmitted and received traffic. The value is denyBOTH. • Allowed IP multicast transmitted traffic. The value is allowTX. • Allowed IP multicast received traffic. The value is allowRX. • Allowed both IP multicast transmitted and received traffic. The value is allowBOTH.

Related Links

Group Access folder on page 259

Group Access folder for ERS 8300

The following table describes the parts of the Group Access folder for ERS 8300.

Part	Description
Interface	Port number or VLAN name.
Group address	Multicast group address of the multicast stream.
Host address	IP address of the host whose membership is to be controlled.
Host mask	Subnet mask of the host whose membership is to be controlled.
Mode	The host address mode, which can be one of the following: • denyTx—deny transmit mode • denyRx—deny receive mode • denyBoth—deny transmit and receive mode

Related Links

Group Access folder on page 259

DVMRP protocol folder

The Distance Vector Multicast Routing Protocol (DVMRP) protocol folder contains subfolders for devices that have various DVMRP protocol features enabled.

The following table describes the parts of the DVMRP protocol folder.

Table 75: Parts of the DVMRP protocol folder

Part	Description
Globals	Displays the devices that have DVMRP globally enabled.
Interfaces folder	Displays the information about the interfaces with DVMRP enabled.
Routes folder	Displays the routing information for devices that participate in multicast routing.
Dvmrp RPB Trees folder	Displays the reverse path broadcast (RPB) tree for all possible sources within the network.

Related Links

Management of Multicast devices on page 236
DVMRP Globals folder on page 262
DVMRP Interfaces folder on page 263
DVMRP Routes folder on page 265
DVMRP RPB Trees folder on page 268

DVMRP Globals folder

The Globals folder of the DVMRP protocol folder shows the devices that have DVMRP globally enabled.

The following table describes the parts of the Globals table.

Table 76: Parts of the DVMRP Globals folder

Part	Description
Devices	The IP address, system name, or host name of the device.
Enable	Indicates whether DVMRP is enabled or disabled.
UpdateInterval	Periodically, each multicast router advertises routing information about each DVMRP interface, using the DVMRP export message. This field shows the time interval, in seconds, between DMVRP updates. The range is from 10 to 2000. The default is 60. In DVMRPv3, this variable is also known as the Route Report Interval.
TriggerredUpdate Interval	Triggered updates are sent when routing information changes. This value is the amount of time, in seconds, between triggered update messages. The range is from 5 to 1000. The default is 5. In DVMRPv3, this variable is also known as the Minimum Flash Update Interval.

Part	Description
LeafTimeOut	When DVMRP advertises a route on an interface, DVMRP waits a period of time for a DVMRP neighbor to respond positively. If no neighbor responds in the given time, the router considers the network attached to the interface to be a leaf network. The leaf timer shows you how long, in seconds, the router waits for a response from a neighbor. The range is from 25 to 4000. The default value is 125.
NbrTimeOut	The neighbor report timer specifies how long, in seconds, the router waits to receive a report from a neighbor before considering the connection inactive. The range is from 35 to 8000. The default of 35.
NbrProbeInterval	How often the DVMRP router sends probe messages on its interfaces. The range is 5 to 30 seconds. The default is 10 seconds.
RouteExpireTimeOut	The route expiration timeout in seconds.
FwdCacheTimeOut	The value used in aging prune entries in seconds.
RouteDiscard TimeOut	The garbage collect route timeout in seconds.
RouteSwitchTimeOut	The route discard timeout in seconds.

Related Links

DVMRP protocol folder on page 261

DVMRP Interfaces folder

The DVMRP Interface folder of the DVMRP protocol folder displays information about the interfaces with DVMRP enabled.

Related Links

DVMRP protocol folder on page 261
Interfaces tab on page 263
Interfaces Advance tab on page 264

Interfaces tab

The following table describes the parts of the Interfaces tab.

Table 77: Parts of the DVMRP Interfaces tab

Part	Description
Interface	DVMRP interface, slot and port number or VLAN identification.

Part	Description
OperState	Current operational state of the DVMRP interface (up or down).
LocalAddress	IP address of the DVMRP router interface.
Metric	The distance metric for the interface is used to calculate the distance vectors. The range is 1 to 31. The default value is 1, and it is only for local delivery.

Related Links

DVMRP Interfaces folder on page 263

Interfaces Advance tab

The following table describes the parts of the Interfaces Advance tab.

Table 78: Parts of the DVMRP Interfaces Advance tab

Part	Description
IfIndex	Provides the DVMRP interface, VLAN, or slot/port number identification.
LocalAddress	Provides the IP address of the DVMRP router interface.
Enable	Enables or disables DRMRP on the interface. The values are true if enabled, and false if disabled.
Metric	Specifies the distance metric for the interface, and calculates distance vectors. The range is from 1 to 31 hops.
InPolicy	Selects the name of the DVMRP accept policy applied to the interface.
OutPolicy	Selects the name of the DVMRP announce policy applied to the interface.
AdvertiseSelf	Sets the interface to advertise (true) or not advertise (false) its local route to neighbors. The default value is True.
DefaultListen	Sets the interface to listen or not listen for the default route. The values are true to listen, and false to not listen. The default is true, which indicates that the interface listens to the default route.
DefaultSupply	Sets the interface to supply or not supply only the default route. The values are true to supply and false to not supply. The default is false, which indicates not to supply a default route on that interface.
DefaultRouteMetric	Sets the metric, which is the number of hops for DVMRP, of the default route. The range is from 1 to 31 hops.

Part	Description
InterfaceType	Sets the interface type as passive or active.

Related Links

DVMRP Interfaces folder on page 263

DVMRP Routes folder

The Routes folder of the DVMRP protocol folder displays routing information for devices that have DVMRP globally enabled.

The following table describes the parts of the Routes folder.

Table 79: Parts of the DVMRP Routes folder

Part	Description
Routes tab	Displays the table of routes learned through DVMRP route exchange.
Neighbors tab	Displays the DVMRP neighbors that are discovered by receiving DVMRP messages.
Next Hops tab	Displays the next hop on outgoing interfaces for routing IP multicast datagrams.

Related Links

DVMRP protocol folder on page 261
Routes tab on page 265
Neighbors tab on page 266
Next Hops tab on page 267

Routes tab

The DVMRP Route tab of the Routes folder displays the table of routes learned through DVMRP route exchange.

The following table describes the parts of the Routes tab.

Table 80: Parts of the DVMRP Routes folder Routes tab

Part	Description
Source	The network address, combined with the corresponding route SourceMask value, identifies the sources for which the entry contains multicast routing information.
SourceMask	The network mask, combined with the corresponding route Source value, identifies the sources for which the entry contains multicast routing information.

Part	Description
Upstream Neighbor	Address of the upstream neighbor, that is the RPF neighbor, from which IP datagrams from these sources are received; or 0.0.0.0 if the network is local.
Interface	DVMRP interface slot and port number, or VLAN ID on which IP datagrams sent by these sources are received.
Metric	Distance in hops to the source subnet. The range is 1 to 32.
ExpiryTime	Amount of time, in seconds, remaining before the entry is aged out.

Related Links

DVMRP Routes folder on page 265

Neighbors tab

The Neighbors tab of the Routes folder displays the DVMRP neighbors that are discovered by receiving DVMRP messages.

The following table describes the parts of the Neighbors tab.

Table 81: Parts of the DVMRP Routes folder Neighbors tab

Part	Description
Interface	The DVMRP slot and port number or the virtual interface (VLAN) used to reach the DVMRP neighbor.
Address	IP address of the DVMRP neighbor for which the entry contains information.
ExpiryTime	Time remaining before the DVMRP neighbor is aged out.
GenerationID	Neighboring router generation ID number.
MajorVersion	Neighboring router major DVMRP version number.
MinorVersion	Neighboring router minor DVMRP version number.
Capabilities	Neighboring router capabilities. The probe flag is 1 byte long with the lower 4 bits containing the following information: • The leaf bit (0) indicates that the neighbor has only one interface with neighbors. • The prune bit (1) indicates that the neighbor supports pruning. • The generationID bit (2) indicates that the neighbor sends its generation ID in probe messages.

Part	Description
	• The mtrace bit (3) indicates that the neighbor can handle mtrace requests.
State	State of neighbor adjacency. The states are: • oneway—The switch recognizes a packet from the neighbor but no adjacency is established. • active—Adjacency exists in both directions. • ignoring—The switch ignores neighbor packets. • down—The interface is not enabled.

Related Links

DVMRP Routes folder on page 265

Next Hops tab

The Next Hop tab of the Routes folder displays the next hop on outgoing interfaces for routing IP multicast datagrams.

The following table describes the parts of the Next Hops tab.

Table 82: Parts of the DVMRP Routes folder Next Hops tab

Part	Description
Interface	DVMRP interface slot and port number or VLAN ID for the outgoing interface for the next hop.
Type	The type is: • leaf—if no downstream dependent neighbors exist on the outgoing virtual interface. • branch—if downstream dependent neighbors exist on the outgoing virtual interface.
Source	The network address that, when combined with the corresponding next hop SourceMask value, identifies the source for which the entry specifies a next hop on an outgoing interface.
SourceMask	The network mask that, when combined with the corresponding next hop Source value, identifies the source for which the entry specifies a next hop on an outgoing interface.

Related Links

DVMRP Routes folder on page 265

DVMRP RPB Trees folder

The DVMRP RPB Trees folder of the DVMRP protocol folder displays the Reverse Path Broadcast (RPB) tree for all possible sources within the network. The following table describes the parts of the DVMRP RPB Trees folder.

Table 83: Parts of the DVMRP RPB Trees folder

Part	Description
Device	The IP address, system name, or host name of the device.
Upstream Neighbor	Address of the upstream neighbor,the RPF neighbor, from which IP datagrams from these sources are received; or 0.0.0.0 if the network is local.
Interface	DVMRP interface, slot and port number, or VLAN ID on which IP datagrams sent by these sources are received.
Metric	Distance in hops to the source subnet. The range is 1 to 32.
ExpiryTime	Amount of time, in seconds, remaining before the entry is aged out.

Related Links

DVMRP protocol folder on page 261

PIM SM protocol folder

Protocol Independent Multicast-Sparse Mode (PIM-SM) routes multicast packets to multicast groups, and establishes distribution trees across wide area networks. The PIM-SM protocol folder contains subfolders for PIM-SM features and elements.

The following table describes the parts of the PIM-SM protocol folder.

Table 84: Parts of the PIM SM protocol folder

Part	Description
Globals	Displays the devices that have PIM globally enabled.
Interfaces folder	Displays the PIM-enabled interface for each device.
Candidate RPs folder	Displays the candidate RP nodes.
Static RPs folder	Displays the static RP nodes.
Redundant RPs folder	Displays all of the multicast groups that are covered by redundant RPs.

Part	Description
Bootstrap Switches folder	Displays all configured BootStrap switches.

Related Links

Management of Multicast devices on page 236
PIM SM Globals folder on page 269
PIM SM Interfaces folder on page 270
PIM SM Candidate RPs folder on page 272
PIM SM Static RPs folder on page 273
PIM SM Redundant RPs folder on page 274
PIM SM Bootstrap Switches folder on page 275

PIM SM Globals folder

The Globals table of the PIM SM protocol folder displays devices that have PIM globally enabled.

The following table describes the parts of the Globals table.

Table 85: Parts of the PIM SM Globals folder

Part	Description
Devices	The IP address, system name, or host name of the device.
Enable	Indicates whether PIM-SM is enabled or disabled.
Mode	The configured mode of this interface. Sparse is the only valid entry.
Mbr	Indicates whether the PIM multicast border router feature is enabled or disabled.
JoinPruneInterval	Specifies how long to wait, in seconds, before the PIM router sends out the next join/prune message to upstream neighbors. The default is 60 seconds.
RegisterSuppTimer	Each source DR maintains, per (S.G.) a register-suppression timer in seconds which the Register-Stop message starts. After the timer expires, the source DR resumes sending data packets to the RP.
StaticRP	Indicates whether the static RP feature is enabled or disabled.
UniRouteChgTimeOut	Timer that provides improved tuning on how fast the routing information is updating from RTM. It is the frequency at which the RTM is polled for routing information updates.
DiscardDataTimeOut	Timer to discard data until the Join is received from the RP. When the timer expires or Join is received, a ipmc discard record is created and deleted.

Part	Description
CRPADVTimeOut	Timer is used to send C-RP-Adv messages periodically by configuring routers as candidate RPs. After expiry a C-RP-Adv message is sent to the elected BSR.
BootStrapPeriod	The interval between the originating Bootstrap messages at the elected BSR.
ActivityChkInterval	Used for polling PIM SG traffic activity information.
FwdCacheTimeOut	The PIM forward cache expiry value in seconds. This value is used for aging PIM mroutes.
FirstJoinPrune	Pim Fast Join Prune.

Related Links

PIM SM protocol folder on page 268

PIM SM Interfaces folder

The PIM SM Interfaces folder displays switch nodes that have PIM globally enabled. Nodes are listed by IP address. After you select a node, two tabs appear in the contents pane:

- Interfaces tab—provides parameters associated with PIM interfaces.
- Clip Interfaces tab—provides parameters associated with circuitless IP (Clip) interfaces.

Parameters appear under the Interfaces tab; each row represents an interface. To add an interface, use the insert + button. You can edit individual interface parameters when the field has a white background. To remove an interface, select the interface and select the delete icon.

Related Links

PIM SM protocol folder on page 268
Interfaces tab on page 270
Clip Interfaces tab on page 271

Interfaces tab

The following table lists the parameters available under the Interfaces tab.

Table 86: Parameters available under the Interfaces tab

Part	Description
IfIndex	The interface index.
Address	The IP address of the PIM interface.
NetMask	The network mask for the IP address of the PIM interface.
Mode	The configured mode of the interface. Valid modes are SSM and Sparse. This is a read-only field.

Part	Description
DR	The router with the highest IP address on a LAN designated to perform these tasks.
HelloInterval	The waiting time in seconds before the PIM switch sends out the next hello message to neighboring switches. The default is 30 seconds.
JoinPruneInterval	The waiting time in seconds before the PIM switch sends out the next join or prune message to its upstream neighbors. The default is 60 seconds.
CBSRPreference	Sets your preference for the local interface to become a Candidate BSR. The Candidate BSR with the highest BSR-priority and address is referred to as the preferred BSR. The default is -1, which indicates that the current interface is not a Candidate BSR.
Type	Indicates if the selected interface is active or passive: • Active—PIM control traffic can be transmitted and received. • Passive—PIM control traffic is not transmitted or received. The passive type reduces the load on a system. To configure a high number of PIM interfaces, connect the interfaces to end users and not to other switches. If the selected interface is disabled, use the type field to change the interface type to passive or active.
OperState	Indicates the status of PIM on the interface. The values are enabled or disabled.

Related Links

PIM SM Interfaces folder on page 270

Clip Interfaces tab

The following table lists the parameters available under theClip Interfaces tab.

Table 87: Parameters available under the Clip Interfaces tab

Part	Description
Interface	The slot and port number, or VLAN identification of the interface.
Ip Address	The IP address of the Clip interface.
PimEnable	Enables or disables PIM on the Interface.

Part	Description
PimMode	The configured mode of the interface. The valid modes are dense, sparse, sparseDense, and SSM.

Related Links

PIM SM Interfaces folder on page 270

PIM SM Candidate RPs folder

A Candidate Rendezvous Point (RP) is a switch configured to advertise itself as a candidate RP for multicast groups. The Candidate RPs folder of the PIM SM protocol folder displays the candidate RP nodes.

The following table describes the parts of the Candidate RPs folder.

Table 88: Parts of the PIM SM Candidate RPs folder

Part	Description
Group address	The IP address of the multicast group. If combined with the group mask, the Group address identifies the prefix that the local router uses to advertise itself as a Candidate RP.
Group mask	The address mask of the multicast group. If combined with the group address, the Group mask identifies the prefix that the local router uses to advertise itself as a Candidate RP.
Interface address	The IP address of the Candidate RP. The interface address must be one of the local PIM-SM enabled interfaces.

Related Links

PIM SM protocol folder on page 268
Adding a device to the PIM_SM candidates RPs folder on page 272
Inserting a device into the PIM_SM Candidates RPs list on page 273

Adding a device to the PIM_SM candidates RPs folder

Perform the following procedure to add a device to the PIM_SM candidates RPs folder.

Procedure

1. From the Multicast Manager Navigation tree, select **PIM_SM** > **Candidates RPs** .
2. From the Multicast Manager toolbar, click **Add Devices**.
3. From the Add Devices list, choose one device, or more than one device.
4. Click **Save**.

Related Links

PIM SM Candidate RPs folder on page 272

Inserting a device into the PIM_SM Candidates RPs list

Perform the following procedure to insert a device into the PIM_SM Candidates RPs list.

Procedure

1. From the Multicast Manager Navigation tree, select **PIM_SM** > **Static RPs**, and select a device.
2. From the Multicast Data Panel toolbar, click **Add Entry with Form**.
3. Enter the following properties:
   - Group Address
   - Group Mask.
   - Address
4. Click **Save**.
5. Click **Apply Changes**.

Related Links

PIM SM Candidate RPs folder on page 272

PIM SM Static RPs folder

Static Rendezvous points (RP) are switches that are configured statically for various multicast groups. The Static RPs folder of the PIM SM protocol folder displays the static RP nodes.

The following table describes the parts of the Static RPs folder.

Table 89: Parts of the PIM SM Static RPs folder

Part	Description
Group address	The IP address of the multicast group. If combined with the group mask, the Group address identifies the prefix that the local router uses to advertise itself as a Static RP.
Group mask	The address mask of the multicast group. If combined with the group address, the Group mask identifies the prefix that the local router uses to advertise itself as a Static RP.
Interface address	The IP address of the Static RP. This address has to be one of the local PIM-SM enabled interfaces.

Related Links

PIM SM protocol folder on page 268

Adding a device to the PIM_SM Static RPs folder on page 274
Inserting a device into the PIM_SM Static RPs list on page 274

Adding a device to the PIM_SM Static RPs folder

Perform the following procedure to add a device to the PIM_SM Static RPs folder.

Procedure

1. From the Multicast Manager Navigation tree, select **PIM_SM** > **Static RPs**.
2. From the Multicast Manager toolbar, click **Add Devices**.
3. From the Add Devices list, choose one device, or more than one device.
4. Click **Save**.

Related Links

PIM SM Static RPs folder on page 273

Inserting a device into the PIM_SM Static RPs list

Perform the following procedure to add a device into the PIM_SM Static RPs list.

Procedure

1. From the Multicast Manager Navigation tree, select **PIM_SM** > **Static RPs**, and select a device.
2. From the Multicast Data Panel toolbar, click **Add Entry with Form**.
3. Enter the following properties:
   - Group Address
   - Group Mask
   - Address
4. Click **Save**.
5. Click **Apply Changes**.

Related Links

PIM SM Static RPs folder on page 273

PIM SM Redundant RPs folder

Redundant rendezvous points (RP) are switches that cover the same multicast groups. The Redundant RPs folder of the PIM SM protocol folder displays all of the multicast groups that are covered by redundant RPs.

The following table describes the parts of the Redundant RPs folder.

Table 90: Parts of the PIM SM Redundant RPs folder

Part	Description
Device name	The system name, host name, or IP address of the device.
Interface Address	The interface address of the device.

Related Links

PIM SM protocol folder on page 268

PIM SM Bootstrap Switches folder

The Bootstrap switches folder of the PIM SM protocol folder displays all configured bootstrap switches, and mismatched switches. To view information about Bootstrap Switches, click a device in the folder.

The following table describes the parts of the Bootstrap switches table.

Table 91: Parts of the PIM SM Bootstrap Switches table

Part	Description
Address	IP address of the current BSR for the local PIM domain.
FragmentTag	A randomly generated number to distinguish the fragments belonging to different Bootstrap messages. Fragments belonging to the same Bootstrap message carry the same fragment tag.
HashMask	Mask used in the hash function to map a group to one of the C-RPs from the RP-Set. The hash-mask allows a small number of consecutive groups to hash always to the same RP.
Priority	Priority of the current BSR. The Candidate-BSR (C-BSR) with the highest BSR priority and address is elected as the BSR for the domain. **Note:** BSR priority is referred as the preferred BSR.
BootStrapTimer	The BSR sends out bootstrap messages when the bootstrap timer expires.

Related Links

PIM SM protocol folder on page 268
Mismatched Switches folder on page 276

Mismatched Switches folder

The Mismatched Switches folder of the PIM SM protocol folder displays all of the multicast groups that are covered by mismatched rendezvous points (RP).

The following table describes the parts of the Mismatched Switches folder.

Table 92: Parts of the PIM SM Mismatched Switches folder

Part	Description
Component	A number uniquely identifying the component. Each protocol instance connected to a separate domain must have a different index value.
GroupAddress	The IP address of the multicast group. If combined with the group mask, the Group address identifies the prefix that the local router uses to advertise itself as a mismatched switch.
GroupMask	The address mask of the multicast group. If combined with the group address, the Group mask identifies the prefix that the local router uses to advertise itself as a mismatched switch.
Address	The address for which the entry contains information.
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).
ExpiryTime	Amount of time, in seconds, remaining before the entry is aged out.

Related Links

PIM SM Bootstrap Switches folder on page 275

MSDP Protocol folder

Multicast Source Discovery Protocol (MSDP) protocol folder contains subfolders for devices that have various MSDP protocol features enabled.

The following table describes the parts of the MSDP protocol folder.

Table 93: Parts of the MSDP Protocol folder

Part	Description
Globals	Displays devices with global options related to the MSDP protocol.

Part	Description
Peers	Displays Rendezvous Point (RP) Peers configuration in the network.
Mesh Group	Displays the Mesh group configuration of the peers in the network.
Cache	Displays the Source-Active (SA) cache.

Related Links

Management of Multicast devices on page 236
MSDP Globals folder on page 277
MSDP Peers folder on page 277
MSDP Mesh Group on page 280
MSDP Cache on page 281

MSDP Globals folder

The Globals table of the MSDP protocol folder displays devices that have MSDP globally enabled.

The following table describes the parts of the Globals table.

Table 94: Parts of the MSDP Globals folder

Part	Description
Devices	The IP address, system name, or host name of the device.
Enabled	Activates MSDP.
ImplicitDefaultPeerEnabled	Accepts all Source-Active messages from the default peer if reverse path forwarding peer rule checks fail.
RPAddress	Specifies the IP address to use as the originator ID. If the address is not a system local address, the system rejects the configuration.

Related Links

MSDP Protocol folder on page 276

MSDP Peers folder

The following table describes the parts of the MSDP Peers table for a device.

Table 95: Parts of the MSDP Peers folder

Part	Description
RemoteAddress	Specifies the IP address of the router that is the MSDP peer.
ConnectRetryInterval	Time interval, in seconds, for the [ConnectRetry-period] for the MSDP peer. The range is from 1–65535 seconds. The default is 30 seconds.
LocalAddress	If configured, this IP address is the source IP address to initiate the MSDP connection. If the local address you configure is not a system local address, the system rejects the configuration. If you do not configure a local address, the IP address of the interface found in the route to reach the peer becomes the default source IP address for the TCP connection.
EncapsulationType	Specifies the type of encapsulation to use when the system encapsulates data in Source-Active messages to this peer.
FsmEstablishedTime	This timestamp is set to the value of sysUpTime when a peer transitions into or out of the established state. The timestamp is set to zero when the MSDP speaker is booted. The syntax is in TimeStamp.
InMessageTime	Specifies the sysUpTime value when the last MSDP message was received from the peer. It is set to zero when the MSDP speaker is booted.
RemotePort	Specifies the remote port for the TCP connection between the MSDP peers. The range is from 0–65535. The default is 639.
LocalPort	Specifies the local port for the TCP connection between the MSDP peers. The range is from 0–65535. The default is 639.
ConnectionAttempts	Specifies the number of times the state machine transitions from inactive to connecting.
DiscontinuityTime	Specifies the value of sysUpTime on the most recent occasion at which one or more of the counters for this entry suffered a discontinuity. View the descriptions of each object to see if it is expected to have discontinuities. These discontinuities may occur at peer connection establishment. If no such discontinuities have occurred since the last reinitialization of the local management subsystem, then this object contains a zero value.
RPFFailures	Specifies the number of Source Active messages received from this peer that failed the Peer-RPF check. Discontinuities in the value of this counter can occur at re-initialization of the management system,

Part	Description
	and at other times as indicated by the value of DiscontinuityTime
DataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, and indicates that the router advertises all SA messages.
HoldTimeConfigured	Specifies the interval, in seconds, at which the MSDP peer waits for keepalive messages from other peers before it declares them down. The range is from 0–65535 seconds. The default is 75 seconds. A value of 0 indicates the MSDP connection is never torn down due to absence of messages from peer.
InDataPackets	Displays the number of MSDP-encapsulated data packets received.
OutDataPackets	Specifies the total number of encapsulated data packets sent to this peer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of DiscontinuityTime.
KeepAliveConfigured	Specifies the interval, in seconds, at which the MSDP peer sends keepalive messages. The range is from 0–21845 seconds. The default is 60 seconds. A value of 0 indicates the router does not send keepalive messages after the peers establish the MSDP session. If you assign a value of 0, Avaya recommends that you configure PeerHoldTimeConfigured on the other side of the peer relationship as 0.

Related Links

MSDP Protocol folder on page 276
Adding a device to the MSDP Peers folder on page 279

Adding a device to the MSDP Peers folder

Perform the following procedure to add a device to the MSDP Peers folder.

Procedure

1. From the Multicast Manager Navigation tree, select **MSDP** > **Peers**.
2. From the Multicast Manager toolbar, click **Add Devices**.
3. From the Add Devices list, choose one device, or more than one device.
4. Click **Save**.

Related Links

MSDP Peers folder on page 277

MSDP Mesh Group

The Mesh Group table of the MSDP protocol folder displays the following:

- devices that have Mesh Groups configured in a Multicast network.
- an MSDP peer that establishes a peering relationship between the local MSDP-enabled router and a peer in another domain.

The following table describes the parts of the Mesh Group table.

Table 96: Parts of the MSDP Mesh Group table

Part	Description
RemoteAddress	Specifies the IP address of the router that is the MSDP peer.
ConnectRetryInterval	Specifies the interval, in seconds, at which the MSDP peer retries the connection after the previous connection establishment to the peer fails. The range is from 1–65535 seconds. The default is 30 seconds.
LocalAddress	If configured, this IP address is the source IP address to initiate the MSDP connection. If the local address you configure is not a system local address, the system rejects the configuration. If you do not configure a local address, the IP address of the interface found in the route to reach the peer becomes the default source IP address for the TCP connection.
EncapsulationType	Specifies the type of encapsulation to use when the system encapsulates data in Source-Active messages to this peer.
PeerDataTtl	Specifies the time-to-live value, from 0–255. The default value is 0, and indicates that the router advertises all SA messages.
PeerHoldTimeConfigured	Specifies the interval, in seconds, at which the MSDP peer waits for keepalive messages from other peers before it declares them down. The range is from 0–65535 seconds. The default is 75 seconds. A value of 0 indicates the MSDP connection is never torn down due to absence of messages from peer.
PeerKeepAliveConfigured	Specifies the interval, in seconds, at which the MSDP peer sends keepalive messages. The range is from 0–21845 seconds. The default is 60 seconds. A value of 0 indicates the router does not send keepalive messages after the peers establish the MSDP session. If you assign a value of 0, Avaya recommends that you configure

Part	Description
	PeerHoldTimeConfigured on the other side of the peer relationship as 0.

Related Links

MSDP Protocol folder on page 276
Adding a device to the MSDP Mesh Group on page 281

Adding a device to the MSDP Mesh Group

Perform the following procedure to add a device to the MSDP Mesh Group.

Procedure

1. From the Multicast Manager Navigation tree, select **MSDP** > **Mesh Group**.
2. From the Multicast Manager toolbar, click **Add Devices**.
3. From the Add Devices list, choose one device, or more than one device.
4. Click **Save**.

Related Links

MSDP Mesh Group on page 280

MSDP Cache

The Cache table of the MSDP protocol folder displays devices that have Cache entries.

The following table describes the parts of the Cache table.

Table 97: Parts of the MSDP Cache table

Part	Description
PeerLearnedFrom	Displays the peer from which the system last accepted this SA cache entry. The address must correspond to a RemoteAddress value in the peer table. The value is 0.0.0.0 on the router that originates the entry.
RPFPeer	Displays the peer from which the system accepts an SA message. This address must correspond to a RemoteAddress value in the peer table, or it can be 0.0.0.0 if no RPF peer exists.
InSAs	Displays the number of SA messages received.
InDataPackets	Displays the number of MSDP-encapsulated data packets received.
UpTime	Displays the time after the entry first appeared in the SA cache.

Part	Description
ExpiryTime	Displays the time before this entry expires from the SA cache.

Related Links

MSDP Protocol folder on page 276

Multicast Route protocol folder

The Multicast Route protocol folder contains subfolders for devices that have various Multicast Route protocol features enabled.

The following table describes the parts of the Multicast Route protocol folder.

Table 98: Parts of the Multicast Route protocol folder

Part	Description
PIM DVMRP Gateway folder	Displays devices that are configured as gateways between PIM and DVMRP domains.
Timed Prune folder	Displays forwarding entries that are not pruned until a configurable timer expires.
Routes folder	Displays protocol-independent multicast route and next hop information.
MRoute RPM Trees folder	Displays the reverse path multicast tree for all active sources.

Related Links

Management of Multicast devices on page 236
Multicast Route PIM DVMRP Gateway folder on page 282
Multicast Route Timed Prune folder on page 283
Multicast Route Routes Folder on page 284
Multicast Route MRoute RPM Trees folder on page 287

Multicast Route PIM DVMRP Gateway folder

The PIM-DVMRP Gateway folder of the Multicast Route protocol folder displays the devices that are configured as gateways between PIM and DVMRP domains.

The following table describes the parts of the PIM-DVMRP Gateway folder.

Table 99: Parts of the Multicast Route PIM DVMRP Gateway folder

Part	Description
Interface	The slot and port number or VLAN ID for which this entry contains information.
TTL	The datagram time to live (TTL) threshold for the interface. Any IP multicast datagrams with a TTL less than this threshold is not forwarded out the interface. The default value of 1 indicates that all multicast packets are forwarded out the interface.
Protocol	The routing protocol running on this interface.

Related Links

Multicast Route protocol folder on page 282

Multicast Route Timed Prune folder

The Timed Prune folder of the Multicast Route protocol folder displays forwarding entries that would not be pruned until a configurable timer expires.

The following table describes the parts of the Timed Prune folder.

Table 100: Parts of the Multicast Route Timed Prune folder

Part	Description
Group address	Indicates the IP Multicast Group Address associated with the IP multicast stream.
Source address	The Source Subnet IP address of the sender of the IP multicast stream.
Source subnet mask	The Source Subnet Mask IP address of the sender of the IP multicast stream.

Related Links

Multicast Route protocol folder on page 282
Adding a device to Multicast Route Timed Prune folder on page 283
Inserting a device into the Multicast Route Time Prune list on page 284

Adding a device to Multicast Route Timed Prune folder

Perform the following procedure to add a device to Multicast Route Timed Prune folder.

Procedure

1. From the Multicast Manager Navigation tree, select **Multicast Route** > **Timed Prune**.
2. From the Multicast Manager toolbar, click **Add Devices**.
3. From the Add Devices list, choose one device, or more than one device.

4. Click **Save**.

Related Links

Multicast Route Timed Prune folder on page 283

Inserting a device into the Multicast Route Time Prune list

Perform the following procedure to insert a device into the Multicast Route Time Prune list.

Procedure

1. From the Multicast Manager Navigation tree, select **Multicast Route** > **Time Prune**, and select a device.
2. From the Multicast Data Panel toolbar, click **Add Entry with Form**.
3. Enter the following properties:
   - Group Address
   - Group Mask
   - Address
4. Click **Save**.
5. Click **Apply Changes**.

Related Links

Multicast Route Timed Prune folder on page 283

Multicast Route Routes Folder

The Routes folder of the Multicast Route protocol folder displays protocol-independent multicast route and next hop information.

The following table describes the parts of the Routes folder.

Table 101: Part of the Multicast Route Routes folder

Part	Description
Routes tab	Displays multicast route information.
Next Hops tab	Displays multicast next hop information.
Interfaces tab	Displays interface information.

Related Links

Multicast Route protocol folder on page 282
Routes tab on page 285
Next Hops tab on page 285
Interfaces tab on page 286

Routes tab

The Routes tab of the Routes folder displays multicast route information.

The following table describes the parts of the Routes tab.

Table 102: Parts of the Multicast Route Routes folder Routes tab

Parts	Description
Group	The IP multicast group address for which the entry contains multicast routing information.
Source	The network address which, if combined with the corresponding route SourceMask value, identifies the sources for which the entry contains multicast routing information.
Source mask	The network mask which, if combined with the corresponding route Source value, identifies the sources for which this entry contains multicast routing information.
Interface	The slot and port number or VLAN ID on which IP datagrams sent by these sources to this multicast address are received.
Upstream neighbor	The address of the upstream neighbor, for example RPF neighbor, from which IP datagrams from these sources to this multicast address are received; or, 0.0.0.0 if the network is local.
Protocol	The routing protocol through which the route was learned.

Related Links

Multicast Route Routes Folder on page 284

Next Hops tab

The Next Hops tab of the Routes folder displays multicast next hop information.

The following table describes the parts of the Next hops tab.

Table 103: Parts of the Multicast Route Routes folder Next Hops tab

Part	Description
Group	The IP multicast group for which the entry specifies a next hop on an outgoing interface.
Source	The network address which, if combined with the corresponding next hop SourceMask value, identifies the source for which the entry specifies a next hop on an outgoing interface.
Source mask	The network mask which, if combined with the corresponding next hop Source value, identifies the

Part	Description
	source for which the entry specifies a next hop on an outgoing interface.
Interface	The slot and port number or VLAN ID for the outgoing interface for this next hop.
Address	The IP address of the VLAN for the next hop.
State	Indicates if the outgoing interface and next hop represented by this entry is currently being used to forward IP datagrams. The values are: • forwarding—indicates it is currently being used. • pruned—indicates it is not being used.
Expiry time	The minimum amount of time remaining before the entry ages out. The value 0 indicates that the entry is not subject to aging.
Closest member hops	The minimum number of hops between a router and any member of the IP Multicast group reached through the next hop on the outgoing interface. Any IP Multicast datagrams for the group that has a TTL less than the number of hops are not forwarded to the next hop.
Protocol	The routing protocol through which the next hop was learned.

Related Links

Multicast Route Routes Folder on page 284

Interfaces tab

The following table describes the parts of the Interfaces tab.

Table 104: Parts of the Multicast Route Routes folder Interfaces tab

Part	Description
Interface	The list identifier.
Ttl	The datagram time-to-live (TTL) threshold for the interface. Any IP Multicast datagram with a TTL less than the threshold is not forwarded from the interface. The default value of 1 indicates that all multicast packets are forwarded.
Protocol	The routing protocol running on the interface. Applies to DVMRP only.

Related Links

Multicast Route Routes Folder on page 284

Multicast Route MRoute RPM Trees folder

The MRoute RPM Trees folder of the Multicast Route protocol folder displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to a router.

The following table describes the parts of the MRoute RPM Trees folder.

Table 105: Multicast Route MRoute RPM Trees folder

Parts	Description
Device	The system name or IP address of the device.
Interface	The DVMRP interface, slot and port number, or VLAN ID on which IP datagrams sent by these sources to the multicast address are received. A value of 0 indicates that datagrams are not subject to an incoming interface check, but may be accepted on multiple interfaces.
Upstream neighbor address	The address of the upstream neighbor from which IP datagrams from these sources to the multicast address are received; or, 0.0.0.0 if the upstream neighbor is unknown.
Protocol	The routing mechanism through which this route was learned.

Related Links

Multicast Route protocol folder on page 282

Policy folder

The Policy folder provides access to prefix lists and policy routes for a switch.

Prefix lists are the base item in a routing policy, and contain lists of IP addresses with their associated masks that support the comparison of ranges of masks.

You can create Policy routes and apply the Policy routes in an accept (in), announce (out), or redistribution capacity.

The policy folder contains an empty Device List folder. After you add devices to the Device List, you can configure prefix lists and policy routes for the device.

The following sections provide the steps for the following procedures:

- Adding a device to the Device List
- Adding a Prefix
- Adding a policy route

- Deleting a device, prefix, or policy route

For a list of the parameters supported through the Policy folder, see Prefix List on page 288, and Policy Route table on page 288.

Related Links

Management of Multicast devices on page 236
Prefix List on page 288
Policy Route table on page 288
Adding a device to the policy folder on page 292
Deleting a device from the Policy folder on page 292
Adding a Prefix on page 293
Deleting a prefix on page 293
Adding a policy route on page 293
Deleting a route policy on page 294

Prefix List

The following table describes the parts of the Policy folder Prefix list.

Table 106: Parts of the Prefix List

Part	Details
Id	The list identifier.
Prefix	The IP address.
PrefixMaskLen	Specified length of the prefix mask. You must enter the full 32-bit mask in order to exact a full match of a specific IP address.
Name	Use to name a specified prefix list during the creation process or to rename the specified prefix list. The name length can be from 1 to 64 characters.
MaskLenFrom	Lower bound of the mask length. The default is the mask length.
MaskLenUpTo	Upper bound of the mask length. The default is the mask length.

Related Links

Policy folder on page 287

Policy Route table

The following table describes the parts of the Policy Route table.

Table 107: Parts of the Policy Route table

Part	Details
Id	The ID of an entry in the Prefix List table.
SequenceNumber	A second index that identifies a specific policy within a route policy group.
Name	Use during the creation process, or to rename a policy after you create the policy. This command changes the name field for all sequence numbers under the given policy.
Enable	Indicates whether the policy sequence number is enabled or disabled. If the policy sequence number is disabled the policy sequence number is ignored.
Mode	Specifies the action to take if a policy is selected for a specific route. Select **permit** to allow the route, or **deny** to ignore the route.
MatchProtocol	Selects the appropriate protocol. If configured, MatchProtocol matches the protocol through which the route is learned. This field is used only for RIP announce purposes.
MatchAsPath	Matches the BGP autonomous system path. This overrides the BGP neighbor filter list information. Applies to the BGP protocol only.
MatchCommunity	Filters incoming and outgoing updates based on a community list. Applies to the BGP protocol only.
MatchCommunityExact	If enabled, indicates the match must be exact; that is, all of the communities specified in the path must match. The default is disable. Applies to the BGP protocol only.
MatchNetwork	If configured, the switch matches the destination network against the contents of the specified prefix list.
MatchIpRouteSource	If configured, matches the next hop IP address for RIP routes and advertising router IDs for OSPF routes against the contents of the specified prefix list. This option is ignored for all other route types.
MatchNext Hop	If configured, matches the next hop IP address of the route against the contents of the specified prefix list. This field applies to nonlocal routes only.
MatchInterface	If configured, the switch matches the IP address of the interface by which the RIP route is learned against the contents of the specified prefix list. This field is used only for RIP routes and is ignored for all other types of routes.
MatchRouteType	Sets a specific route-type to be matched. Externaltype1, and Externaltype2 specify the OSPF

Part	Details
	routes of the specified type only. OSPF internal refers to intra and inter area routes. Applies to OSPF routes only.
MatchMetric	If configured, the switch matches the metric of the incoming advertisement or existing route against the specified value from 1to 65535. If 0, then this field is ignored. The default is 0.
MatchTag	Specifies a list of tags used during the match criteria process. It contains one or more tag values. Applies to the BGP protocol only.
SetRoutePreference	Sets the preference greater than zero to specify the route preference value to be assigned to the routes that matches the policy. The values are from 0 to 255. Applies to Accept policies only.
SetAsPath	Indicates the AS path value to use whether the SetAsPathMode field is Tag or Prepend. Applies to the BGP protocol only.
SetAsPathMode	The mode is either Tag or Prepend tag, and is applicable only while redistributing routes to BGP. the mode converts the tag of a route into AS path. Applies to the BGP protocol only.
SetAutomaticTag	The default is disable. Applies to the BGP protocol only.
Set CommunityNumber	A number from 1 to 42949672000, or a value of no-export or no-advertise. Applies to BGP advertisements only.
Set CommunityMode	The values are: • Append—Adds the community number specified in SetCommunityNumber to the community list attribute. • None—Removes the community in the route path additive. • Unchanged—Keeps the community attribute in the route path as it is. The default value is Unchanged. Applies to the BGP protocol only.
SetMetricTypeInternal	Sets the MED value for routes advertised to BGP numbers to the Interior Gateway Protocol (IGP) metric value. The default is 0.
SetMetric	If configured, the switch sets the metric value for the route while announcing or redistributing. The default-import-metric is 0. If the default is configured, the original cost of the route is advertised into OSPF; for

Part	Details
	RIP, the original cost of the route or the default value is used.
SetMetricType	If configured, sets the metric type for the routes to be announced into the OSPF routing protocol that matches the policy. The default is type 2. Applies to OSPF announce policies only.
SetNextHop	The IP address of the next hop router. SetNextHop is ignored for Distance Vector Multicast Routing Protocol (DVMRP) routes. The default is 0.0.0.0. Applies to the BGP protocol only.
SetOrigin	The values are: • IGP • EGP • incomplete • unchanged If you do not configure SetOrigin, the system uses the route origin from the Ip routing table (protocol). The default is unchanged. Applies to the BGP protocol only.
SetLocalPref	Use during the route decision process in the BGP protocol. The default is 0. Applies to the BGP protocol only.
SetOriginEgpAs	Indicates the remote autonomous systems number. The default is 0. Applies to the BGP protocol only.
SetTag	The range is from 0 to 65535. The default is 0. Applies to the BGP protocol only.
SetWeight	The weight value for the routing table that you must use with match as-path condition. The value overrides the weight configured through the NetworkTableEntry, FilterListWeight, or NeighborWeight. The default is 0. Applies to the BGP protocol only.
SetInjectNetList	If configured, the switch replaces the destination network of the route that matches the policy with the contents of the specified prefix list.
SetMask	If configured, the switch sets the mask of the route that matches the policy. Applies only to RIP accept policies.
NssaPbit	Sets or resets the P-bit in the specified type 7 link state advertisement (LSA). By default, the P-bit is always set because you may set it to a disable state for a particular route policy other than all (type 7). LSAs associated with the route policy have the P-bit

Part	Details
	cleared. With this intact the not so stubby area (NSSA) area border router (ABR) does not perform a translation of the LSAs to type 5. The default is disable.

Related Links

Policy folder on page 287

Adding a device to the policy folder

Perform the following procedure to add a device to the policy folder. You can add more than one device to the policy folder.

Procedure

1. From the Multicast Manager navigation pane, open the **Policy** folder.
2. Click **Device List**.
3. From the Multicast Manager tool bar, click the plus (+) sign.

   The Device List Insert dialog box appears that lists the devices discovered by Multicast Manager.
4. Perform one of the following actions.
   - Select one device, or more than one device, from the list of devices and click **Save**.
   - To add a contiguous block of devices, hold down the Shift key, click on the first device in the list, click on the last device, release the Shift key, and click **Save**.

Related Links

Policy folder on page 287

Deleting a device from the Policy folder

Perform the following procedure to delete a device from the Policy folder.

Procedure

1. From the Multicast Manager navigation pane, open the **Policy** folder.
2. Open the **Device List**.
3. Select the device.
4. From the Multicast Manager tool bar, select **Remove Device**.

Related Links

Policy folder on page 287

Adding a Prefix

Perform the following procedure to add a prefix.

Procedure

1. From the Multicast Manager navigation pane, open the **Policy** folder.
2. Open the **Device List**.
3. Select the device.
4. If the Prefix List tab is not open, click the **Prefix List** tab.
5. From the Prefix List tool bar, select **Add Entry with Form**.

   An Insert dialog box appears with a data entry field for each prefix list parameter.
6. Perform one of the following actions.
   - To continue, enter the value for each parameter in the respective field, and then click **Save**.
   - To exit without adding a prefix, click **Cancel**.

Related Links

Policy folder on page 287

Deleting a prefix

Perform the following procedure to delete a prefix from the policy prefix list.

Procedure

1. From the Multicast Manager navigation pane, open the **Policy** folder.
2. Open the **Device List**.
3. Select the device.
4. Select the **Prefix List** tab.
5. Click the row that represents the prefix to delete.
6. From the Prefix List tool bar, select **Delete Entry**.

Related Links

Policy folder on page 287

Adding a policy route

Perform the following procedure to add a policy route.

Procedure

1. From the Multicast Manager navigation pane, open the **Policy** folder.
2. Open the **Device List**.
3. Select the device.
4. If the Route Policy tab is not open, click the **Route Policy** tab.
5. From the Route Policy tool bar, select **Add Entry with Form**.

   An Insert dialog box appears with a data entry field for each policy route parameter.
6. Perform one of the following actions.
   - To continue, enter the value for each parameter in the respective field, and then click **Save**.
   - To exit without adding a policy route, click **Cancel**.

Related Links

Policy folder on page 287

Deleting a route policy

Perform the following procedure to delete a route policy from the policy folder.

Procedure

1. From the Multicast Manager navigation pane, open the **Policy** folder.
2. Open the **Device List**.
3. Select the device.
4. Select the **Route Policy** tab.
5. Click the row that represents the route policy to delete.
6. From the Route Policy tool bar, select **Delete Entry**.

Related Links

Policy folder on page 287

Highlight multicast data in the topology map

You can highlight the following information in the topology:

- Multicast device
- Multicast forwarding tree

Related Links

Management of Multicast devices on page 236
Highlighting a multicast device in the topology map on page 295
Highlighting a multicast forwarding tree on page 295
Highlighting a multicast forwarding tree using multicast protocol features on page 296

Highlighting a multicast device in the topology map

Perform the following procedure to highlight a multicast device in the topology map.

Procedure

1. In the Multicast Manager navigation pane, perform one of the following actions.
   - Select a subfolder under a protocol folder.
   - Select a single device.

   Devices supported by the protocol are highlighted.
2. From Multicast Manager menu bar, select **View** > **Highlight Topology**.

   The Highlight Topology option remains selected until you deselect it.
3. Return to the COM Topology tab window.
   - If you select a subfolder under a protocol folder, all devices that support the feature are highlighted.
   - If you select a single device, the device is highlighted.

Related Links

Highlight multicast data in the topology map on page 294

Highlighting a multicast forwarding tree

Perform the following procedure to highlight a multicast tree rooted at a source subnet within a multicast group.

Procedure

1. In the Multicast Manager navigation pane, select a tree icon in the Dvmrp RPB Trees folder or the MRoute RPM Trees folder.
2. From Multicast Manager menu bar, select **View** > **Highlight Topology**.
3. Return to the COM topology map.

   The devices and forwarding paths are highlighted.

Related Links

Highlight multicast data in the topology map on page 294

Highlighting a multicast forwarding tree using multicast protocol features

You can select a multicast protocol feature in the Multicast Manager and view, on the COM topology map, the devices that are actively using the multicast protocol feature.

Perform the following procedure to view devices using multicast protocol features.

Procedure

1. In the Multicast Manager navigation pane, select a multicast protocol feature icon from the folders and subfolders of the navigation tree.
2. Return to the COM topology window tab.

   The devices using DVMRP are highlighted.

Related Links

Highlight multicast data in the topology map on page 294

Chapter 12: Virtual Services Network Manager

The Virtual Services Network (VSN) Manager enabled you to view and to configure SPBm (Shortest Path Bridging Mac-in-Mac) based L2 and L3 Virtual Services Networks (VSNs), as well as IP-shortcut based VSNs. With VSN Manager, you can view and configure these features on multiple devices that have SPBm enabled. L2 VSNs can be based on C-Vlans, Swicthed UNI Vlans or based on Transparent UNI (T-UNI). You can configure Multicast-over-SPBm for L2, L3, and IP-shotcuts based VSNs.

The VSN Manager provides the following views:

- VSN centric view
- Device centric view

Before VSN Manager can be used, you must install a feature license for the VSN feature.

Note:

Switched UNI Vlans can be configured for VSP 7000 v10.2 and above and ERS 4800 v5.7 and above devices only.

Note:

VSP 8000 does not support L3 VSN and BGP VPNs.

The following table outlines the supported devices for the VSN Manager:

Supported device for VSN Manager	Features supported
ERS 4800 v5.7	L2 VSN
ERS 8600/8800 v7.1 and v7.1.3	L2 VSN L3 VSN BGP-VPN VRF table CLIP CFM
ERS 8600/8800 v7.2 and above	L2 VSN L2 MoSPBm L3 VSN

Supported device for VSN Manager	Features supported
	L3 MoSPBm GRT–IP Shortcuts BGP-VPN VRF table Multicast Route Table SPBm Multicast Tree CLIP CFM Globals
VSP 4000 v3.0.1	L2 VSN L3 VSN BGP-VPN VRF table CLIP CFM Globals
VSP 4000 v3.1 and above	L2 VSN L2 MoSPBm L3 VSN L3 MoSPBm GRT–IP Shortcuts BGP-VPN VRF table Multicast Route Table SPBm Multicast Tree CLIP CFM Globals
VSP 7000 v10.1, v10.2, v10.3, and v10.3.1 [1]	L2 VSN
VSP 8000 v4.0	L2 VSN
VSP 9000 v3.2 and v3.3	L2 VSN L3 VSN BGP-VPN VRF table CLIP
VSP 9000 v3.4, and v4.0	L2 VSN L2 MoSPBm

Supported device for VSN Manager	Features supported
	L3 VSN L3 MoSPBm BGP-VPN GRT–IP Shortcuts VRF table Multicast Route Table SPBm Multicast Tree CLIP CFM Globals

1 — SPB Infrastructure and L2 SPB Service support only

VSN license

Avaya Configuration and Orchestration Manager (COM) 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**.

   COM perfoms a discovery. After the discovery is complete, the Operation Result dialog box displays.
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.

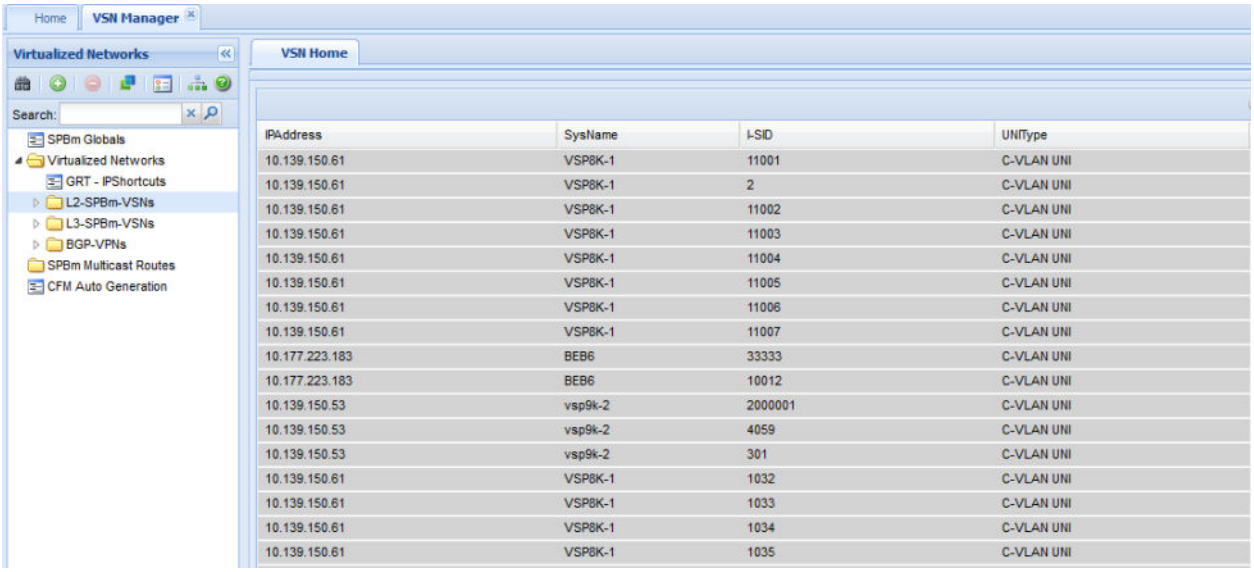
VSN-centric view

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. In addition to the VSN data, the VSN-centric view contains the following :

- SPBm Globals (Global SPBm configuration data)
- SPBm Multicast Route tables
- CFM Global configuration

Various VSN-centric features are described in detail in subsequent sections of the document.

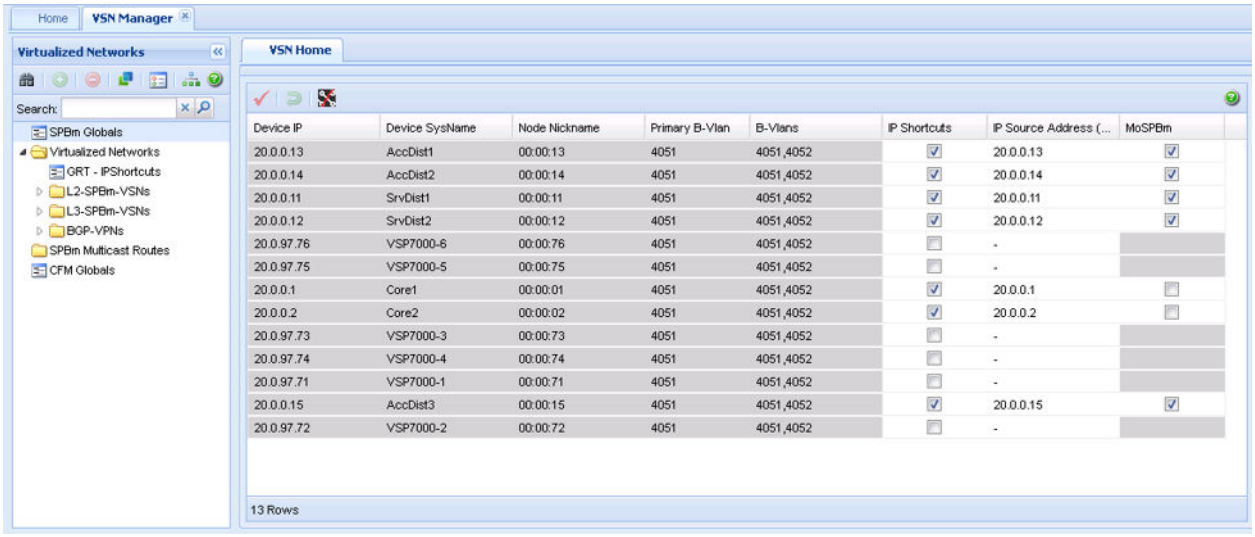
The following figure shows the VSN-centric view.



SPBm Globals

In the SPBm Globals table, you can enable or disable IP-shortcuts and Multicast-over-SPBm globally on the devices that have these capabilities. SPBm Globals table is available in the VSN Centric View.

The following graphic shows the SPBm Globals table.



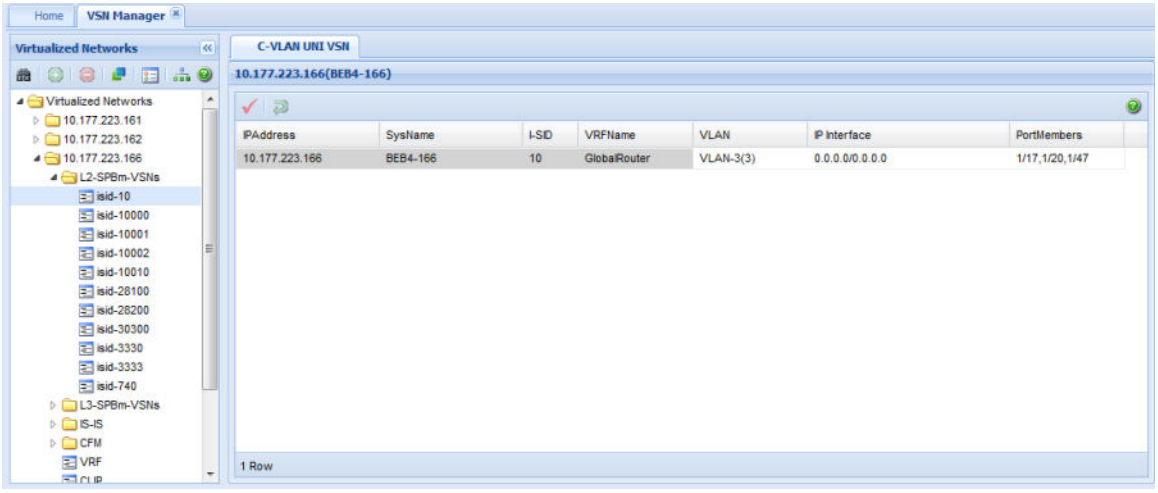
Device centric view

The default view on the VSN Manager is the VSN centric view. To change the view to a device centric view, on the VSN Manager toolbar, click on **Toggle Device/VSN centric view**.

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 VSN 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.

In the device-centric view of the VSN network, the tree is organized by each device in the network. The VSN types display beneath each device permitting you to browse the VSNs by type, to look inside each device, and to browse the VSNs configured in each device.

The following figure shows the device centric view.



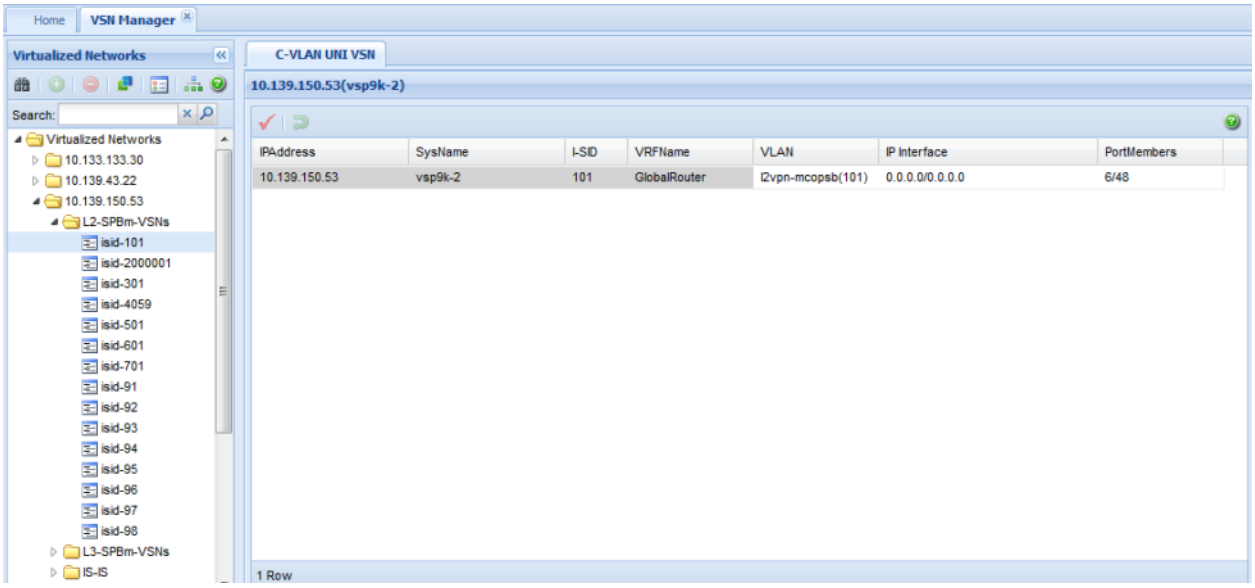
The following sections describe components of the VSN Manager device centric view.

Device node

After you select the required device node from the VSN Manager device centric view, the following device information displays in the contents pane:

- IP Address
- SysName
- I-SID
- VRFName
- VLAN
- IP Interface
- PortMembers

The following figure is an example of the VSN Manager Device centric view.

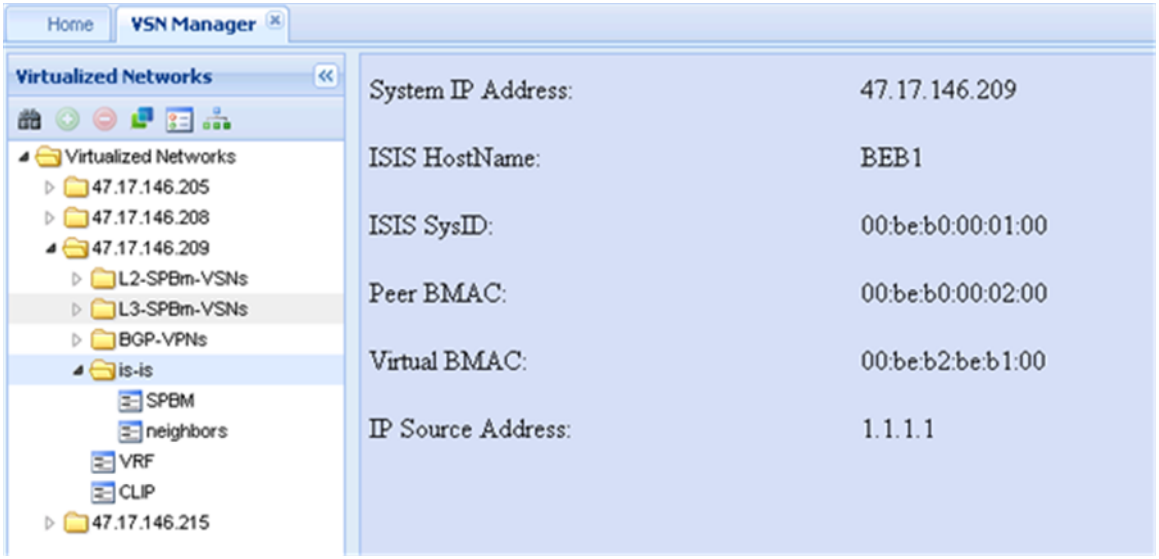


IS-IS

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

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.

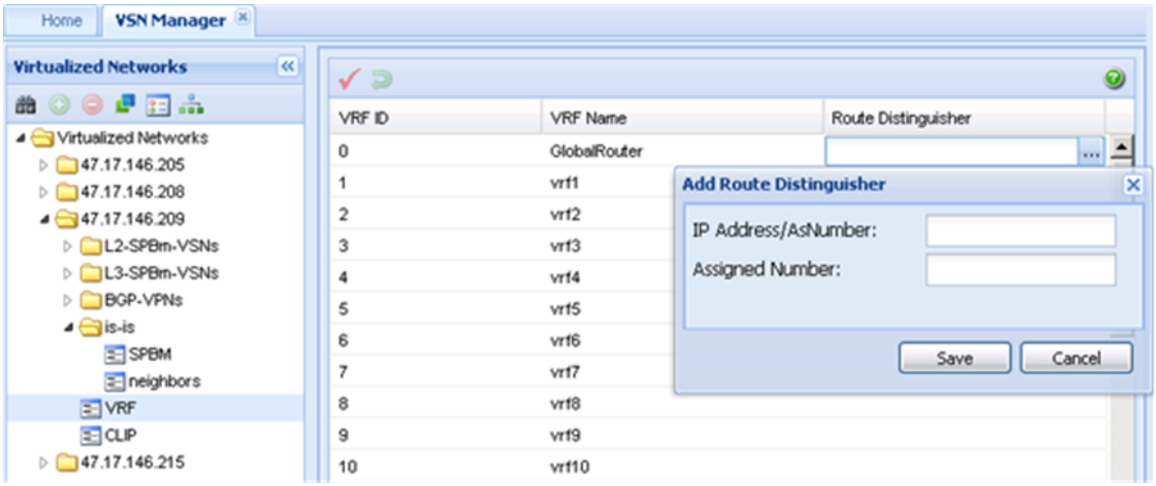
VRF table

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.

Note:

The VRF features is not supported for VSP 7000 v10.2.

The following figure is an example of a VRF table showing the edit box for Route Distinguisher.



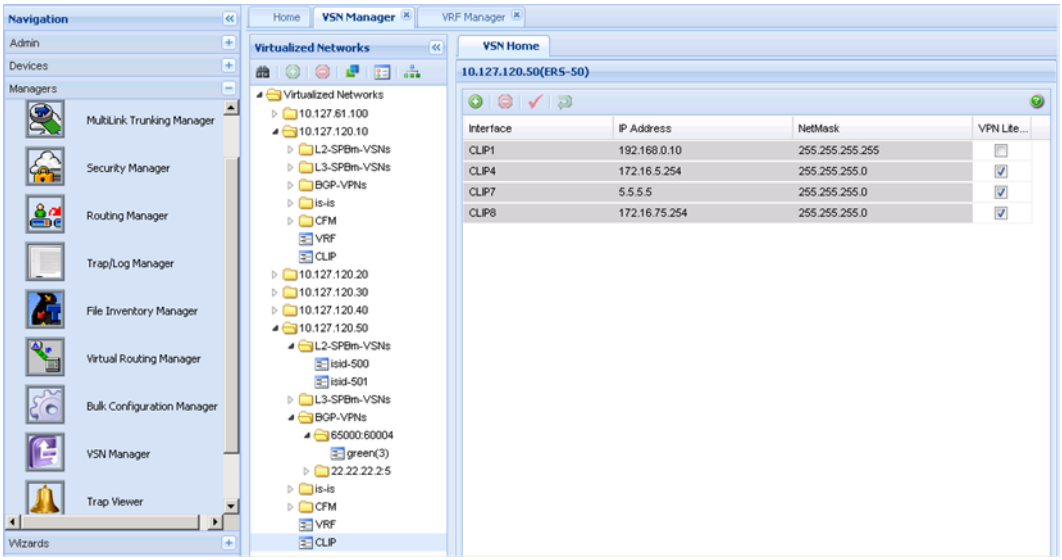
CLIP

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.

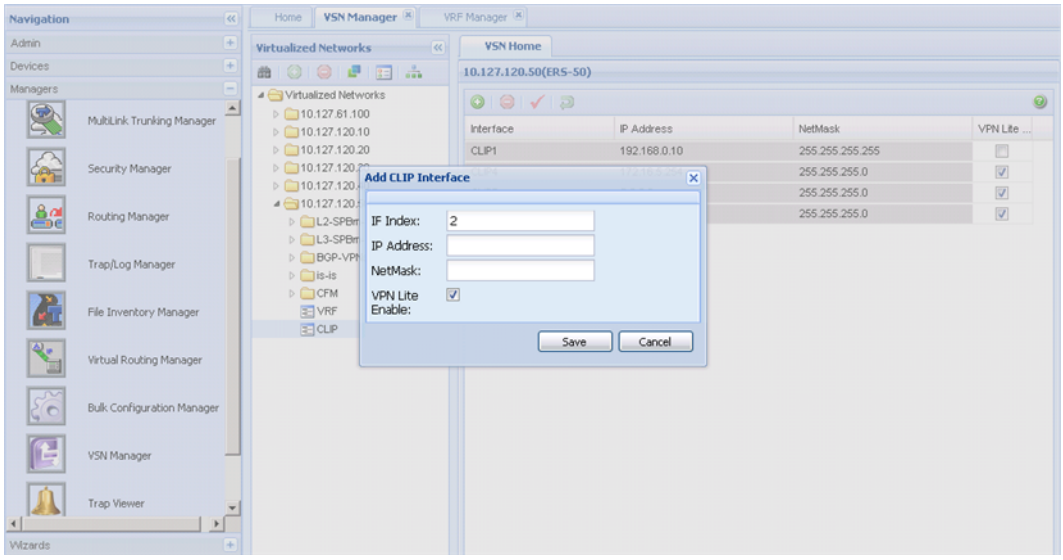
The following figure is an example of the CLIP contents pane.

Note:

The CLIP features is not supported for VSP 7000 v10.2.



The following figure is an example of the CLIP contents pane with the Add CLIP Interface dialog box.



Connectivity Fault Management — Device view

Connectivity Fault Management (CFM) components display for each device.

The read-only view of MDs, MAs and MEPs is supported in COM in the VSN Manager's **device centric view**. 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 Traceroutes 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.

Note:

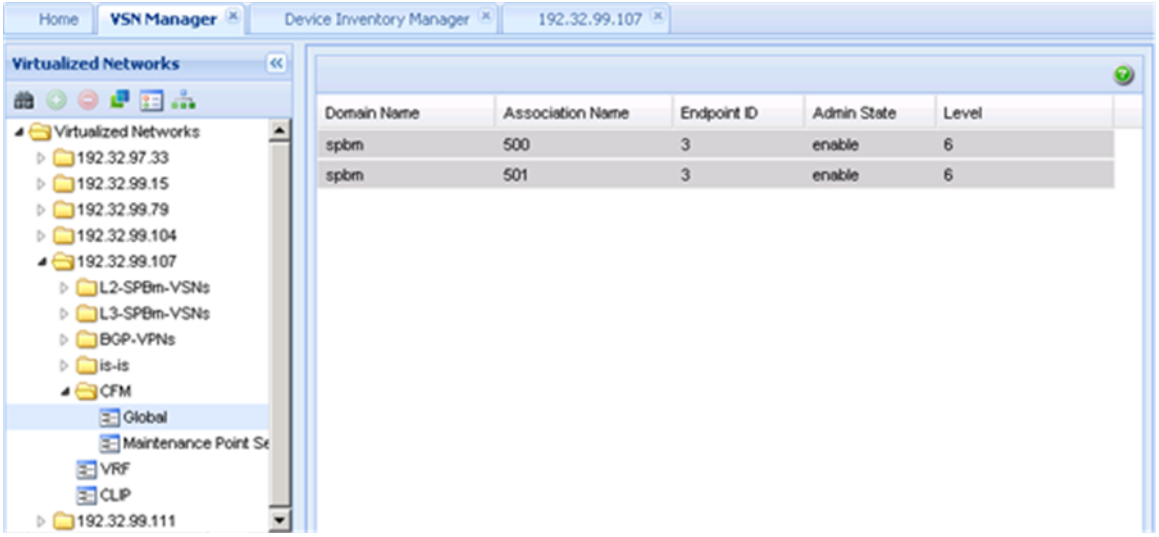
MEP and MIP Nodal is not supported for VSP 7000 v10.2.

The following sections describe the Global node and the Maintenance Point Service node.

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.



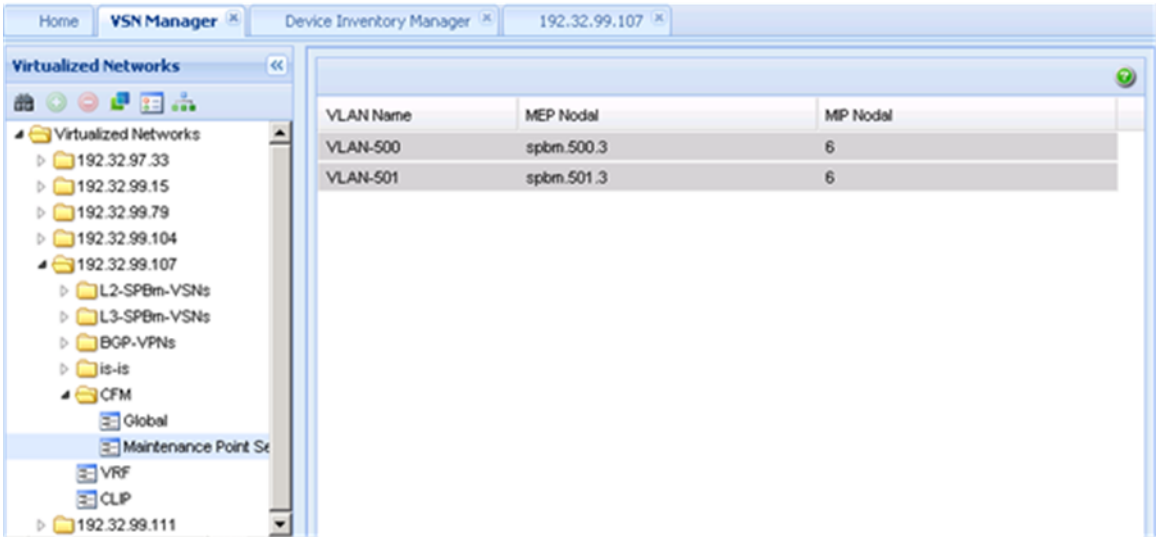
The following table describes the CFM Global table.

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 No support available for VSP 7000 v10.2.	Identifies the VLANs of the device.
MEP Nodal No support available for VSP 7000 v10.2.	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.

Private VLAN overview

Private VLANs are used to provide isolation between ports within a Layer-2 service. A Layer-2 (L2) service is typically realized as a VLAN or a L2VSN. All the access-points in the service can communicate with one another using standard L2 MAC address lookup operations. Broadcast, Multicast, and Unknown Unicast traffic within a L2 service flood to all the access-points within the service.

A Private VLAN behaves differently from a traditional VLAN by providing isolation between some of the ports within the private VLAN. The ports that are members of a private VLAN can be classified into the following three groups:

- Promiscuous Ports: Ports within this group can communicate with all other ports within the private VLAN. These ports can be tagged or untagged ports and can be standalone ports or a member of an MLT.
- Isolated Ports: Isolated ports can communicate with promiscuous ports, but not with any other isolated port. These ports can be tagged or untagged ports and can be standalone ports or a member of an MLT.
- Trunk Ports: Trunk ports are used to carry traffic between other port members within the private VLANs. These ports are always tagged ports and can be standalone ports or a member of an MLT

Each private VLAN instance is associated with two different VLAN_ID values: primary VLAN and secondary VLAN.

The following rules describe how the VLAN_ID values are used:

1. On tagged promiscuous ports – only the primary VLAN is used.
2. On tagged isolated ports – only the secondary VLAN is used.
3. On untagged ports – there is not tag on the packets. Untagged ports are not allowed to be trunk ports.
4. On trunk ports – traffic that originated from isolated ports is tagged with the secondary VLAN_ID.
5. On trunk ports – traffic that originated from a promiscuous port is tagged with the primary VLAN_ID.

There is a combined L2 MAC table for both the primary and secondary VLANs within a private VLAN. MAC addresses from both promiscuous and isolated ports are both learnt into the same table. This means that traffic between an isolated and a promiscuous port can be forwarded in unicast fashion even though one of them is learnt on the primary VLAN_ID and the other is learnt on the secondary VLAN_ID.

The following figure shows a private VLAN on five switches. All the ports connecting the other switches to L2 SWITCH-5 are trunk ports. All other ports are either promiscuous or isolated ports.

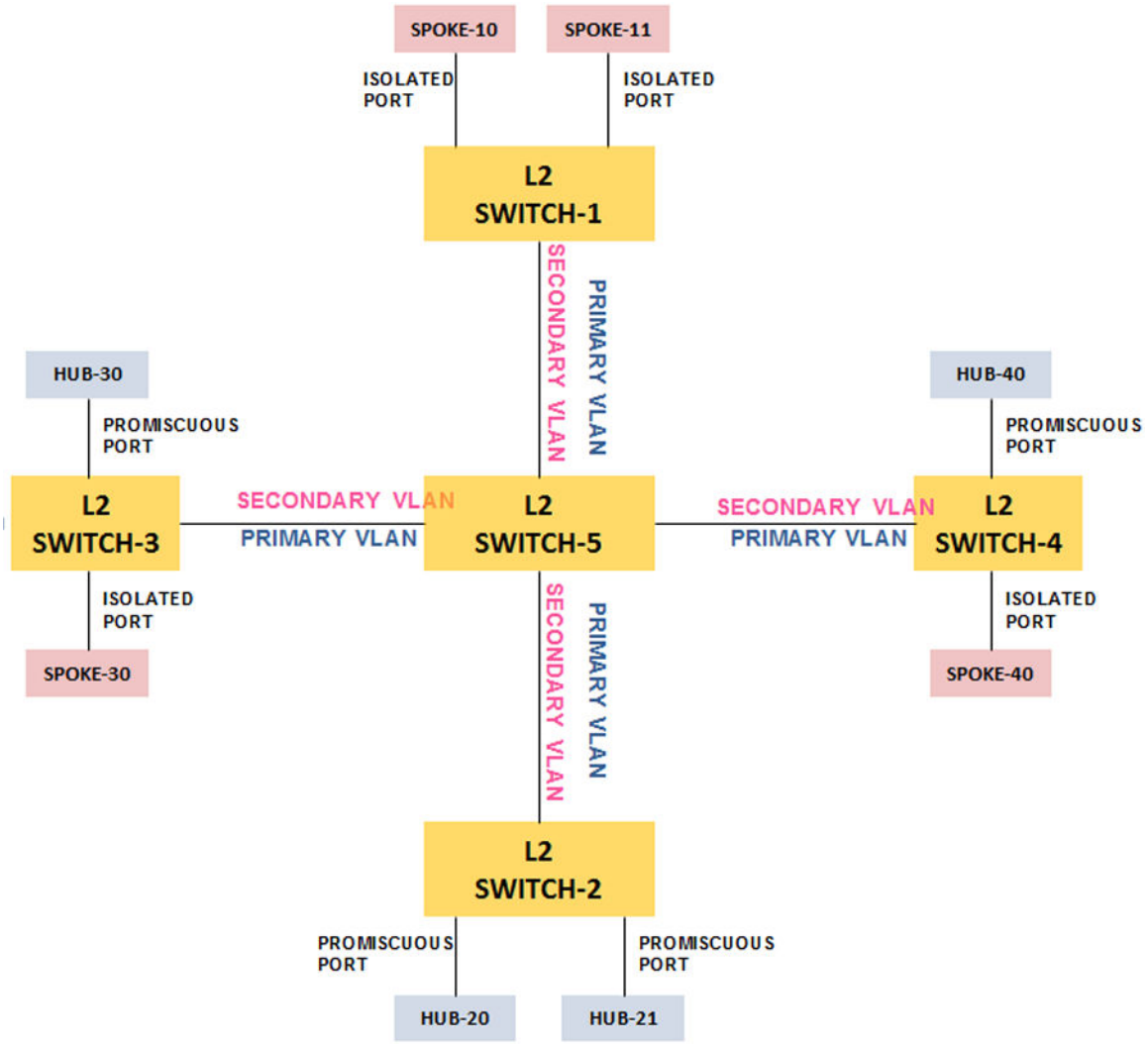


Figure 12: Private VLAN on five switches

Etree overview

An ETREE instance consists of islands of a private VLAN connected by a SPB Core network. Transport within the SPB core network by associating the private VLAN with a pair of I-SID values.

- ETREE: A PRIVATE VLAN whose core transport is done using SPBM.

Note:

This still allows for TRUNK ports to be present in the access networks connecting to an SPBM core.

- HUB: An access-point into the ETREE that is allowed to communicate with all other access-points in the ETREE. It is also used interchangeably with the PROMISCUOUS port definition in the context of ETREE.
- SPOKE: An access-point into the ETREE that is **not** allowed to communicate with any other SPOKE in the ETREE. A SPOKE is only allowed to communicate with HUBs. Used interchangeably with the ISOLATED port definition in the context of ETREE.
- PRIMARY/SECONDARY ISID: The I-SID used to carry traffic from a HUB/ SPOKE inside the SPBM network.

The following figure shows an Etree reference model. The private VLAN is transported across the SPBM cloud.

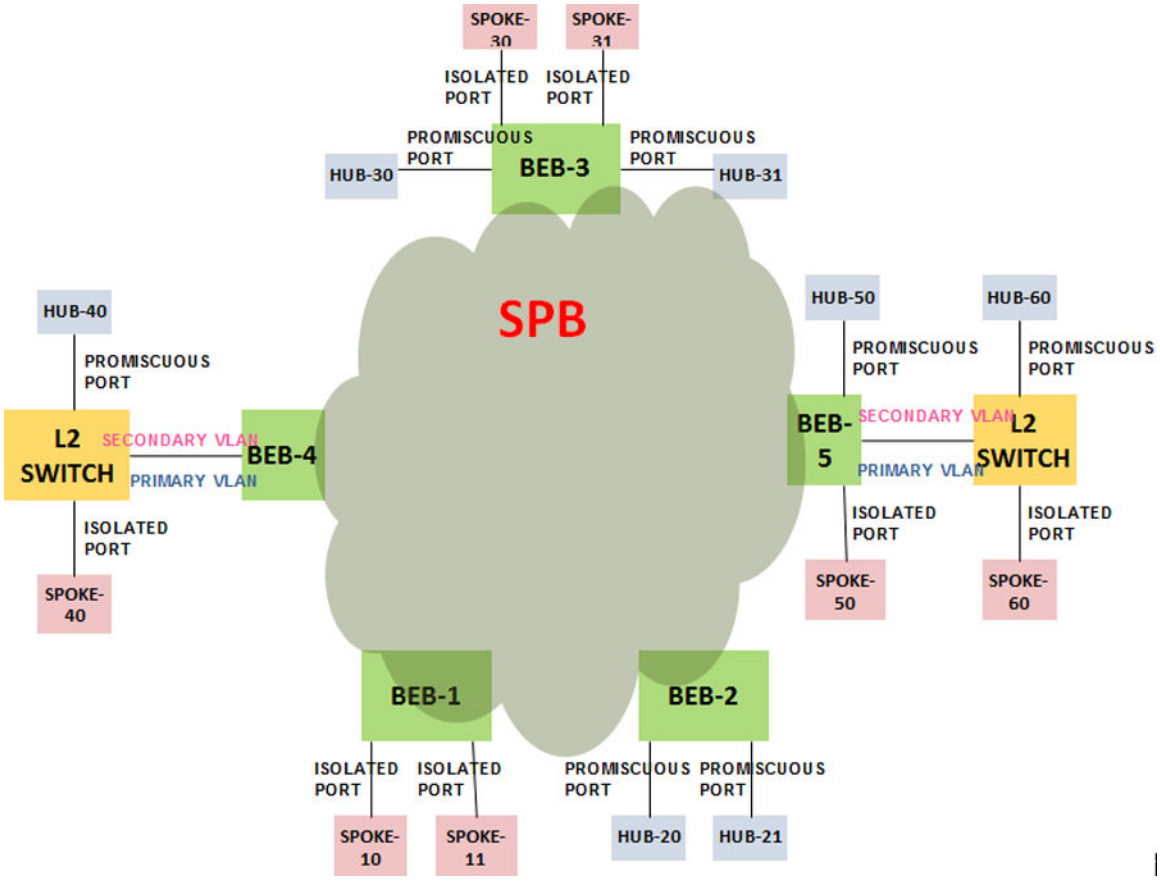
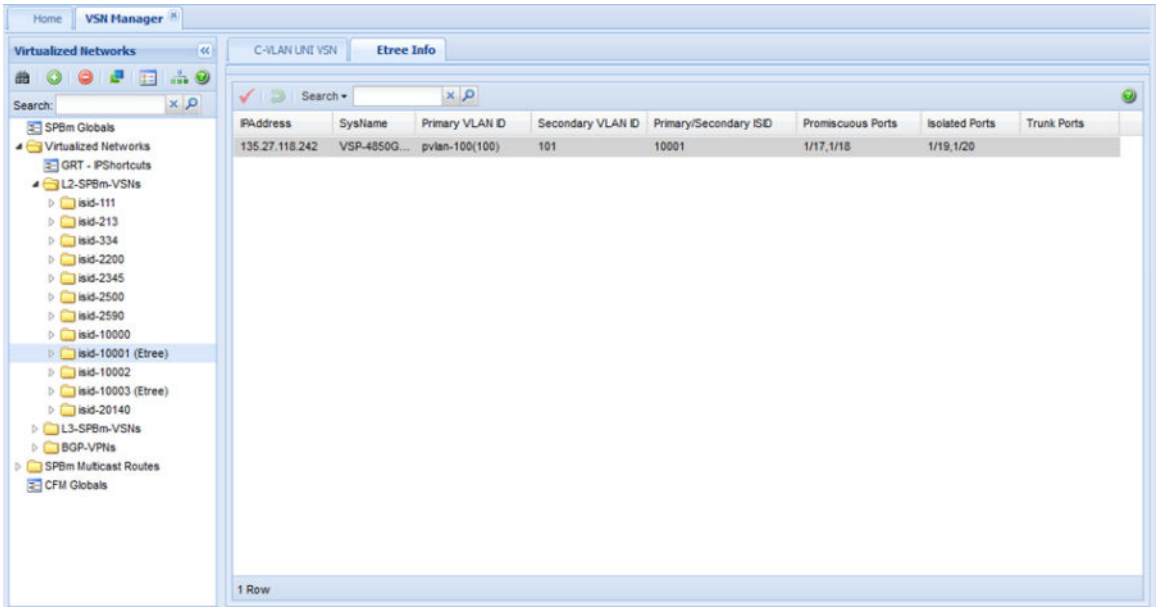


Figure 13: Etree reference model

In COM, an Etree instance can be created by associating C-Vlan of type private to an I-SID.

When Etree I-SID in L2-SPBm-VSNs tree is selected, the **Etree Info** tab provides addition information about the associated private vlan.

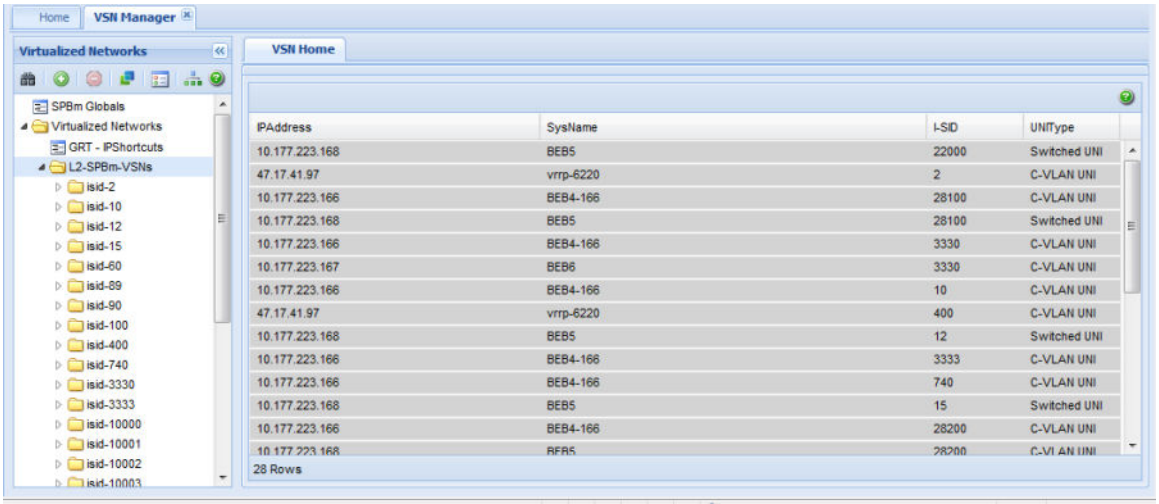


L2 SPBm functionality

Before you 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 Network (VSN) Manager 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.

SPBm and ISIS infrastructure configurations can be done using the VSN Wizard. For information on the VSN Wizard, refer to VLAN wizard on page 418.

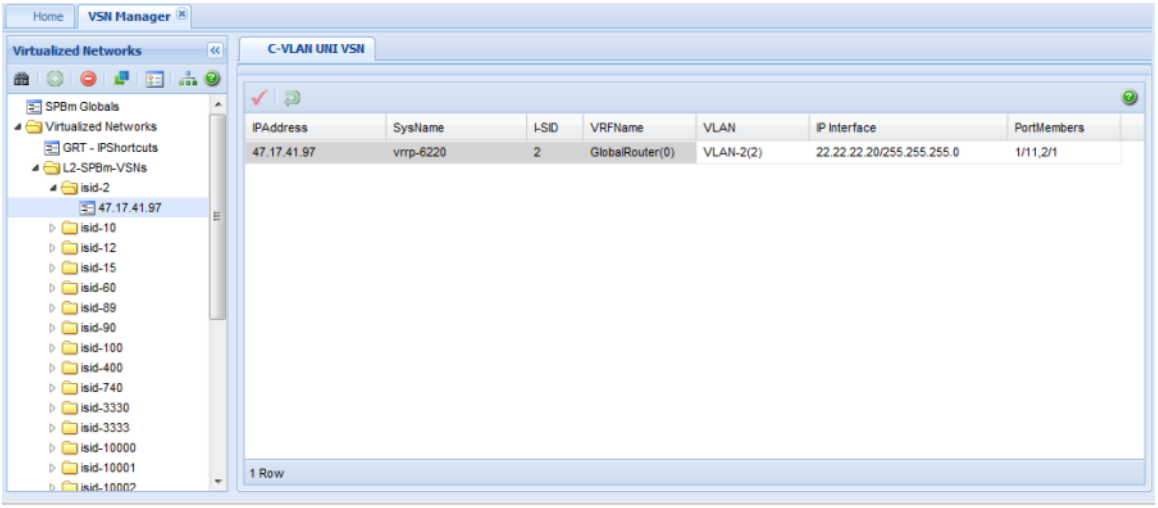
The following figure shows the top level L2 SPBm view.



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 UNI Type column distinguishes between the types of UNI associated with each I-SID entries. The values are **C-Vlan UNI** , **Switched UNI** , and **Both** based on the UNI type associated.

The following figure is an example of the VSN Manager window showing all the devices that belong to ISID-2.



In the preceding image, a customer VLAN is mapped to the ISID-2. Only one customer VLAN is mapped to a particular ISID.

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.

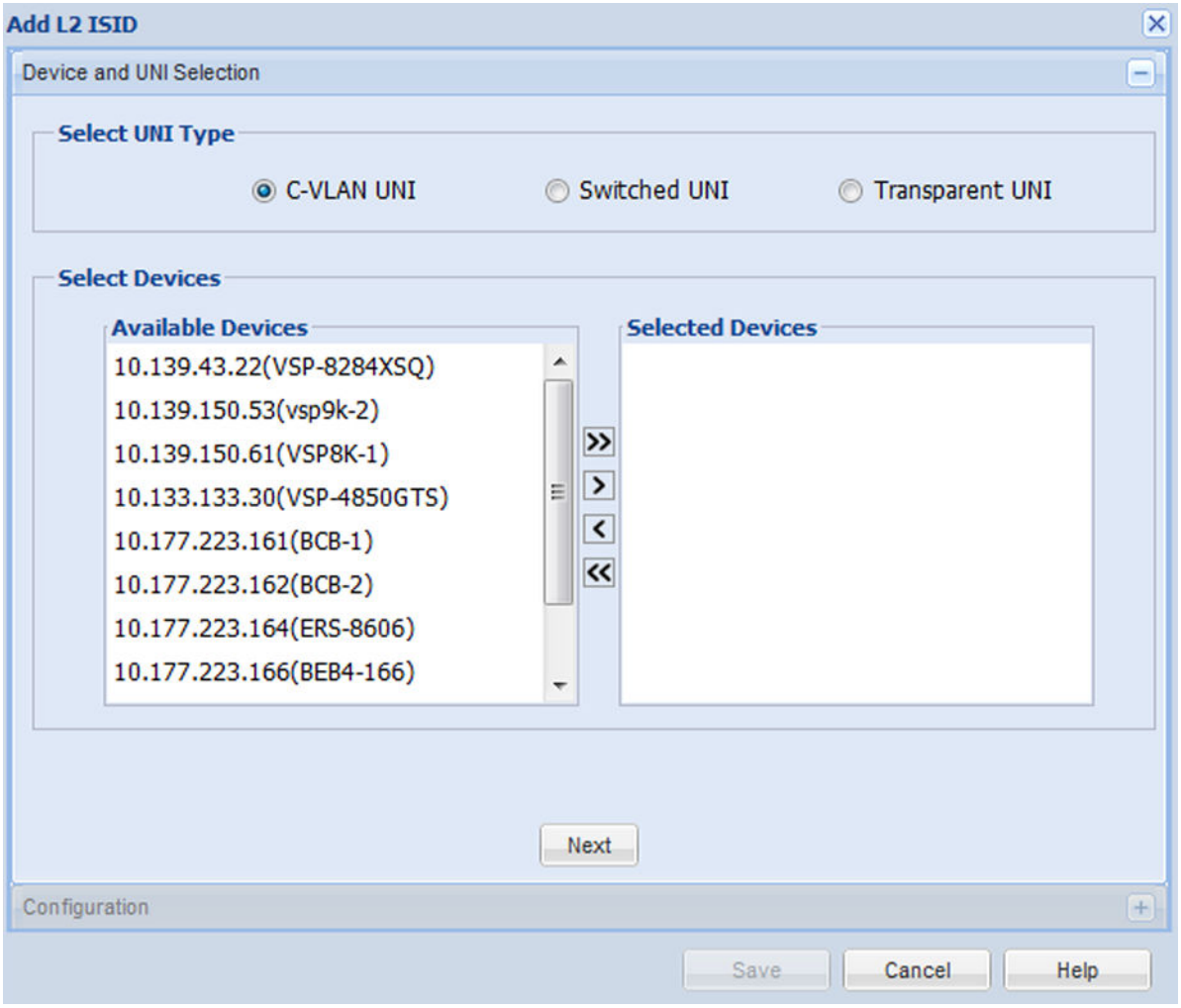
Note:

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 Add L2 ISID window displays.



3. Click C-VLAN UNI, Switched UNI, or Transparent UNI.
4. 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.

5. Click **Next**.

   After you have select the required devices, the server discovers all the available customer VLANs that are mapped to the ISID. The UI closes the selection panel, and the Configuration page displays.

6. In the Configuration page, type the ISID number in the **ISID Number** field.

   Note:

   If you selected Transparent UNI as the UNI Type, you can select the option to allow ports/MLTs belonging to Vlans to be selected.

The device table shows modifications for the devices that have a VLAN selected. For devices that do not have a selected VLANs, no modifications display.

7. For the devices that remain unmodified, you can either select a different 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 Add L2 ISID page displays.
3. Click **C-VLAN UNI**,**Switched UNI**, or **Transparent UNI**.
4. 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.
5. Click **Next**.

   After you have selected the required devices, the Configuration page displays.

   Note:

   If you selected Transparent UNI as the UNI Type, you can select the option to allow ports/MLTs belonging to Vlans to be selected.

   The device table shows modifications for the devices that have a VLAN selected. For devices that do not have a selected VLAN, no modifications appear. You cannot modify the ISID number.
6. For the devices that remain unmodified, you can either select a different 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 **Delete**.

Editing L2 SPBm tables

You can edit L2 Shortest Path Bridging MAC (SPBm) tables at the following two levels:

- ISID level
- Device level

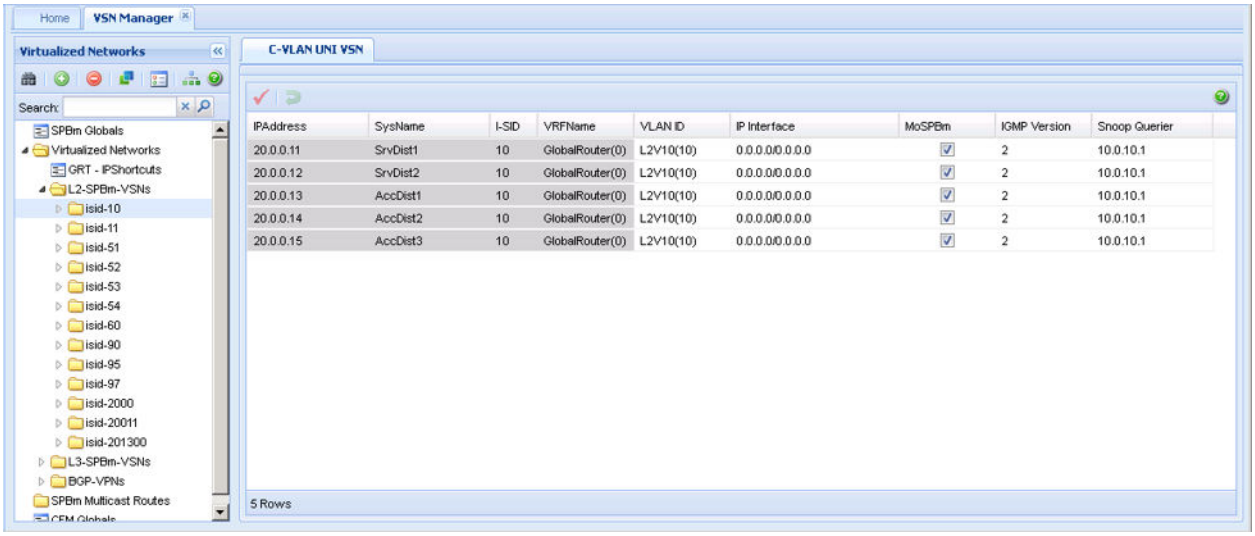
Editing L2 SPBm tables at the ISID level

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:

- VLAN ID for a particular ISID
- MoSPBm
- IP Interface
- IGMP version
- Snoop Querier

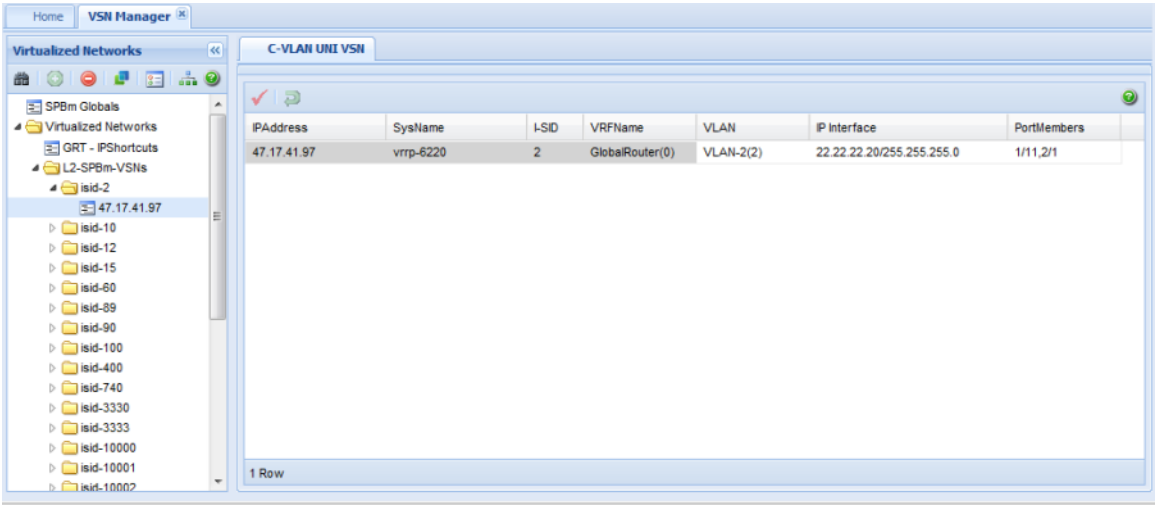
The VLAN ID field provides a list of all available VLANs on the selected device.

You can enable or disable the MoSPBm feature for a device from the MoSPBm checkbox column.



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 displays in a table in the contents pane.



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.

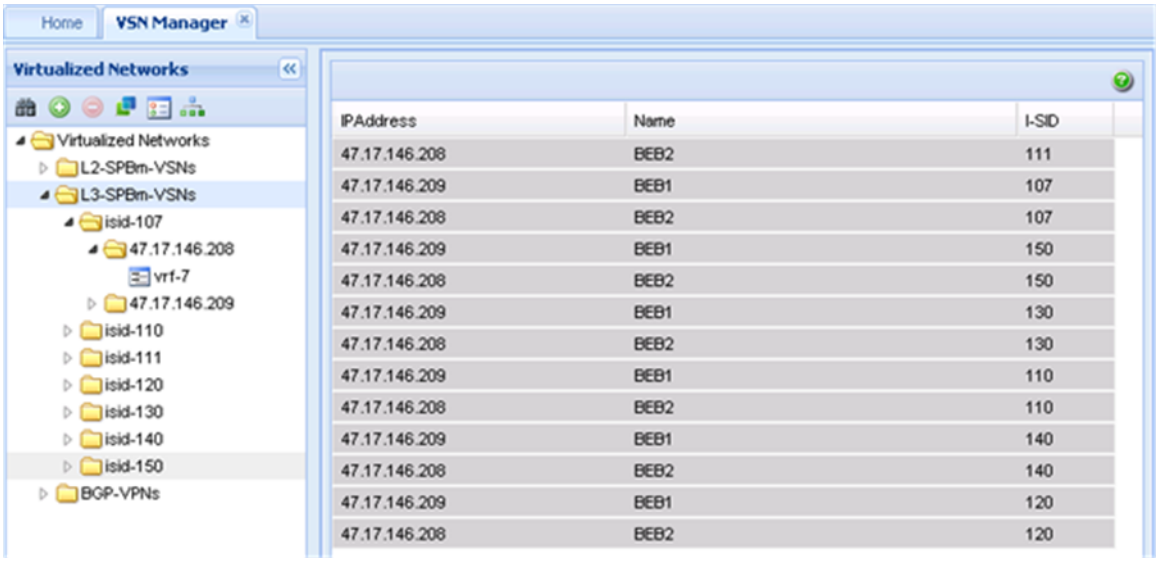
Note:

The L3 SPBm feature is not supported for VSP 7000 v10.2.

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.

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 231.

   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 72.

   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.

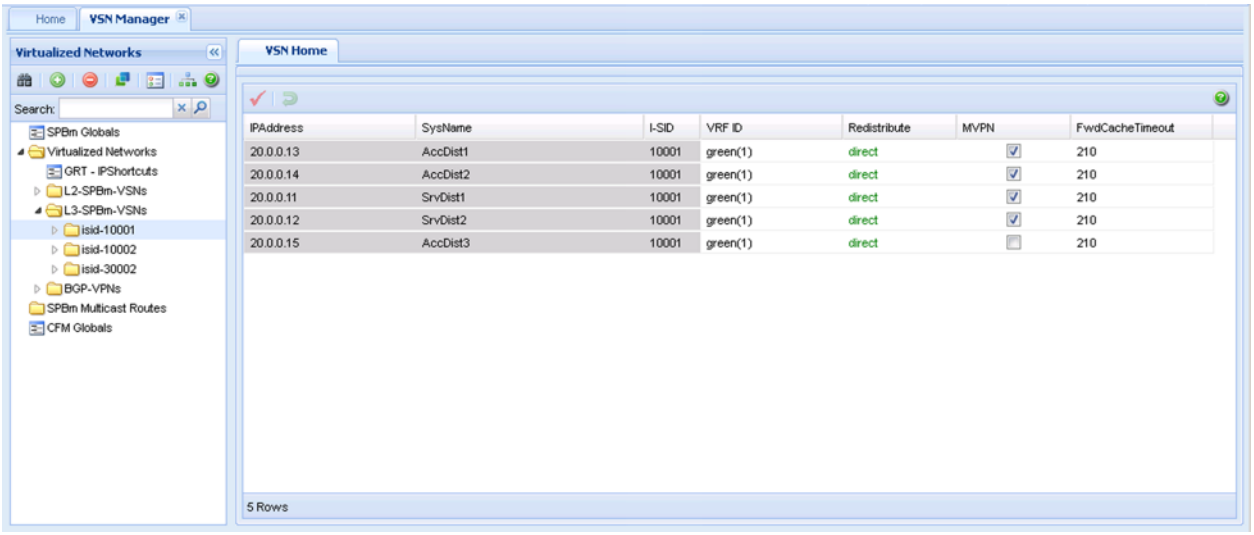
Procedure steps

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

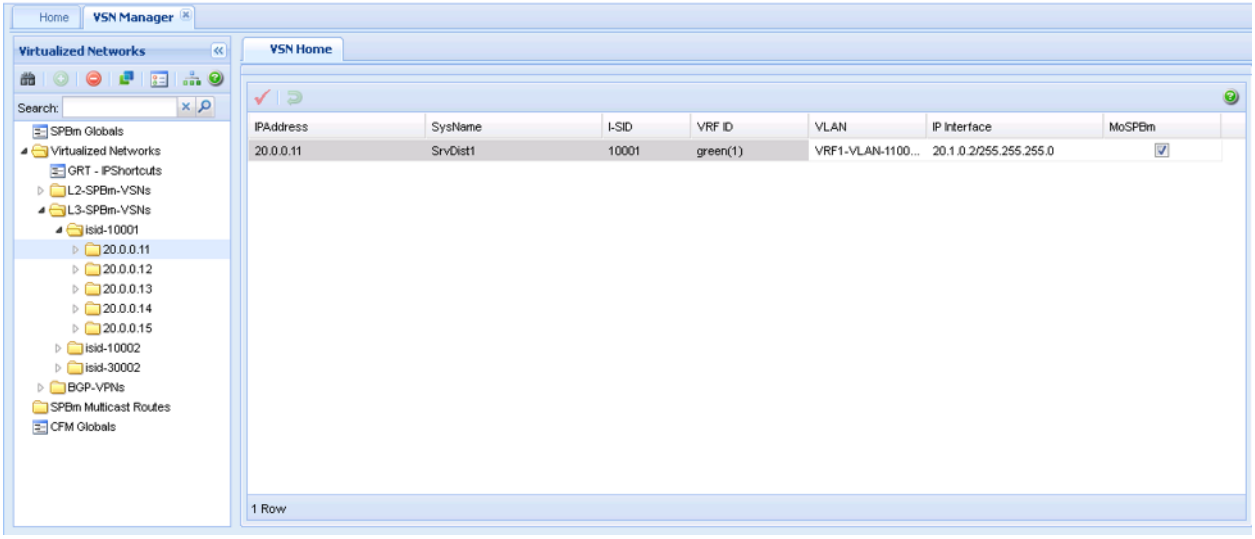
You can edit the configuration of the L3 Shortest Path Bridging MAC (SPBm) on multiple levels. After you select the required ISID, the information about that ISID appears in a table in the contents pane. In the ISID table, you can modify the following information:

- VRF ID
- mpvn
- Redistribute
- Fwd Cache Timeout



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:

- VLAN ID
- IP Interface
- Port Member
- MoSPBm
- Interface IP
- IGMP version



Editing Global Routing Table — IP Shortcuts

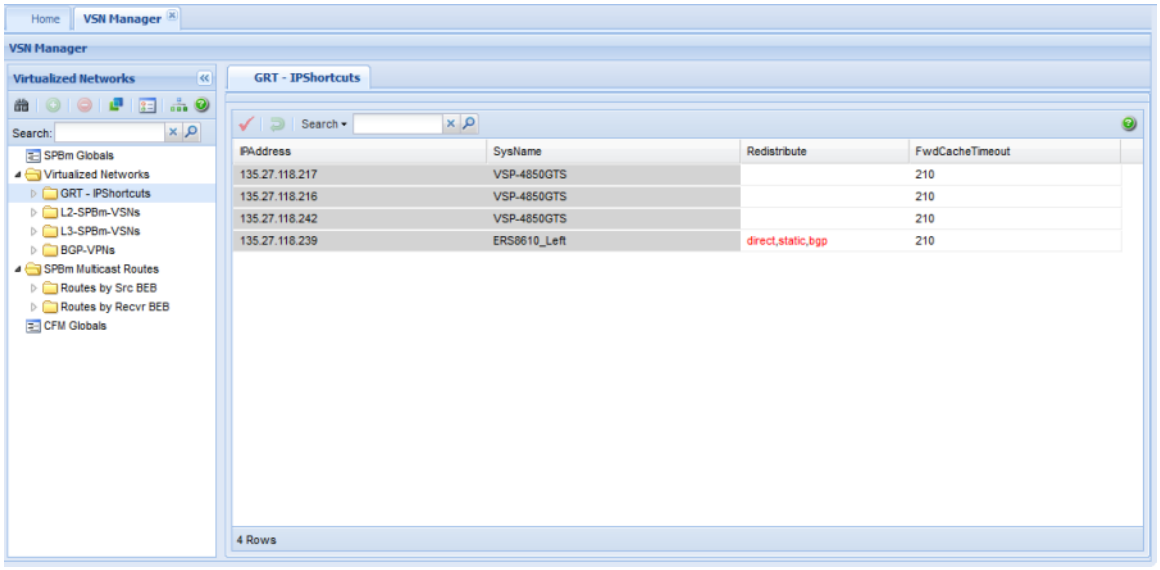
You can configure Global Routing Table (GRT) level attributes for IP Shortcuts and for IP Multicast over SPBm (MoSBBm).

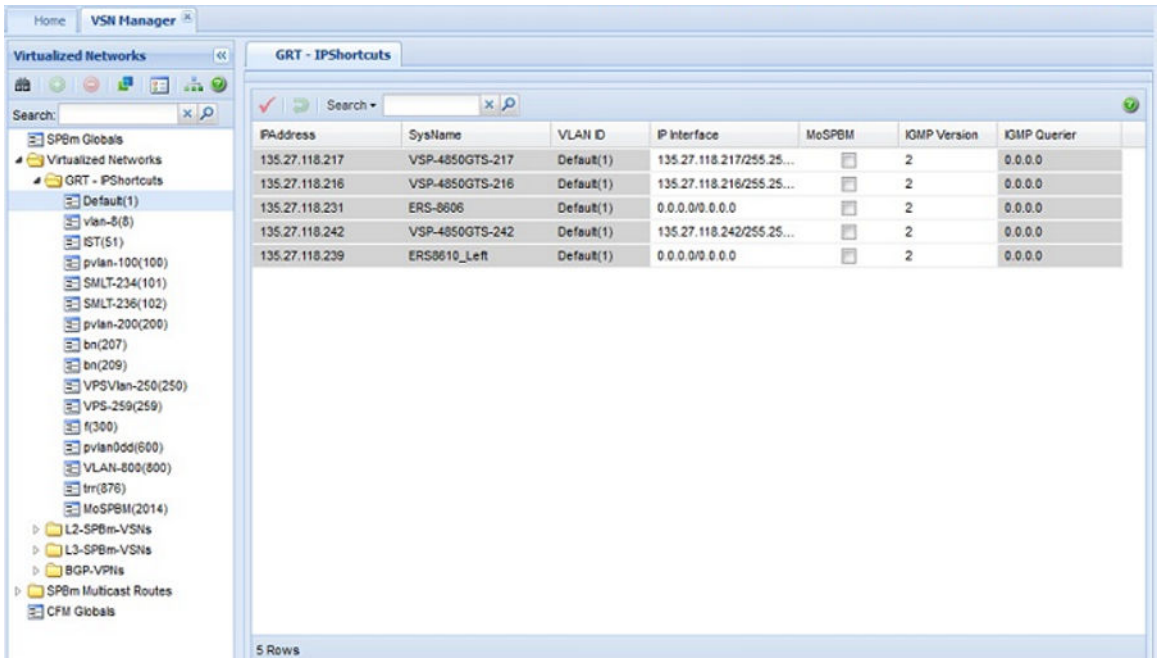
After you select an GRT—IP Shortcuts from the VSN Manager VSN-centric view, information displays in a table in the contents pane. In the GRT—IP Shortcuts table, you can modify the following information:

- Route Redistribute options
- MC Fwd Cache Timeout

After you select a device from GRT-IP Shortcuts, from the VSN Manager VSN-centric view, information on that device displays in a table in the contents pane. In the table, you can modify the following information:

- MoSPBm
- IGMP version



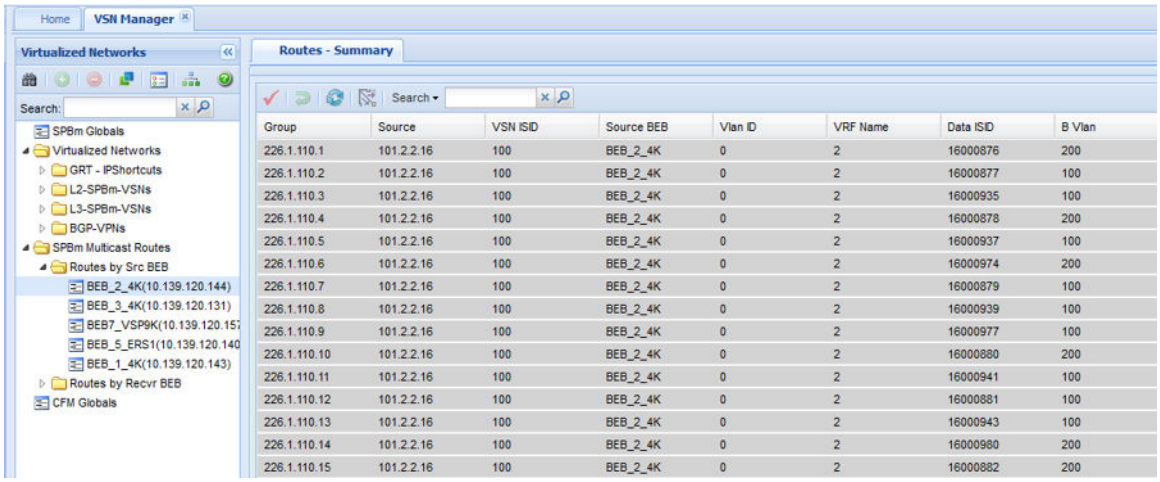


SPBm Multicast Route table

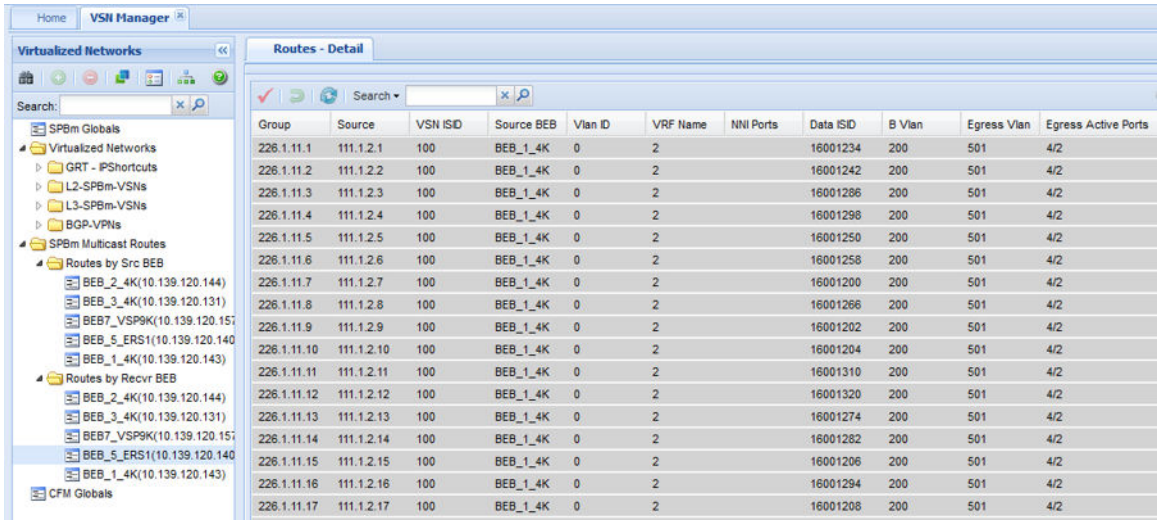
When you select the SPBm Multicast Route from the VSN Manager VSN-centric view, you can choose routes based on the source or the receiver BEB in the tree pane. Source BEB has multicast route entries for the sender of a multicast stream in the SPBm network; whereas the receiver BEB has multicast route entries for the receiver of a multicast stream.

When you select a device based on the source or receiver SPBm, corresponding route entries display in the contents pane.

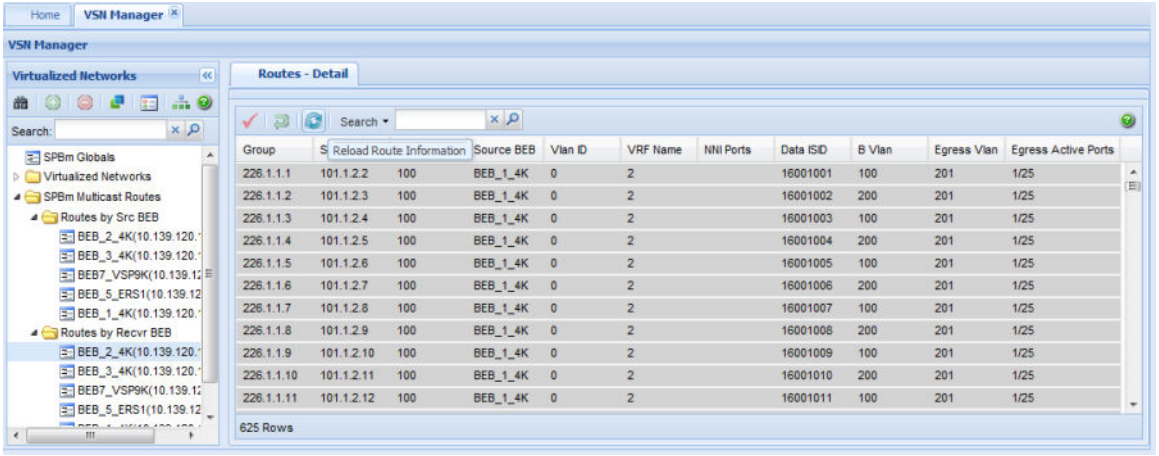
The following figure shows Multicast Routes by Src BEB.



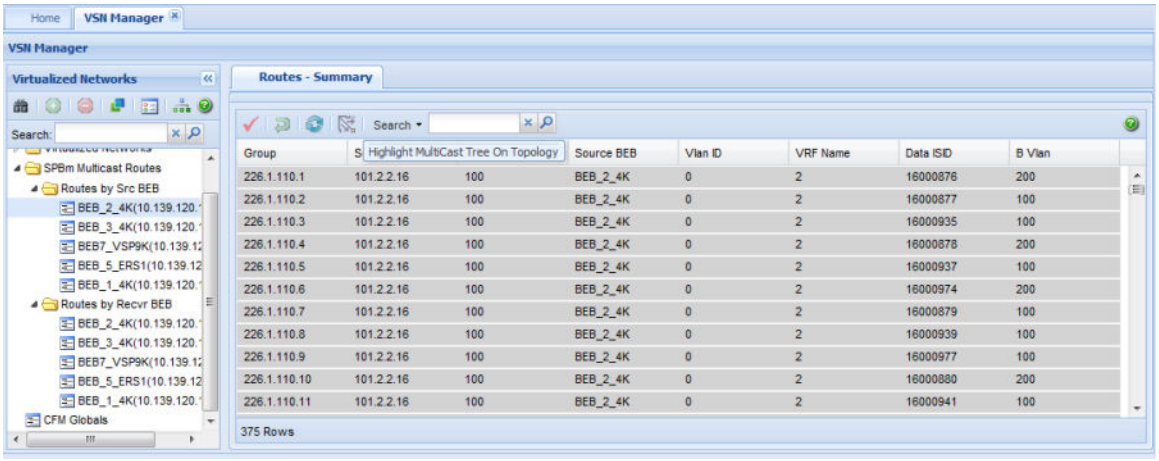
The following figure shows Multicast Routes by Receiver BEB.



Select **Reload Route Information** to reload the route data for the selected Source BEB.



Select **Highlight Multicast Tree on Topology** to show the selected source route/stream on the topology map. The SPBm Topology tab must be open for this operation.



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.

Note:

The BGP-VPN feature is not supported for VSP 7000 v10.2.

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.

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 326
2. Adding a Route Distinguisher to the VRF on page 327
3. Enabling the VPN status on page 327

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.

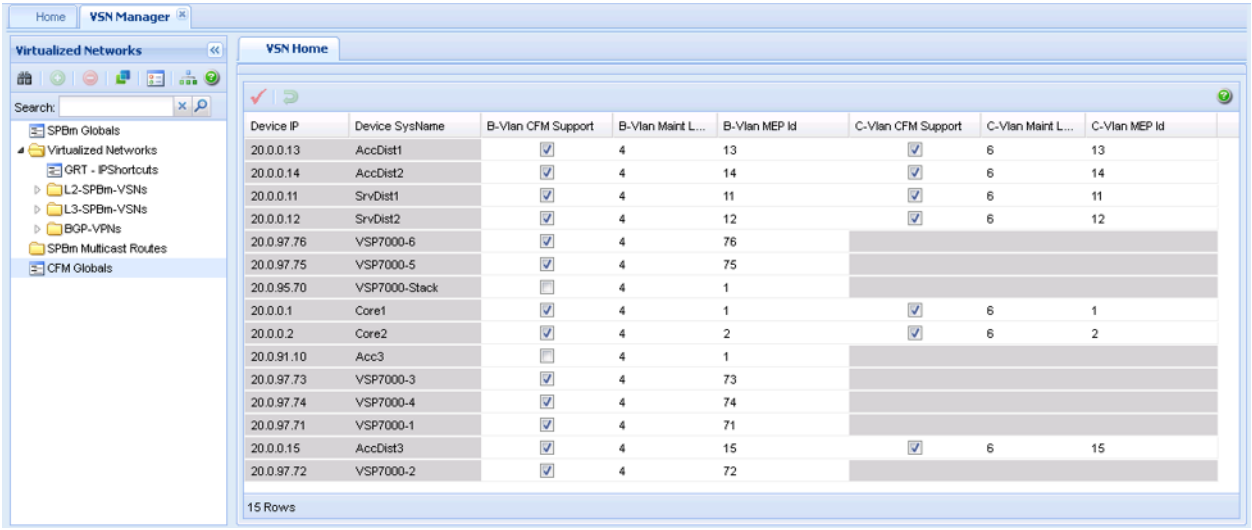
Procedure steps

1. From the **VSN Manager** navigation tree, select **BGP-VPNs**, and select a Route Target node.
2. From the **VSN Manager** toolbar, click **Delete**.

CFM Globals

CFM Globals table supports configuration of autogenerated CFM MEPs for both B-vlans and C-vlans. This support is provided in the VSN centric view.

The following figure shows the CFM Globals table.



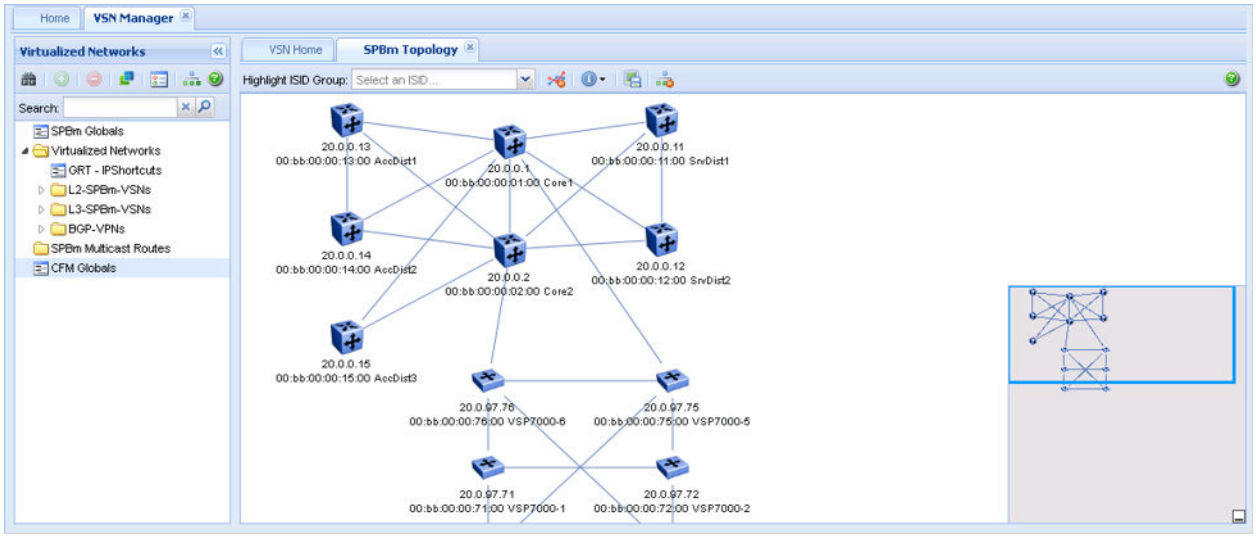
SPBm topology

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 figure is an example of the VSN Manager with SPBm Topology view.



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**.

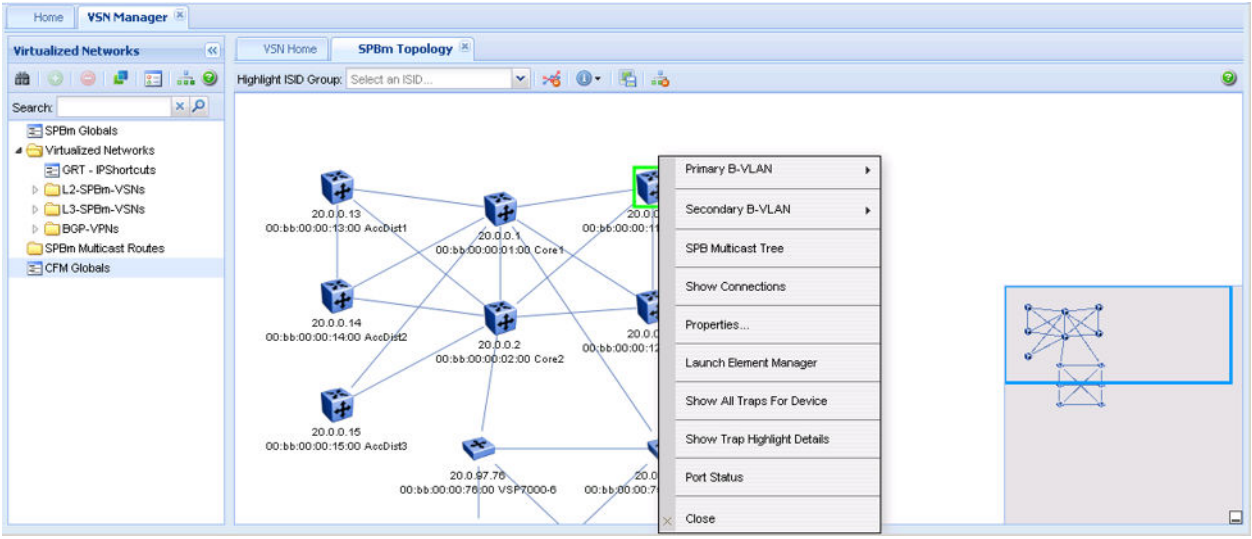
   COM performs a discovery, and then the Operation Result dialog box displays.

2. Click **Ok**.
3. From the **VSN Manager** toolbar, click **Show SPBm Topology**.

   The SPBM Topology view displays in the center of the contents pane.

SPB Multicast Tree

SPB Multicast Tree menu item displays Multicast Source (S), Multicast Group (G) and Scope Vsn / Vlan / Vrf combination for those devices that have IP Multicast over SPBm (MoSPBm) enabled. You can select **Highlight Computed Tree**, **Highlight L2TraceMRoute** and **Compare Multicast Trees.** options.



Generating computed SPBm Multicast Tree

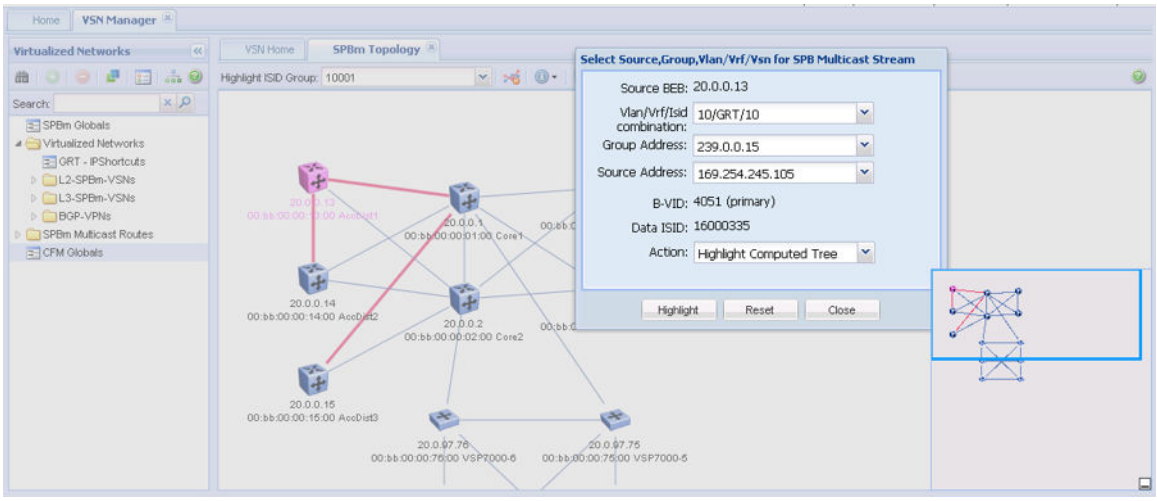
About this task

Perform the following procedure to generate a computed SPBm Multicast Tree.

Procedure

1. Generate an SPBm topology view. Refer to Generating an SPBm topology view on page 330.
2. Select the Multicast over SPBm (MoSPBm) enabled device.

   The Select Source,Group,Vlan/Vrf/Vsn for SPB Multicast Stream window displays.



3. Select the Vlan/Vrf/Isid from the list.
4. Select the Group Address from the list.
5. Select the Source Address from the list.

6. Select **Highlight Computed Tree** from the Action list.
7. Click **Highlight**.

Generating L2tracemroute tree

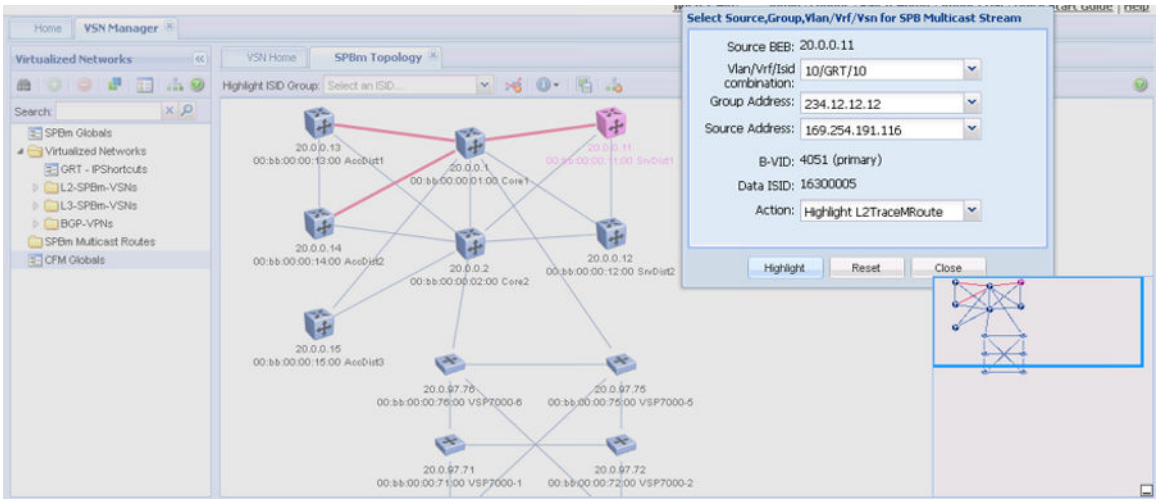
About this task

Perform the following procedure to generate an L2tracemroute tree.

Procedure

1. Generate an SPBm topology view. Refer to Generating an SPBm topology view on page 330.
2. Select the Multicast over SPBm (MoSPBm) enabled device.

   The Select Source,Group,Vlan/Vrf/Vsn for SPB Multicast Stream window displays.



3. Select the Vlan/Vrf/Isid from the list.
4. Select the Group Address from the list.
5. Select the Source Address from the list.
6. Select **Highlight L2TraceRoute** from the Action list.
7. Click **Highlight**.

Comparing computed and L2TraceRoute trees

About this task

Perform the following procedure to compare computed and L2TraceRoute trees.

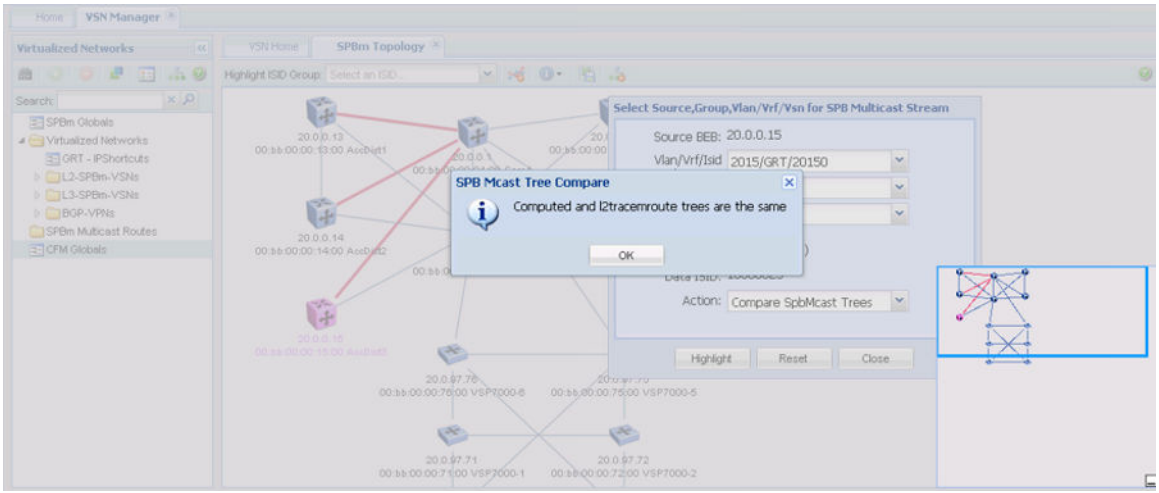
Procedure

1. Generate an SPBm topology view. Refer to Generating an SPBm topology view on page 330.
2. Select the Multicast over SPBm (MoSPBm) enabled device.

The Select Source,Group,Vlan/Vrf/Vsn for SPB Multicast Stream window displays.

3. Select the Vlan/Vrf/Isid from the list.
4. Select the Group Address from the list.
5. Select the Source Address from the list.
6. Select **Compare SbpMcast Trees** from the Action list.
7. Click **Highlight**.

   The SPB Mcast Tree Compare window displays.



8. Click **OK**.

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. The options are: • Multicast Path • Multicast Path by ISID

Option	Description
	• Unicast Path • Compare Unicast Path • L2 Trace Route • L2 Ping
Secondary B-VLAN	Displays the secondary VLAN map highlighting options. The options are: • Multicast Path • Multicast Path by ISID • Unicast Path • Compare Unicast Path • L2 Trace Route • 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.
Show All Traps For Device	Use this option to show all traps for a device. You can select this option by right-clicking on a device only.
Show Trap Highlight Details	Use this option to show trap highlight details of a device. You can select this option by right-clicking on a device only.
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.
L2 Trace Route	Performs an L2 Trace Route between two selected devices.
L2 Ping	Performs an L2 Ping between two selected devices.

Chapter 13: Management of Auto Detection and Auto Configuration on the Avaya Switch

The Avaya Configuration and Orchestration Manager (Avaya COM) Multimedia Manager manages Auto Detection/Auto Configuration (ADAC) and 802.1ab parameters of the Avaya switch. With ADAC, a switch supports and prioritizes Avaya IP Phone traffic without administrator intervention. With ADAC enabled, the switch automatically detects an Avaya IP phone after the phone connects to the switch, and then automatically configures the VLAN, port, and QoS settings for the phone.

Multimedia Manager supports the following 802.1ab parameters.

- For LLDP: Globals, Ports, and Neighbor
- For Port dot1: Local VLAN Id, Local Protocol VLAN, and Local VLAN Name
- For Port dot3: Local PoE, Local Link Aggregate, and Local Max Frame
- For Port med: Local Policy, Local Location, Local PoE PSE, Neighbor Capabilities, and Neighbor Inventory

Multimedia Manager requires COM 3.1 installation, and one or more of the following Avaya devices:

- ERS 2500 v4.1.0
- ERS 4500 v5.1.0
- ERS 55xx v5.0.0
- ERS 8300 v3.0
- ES 460/470 v3.6
- VSP 7000 v10.2 and above
- ERS 3500 v5.1 and above

Related Links

[About Multimedia Manager](#) on page 337
[Starting the Multimedia Manager](#) on page 337
[Actions](#) on page 338
[Navigation tree structure](#) on page 340
[Using tables to change device configuration](#) on page 340
[ADAC tables](#) on page 341
[802.1ab LLDP tables](#) on page 347

802.1ab Port dot1 tables on page 350
802.1ab Port dot3 tables on page 352
802.1ab Port med tables on page 354

About Multimedia Manager

You launch the Multimedia Manager from the Avaya Configuration and Orchestration Manager (COM) navigation pane; the Multimedia Manager user interface (UI) displays in a separate COM tab.

After you select the Multimedia Manager for the first time, the Multimedia Manager performs a discovery of devices, and displays the progress of the discovery.

The Multimedia Manager UI is composed of two parts, presented side by side.

- The Multimedia Manager navigation tree—displays furthest to the left. Expand or collapse the nodes by clicking on the node handles that appear in front of the node, and then select the node.
- The Multimedia Manager Content Panel—displays to the right of the Multimedia Manager navigation tree. After you select a node in the Multimedia navigation tree, information about the node displays in the Multicast Manager content pane.

Note:

VSP 8000 does not support Multimedia Manager functionality.

Related Links

Management of Auto Detection and Auto Configuration on the Avaya Switch on page 336

Starting the Multimedia Manager

Perform the following procedure to launch the Mutimedia Manager.

Procedure

1. From the COM navigation panel, expand **Managers**.
2. Click **Multimedia Manager**.

   The Multimedia Manager user interface (UI) appears in a separate COM tab.

Related Links

Management of Auto Detection and Auto Configuration on the Avaya Switch on page 336

Actions

With the Multimedia Manager, you can perform manager actions and table actions.

Manager actions

You can perform the following actions in the Multimedia Manager context.

- Discover—rediscovers device information.
- Preferences—manage user preferences.
- Help—launch help information.

Table actions

You can perform the following actions in the Multimedia Manager single table context; not all operations are available for all tables.

- Add—add a new table row.
- Delete—removes table row.
- Save—sends user changes to the device.

Related Links

Management of Auto Detection and Auto Configuration on the Avaya Switch on page 336
Performing a Multimedia discovery on page 338
Selecting preferences for the Multimedia Manager on page 338
Adding a table row on page 339
Deleting a table row on page 340

Performing a Multimedia discovery

Perform the following procedure to discover devices in the Multimedia Manager.

Procedure

1. From the Multimedia Manager menu bar, click **Discover Multimedia**.

   The Multimedia discovery progress bar appears.
2. To view details of the discovery, click **Details**.
3. After the discovery is complete, click **OK**.

Related Links

Actions on page 338

Selecting preferences for the Multimedia Manager

Perform the following procedure to manage user preferences for the Multimedia Manager.

Procedure

1. From the Multimedia Manager menu bar, click **Preferences**.

   The Multimedia Manager Preferences dialog box appears.

2. Select or clear the check box to enable or disable the associated filters to manage devices in current group context. The available options to configure Multimedia Manager preferences are:

   - Manage by device family—allows you to choose the supported device families: VSP 7XXX, VSP 9XXX, ERS 8000, ERS 16XX, Ethernet Switch/ERS 25XX, Alteon, Legacy BayStack, Legacy ERS 1424/16XX, ERS 55XX/56XX/45XX/35XX, WC 8XXX, and WLAN AP.
   - 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 and click the right-pointing arrow to move the devices to the Selected Devices list.

3. Click **OK**.

Related Links

Actions on page 338

Adding a table row

Perform the following procedure to add a table row in the Multimedia Manager ADAC MAC Address Ranges table.

Note:

Not all operations are available for all tables.

Procedure

1. From the Multimedia Manager table toolbar, click **Add**.

   The Add New Entry dialog box appears.

2. In the Low End Index field, enter a value.
3. In the High End Index field, enter a value.
4. Click **Save**.

Related Links

Actions on page 338

Deleting a table row

Perform the following procedure to delete a table row from the Multimedia Manager.

Note:

Not all operations are available for all tables.

Procedure

1. From the Multimedia Manager table, select a row.
2. From the table toolbar, click **Delete**.
3. In the Remove dialog box, click **Yes**.

Related Links

Actions on page 338

Navigation tree structure

The navigation tree of the Multimedia Manager contains the Multimedia Networks root node. The Multimedia Networks node contains the following sub-nodes.

- ADAC—displays nodes for discovered devices that have ADAC enabled.
- 802.1ab—is further divided into sub-nodes for the following network layer 2 discovery protocol: LLDP, Port dot 1, Port dot 3, Port med; each protocol node displays nodes for devices operating that protocol.

The following sections describe the major folders and the content within the folders.

Related Links

Management of Auto Detection and Auto Configuration on the Avaya Switch on page 336

Using tables to change device configuration

The Multimedia Manager data for a device appears in tables in the contents pane. To access the Multimedia Manager data, navigate through the required tree, and select the required device. A table appears in the contents pane and its cells containing data specific to the device. Each tab above the table represents a different table.

If a cell has a white background, you can configure the cell by changing the data in the cell. However, if you change the data in the cell, you change the configuration of the device.

Related Links

Management of Auto Detection and Auto Configuration on the Avaya Switch on page 336

ADAC tables

ADAC tables appear in the content pane after you select the device node in the ADAC folder of the navigation tree.

The following sections list and describe the parts of the ADAC tables.

Related Links

Management of Auto Detection and Auto Configuration on the Avaya Switch on page 336
Global table on page 341
Ports table on page 343
Mac Ranges table on page 345
ADAC support by device and version on page 345
Resetting the ADAC MAC ranges on page 347

Global table

The following table describes the parts of the ADAC Global table.

Table 108: Global table

Part	Details
AdminEnable	Administratively enables or disables ADAC. The values are True (1) for enabled, and False (2) for disabled. ADAC can be disabled operationally even if it is enabled administratively. To determine if ADAC is enabled operationally, see OperEnable. The following devices support ADAC: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.0.0 and above, and ES 460/470 v3.6.0 and above.
OperatingMode	This setting depends on how the IP Phones are configured to send frames, tagged or untagged, and on the level of complexity required for auto-configuration. The options are: • untaggedFramesBasic (1)—The IP Phones send untagged frames. A Voice-VLAN is not created; that is, only apply QoS autoconfiguration. • untaggedFramesAdvanced (2)—The IP Phones send untagged frames, the Voice VLAN is created, and QoS autoconfiguration is applied. • taggedFrames (3)—The IP Phones send tagged frames, the Voice VLAN is created, and QoS autoconfiguration is applied.

Part	Details
	If VoiceVlan has the value 0, or if both CallServerPort and UplinkPort have the value 0, you cannot select the untaggedFramesAdvanced and taggedFrames. The following devices support OperatingMode: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.0.0 and above, and ES 460/470 v3.6.0 and above.
VoiceVlan	Uniquely identifies the Voice Virtual LAN associated with ADAC, and only applies if OperatingMode is untaggedFramesAdvanced or taggedFrames. If either of these options is selected, you cannot change VoiceVlan to 0. The following devices support VoiceVlan: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.0.0 and above, and ES 460/470 v3.6.0 and above.
NotificationControl Enable	Controls the generation of a PortConfigNotification after the port status changes. If the value is True (1), notifications are generated; if the value is False (2), notifications are not generated. The following devices support Notification ControlEnable: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.0.0 and above, and ES 460/470 v3.6.0 and above.
CallServerPort	The port on which the Call Server is connected, and only applies if OperatingMode is untaggedFramesAdvanced, or taggedFrames. If either of these options is selected, you cannot change CallServerPort to 0. The following devices support CallServerPort: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.0.0 and above, and ES 460/470 v3.6.0 and above.
UplinkPort	Uniquely identifies the Voice Virtual LAN associated with ADAC, and only applies if OperatingMode is untaggedFramesAdvanced or taggedFrames. If either of these options is selected, you cannot change UplinkPort to 0. Usually applies if the Call Server is not connected directly to the current module/stack. The following devices support UplinkPort: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.0.0 and above, and ES 460/470 v3.6.0 and above.
MacAddrRange Control	Returns a value of none (1) to indicate that no option is selected. The options are: • clearTable—Deletes all entries from the MAC address range table. • defaultTable—Deletes all entries from the MAC address range table and replaces them with factory defaults. The following devices support MacAddrRange Control: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.0.0 and above, and ES 460/470 v3.7.0 and above.
OperEnable	Indicates if ADAC is enabled operationally. The values are True (1) for enabled, and False (2) for disabled. This is a read only parameter.

Part	Details
	A value of False for OperEnable combined with a value of True for AdminEnable indicates that ADAC is not operational due to a condition such as missing Uplink and Call Server ports. The following devices support OperEnable: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.1.0 and above, and ES 460/470 v3.7.0 and above.

Related Links

ADAC tables on page 341

Ports table

The following table describes the parts of the ADAC Ports table.

Table 109: Ports table

Part	Details
AdminEnable	Enables or disables ADAC on the port. The values are True (1) for enabled, and False (2) for disabled. The following devices support AdminEnable: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.0.0 and above, and ES 460/470 v3.6.0 and above.
AdacStatus	Enables or disables ADAC on the port. The values are True (1) for enabled, and False (2) for disabled. The following devices support AdacStatus: ERS 8300 v3.0 and above.
ConfigStatus	Status of auto configuration on the port. The values are: • configApplied (1)—indicates that the ADAC configuration has been applied • configNotApplied (2)—indicates ADAC configuration has not been applied. The following devices support ConfigStatus: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.0.0 and above, and ES 460/470 v3.6.0 and above.
TaggedFramesPvid	The PVID value that auto configuration applies to a port. The port must have auto detection enabled, and must be running in Tagged-Frames operational mode. For example: • AdminEnable is True • OperatingMode, ADAC table, is set to taggedFrames

Part	Details
	The following devices support TaggedFrames Pvid: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.1.0 and above, and ES 460/470 v3.7.0 and above.
TaggedFrames Tagging	The tagging value that auto configuration applies to a port. The options are: • tagAll - 1 • tagPvidOnly - 2 • untagPvidOnly - 3 • noChange - 4 The port must have auto detection enabled, and must be running in Tagged-Frames operational mode. For example: • AdminEnable is True • OperatingMode, ADAC table, is set to taggedFrames The following devices support TaggedFrames Tagging: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.1.0 and above, and ES 460/470 v3.7.0 and above.
PortType	ADAC classification of the port. The options are: • telephony (1)—indicates that auto detection is enabled; AdminEnable is True • callServer (2)—indicates that the port is configured as Call Server • uplink (3)—indicates that the port is configured as Uplink or it is part of the same trunk as the port that is currently configured as Uplink • other (4)—indicates that none of the above types applies The following devices support PortType: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.1.0 and above, and ES 460/470 v3.7.0 and above.
OperEnable	Indicates if auto detection is enabled operationally. The values are True (1) for enabled, and False (2) for disabled. The following devices support OperEnable: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, and ERS 55xx v5.1.0 and above.
MacDetectionEnable	Status of auto detection based on MAC address. The values are True (1) for auto detection by MAC address, and False (2) if not by MAC address. If auto detection is enabled, and AdminEnable is True, MacDetectionEnable cannot be set to False unless another detection mechanism is enabled on the port. For example: LldpDetectionEnable.

Part	Details
	The following devices support MacDetection Enable: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, and ERS 55xx v5.1.0 and above.
LldpDetectionEnable	Status of auto detection based on 802.1ab. The values are True (1) for auto detection by 802.1ab, and False (2) if not by 802.1ab. If auto detection is enabled, and AdminEnable is True, LldpDetectionEnable cannot be set to False unless another detection mechanism is enabled on the port. For example: MacDetectionEnable. The following devices support LldpDetection Enable: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, and ERS 55xx v5.1.0 and above.

Related Links

ADAC tables on page 341

Mac Ranges table

The following table describes the parts of the ADAC Mac Ranges table.

Table 110: Mac Ranges table

Part	Details
MacAddrRangeLowEndIndex	The low end of the MAC Address range supported by ADAC. The following devices support MacAddrRange LowEndIndex: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.0.0 and above, and ES 460/470 v3.7.0 and above.
MacAddrRangeHighEndIndex	The high end of the MAC Address range supported by ADAC. MacAddrRange HighEndIndex The following devices support MacAddrRange HighEndIndex: ERS 2500 v4.1.0 and above, ERS 4500 v5.1.0 and above, ERS 55xx v5.0.0 and above, and ES 460/470 v3.7.0 and above.

Related Links

ADAC tables on page 341

ADAC support by device and version

You can configure ADAC globally or on a port-by-port basis, depending on the device and version. Support for ADAC tables and individual parameters also depends on the device and version. Support for individual parameters is listed with the parameter.

The following table outlines the table-level support, and indicates if the device supports global configuration.

Table 111: ADAC configuration options for devices

Device	Version	Configuration options
ERS 2500	v4.1.0 and above	• Global and port-by-port. • Port settings override global settings. • ADAC, ADAC Mac Ranges, and ADAC-Ports tables available.
ERS 4500	v5.1.0 and above	• Global and port-by-port. • Port settings override global settings. • ADAC, ADAC Mac Ranges, and ADAC-Ports tables available.
ERS 55xx	v5.0.0	• By port only. • ADAC-Ports table available.
ERS 55xx	v5.1.1 and above	• Global and port-by-port. • Port settings override global settings. • ADAC, ADAC Mac Ranges, and ADAC-Ports tables available.
ERS 8300	all versions	• By port only. • ADAC-Ports table available.
ES 460	v3.6.0	• Global and port-by-port. • Port settings override global settings. • ADAC and ADAC-Ports tables available.
ES 470	v3.6.0	• Global and port-by-port. • Port settings override global settings. • ADAC and ADAC-Ports tables available.
ES 460	v3.7.0	• Global and port-by-port. • Port settings override global settings. • ADAC, ADAC Mac Ranges, and ADAC-Ports tables available.
ES 470	v3.7.0	• Global and port-by-port. • Port settings override global settings. • ADAC, ADAC Mac Ranges, and ADAC-Ports tables available.
VSP 7000	v10.2 and above	• Global and port-by-port. • Port settings override global settings.

Device	Version	Configuration options
		• ADAC, ADAC Mac Ranges, and ADAC-Ports tables available.
ERS 35xx	v5.1 and above	• Global and port-by-port. • Port settings override global settings. • ADAC, ADAC Mac Ranges, and ADAC-Ports tables available. **Note:** Functionality for 802.1ab Port dot1 tables and 802.1ab Port dot3 tables is not supported.
All	All	• A port can support an unlimited number of IP Phones.

Related Links

ADAC tables on page 341

Resetting the ADAC MAC ranges

Perform the following procedure to reset the ADAC MAC ranges.

Procedure

1. From the Multimedia Manager, select the **ADAC Global** tab.
2. Select a device.
3. In the MAC Address Range Control column, click the down arrow, and select **clearTable**.
4. Click **Apply**.

Related Links

ADAC tables on page 341

802.1ab LLDP tables

LLDP tables are presented in the content pane after you select the device node in the 802.1ab, LLDP folder in the navigation tree.

The following sections list and describe the parts of the LLDP tables.

Related Links

Management of Auto Detection and Auto Configuration on the Avaya Switch on page 336
Global table on page 348
Ports table on page 349
Remote table on page 350

Global table

The following table describes the LLDP Global table.

Table 112: LLDP Global table

Part	Details
MessageTxInterval	The interval at which LLDP frames are transmitted on behalf of this LLDP agent.
MessageTxHold Multiplier	The time-to-live value expressed as a multiple of MessageTxInterval.
ReinitDelay	Indicates the delay, in seconds, between the time that PortConfigAdminStatus becomes disabled and the time that re-initialization is attempted. For more information, see Port.
TxDelay	Indicates the delay, in seconds, between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.
NotificationInterval	Controls the transmission of LLDP notifications.
StatsRemTablesLast ChangeTime	The value of sysUpTime, AS defined in IETF RFC 3418, at the time an entry is created, modified, or deleted in the tables associated with lldpRemoteSystemsData objects and all LLDP extension objects associated with remote systems.
StatsRemTables Inserts	The number of times the complete set of information advertised by a particular MSAP has been inserted into tables contained in lldpRemoteSystemsData and lldpExtensions objects.
StatsRemTables Deletes	The number of times the complete set of information advertised by a particular MSAP has been deleted from tables contained in lldpRemoteSystemsData and lldpExtensions objects.
StatsRemTables Drops	The number of times the complete set of information advertised by a particular MSAP could not be entered into tables contained in lldpRemoteSystemsData and lldpExtensions objects because of insufficient resources.
StatsRem TablesAgeouts	The number of times the complete set of information advertised by a particular MSAP has been deleted from tables contained in lldpRemoteSystemsData and lldpExtensions objects because the information timeliness interval has expired.
FastStartRepeat Count	The number of times the fast start LLDPDU are being sent during the activation of the fast start mechanism defined by LLDP-MED.

Related Links

802.1ab LLDP tables on page 347

Ports table

The following table describes the LLDP Ports table.

Table 113: LLDP Ports table

Part	Details
PortConfigPortNum	The index value used to identify the port component, contained in the local chassis with the LLDP agent, associated with the entry.
PortConfigAdmin Status	The administratively desired status of the local LLDP agent. The options are: • txOnly (1) • rxOnly (2) • txAndRx (3) • disabled (4)
PortConfig NotificationEnable	Controls, on a per port basis, whether or not notifications from the agent are enabled. The values are True (1) for enabled, and False (2) for disabled.
PortConfigTLVsTx Enable	A bitmap that includes the basic set of LLDP TLVs that transmit on the local LLDP agent by the network management. Each bit in the bitmap corresponds to a TLV type associated with a specific optional TLV.
Xdot1ConfigPort VlanTxEnable	A truth-value that is configured by the network management, and determines whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is allowed on a given LLDP transmission capable port.
Xdot3PortConfig TLVsTxEnable	A bitmap that includes the IEEE 802.3 organizationally defined set of LLDP TLVs that transmit on the local LLDP agent by the network management. Each bit in the bitmap corresponds to an IEEE 802.3 subtype associated with a specific IEEE 802.3 optional TLV. The bit 0 is not used because there is no corresponding subtype.
XMedPortCap Supported	A bitmap that includes the MED organizationally defined set of LLDP TLVs that can transmit for the respective port on the LLDP agent of the device. Each bit in the bitmap corresponds to an LLDP-MED subtype associated with a specific TIA TR41.4 MED optional TLV. If the bit is set, the agent supports the corresponding TLV.
XMedPortConfig TLVsTxEnable	A bitmap that includes the MED organizationally defined set of LLDP TLVs that transmit on the local LLDP agent by the network management. Each bit in the bitmap corresponds to an LLDP-MED subtype associated with a specific TIA TR41.4 MED optional TLV. If the bit is set, the agent will send the corresponding TLV if the respective capability is supported per port.
XMedPortConfig NotifEnable	Enables or disables the sending of the topology change traps on this port. The values are True (1) for enable, and False (2) for disable.

Related Links

802.1ab LLDP tables on page 347

Remote table

The following table describes the LLDP Remote table.

Table 114: LLDP Remote table

Part	Details
TimeMark	A TimeFilter for this entry.
LocalPortNum	The index value used to identify the port component, contained in the local chassis with the LLDP agent, associated with this entry. LocalPortNum identifies the port on which the remote system information is received.
Index	Represents an arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated remote system.
ChassisIdSubtype	The type of encoding used to identify the chassis associated with the remote system.
ChassisId	The string value used to identify the chassis component associated with the remote system.
SysCapSupported	The bitmap value used to identify which system capabilities are supported on the remote system.
SysCapEnabled	The bitmap value used to identify which system capabilities are enabled on the remote system.
SysName	The string value used to identify the system name of the remote system.
SysDesc	The string value used to identify the system description of the remote system.
PortIdSubtype	The type of port identifier encoding used in the associated PortId.
PortId	The string value used to identify the port component associated with the remote system.
PortDesc	The string value used to identify the description of the given port associated with the remote system.

Related Links

802.1ab LLDP tables on page 347

802.1ab Port dot1 tables

Port dot1 tables are presented in the content pane when the device node is selected in the 802.1ab/Port dot 1 folder in the navigation tree.

You can configure 802.1ab Port dot1 parameters on the following devices:

- ERS 4500 v5.1.0 and above
- ERS 55xx v5.0.0 and above
- ERS 8300 v3.0 and above
- VSP 7000 v10.2 and above

The following sections list and describe the 802.1ab Port dot1 tables.

Related Links

Management of Auto Detection and Auto Configuration on the Avaya Switch on page 336
Local VLAN Id table on page 351
Local Protocol VLAN table on page 351
Local VLAN Name table on page 352

Local VLAN Id table

The following table describes the Local VLAN Id table.

Table 115: Local VLAN Id table

Part	Details
PortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
VlanId	The integer value that identifies the port VLAN identifier associated with the local system. A value of zero indicates that the system does not know the PVID, or does not support port-based VLAN operation.

Related Links

802.1ab Port dot1 tables on page 350

Local Protocol VLAN table

The following table describes the Local Protocol VLAN table.

Table 116: Local Protocol VLAN table

Part	Details
PortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
ProtoVlanId	The integer value that identifies the port and protocol VLANs associated with the given port associated with the local system. A value of zero indicates that the system does not know the protocol VLAN ID (PPVID) or does not support port and protocol VLAN operation

Part	Details
ProtoVlanSupported	The truth-value that indicates if the given port, associated with the local system, supports port and protocol VLANs.
ProtoVlanEnabled	The truth-value that indicates if the port and protocol VLANs are enabled on the given port associated with the local system.
ProtoVlanTxEnable	The Boolean value that indicates if the corresponding Local System Port and Protocol VLAN instance is transmitted on the port defined by the given ProtoVlanId.

Related Links

802.1ab Port dot1 tables on page 350

Local VLAN Name table

The following table describes the Local VLAN Name table.

Table 117: Local VLAN Name table

Part	Details
PortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
VlanId	The integer value that identifies the IEEE 802.1Q VLAN IDs with which the given port is compatible.
VlanName	The string value that identifies the VLAN name identified by the Vlan Id associated with the given port on the local system. VlanName must contain the value of the dot1QVLANStaticName object, as defined in IETF RFC 2674, identified with the given VlanId.
VlanNameTxEnable	The Boolean value that indicates if the corresponding Local System VLAN name instance is transmitted on the port defined by the given VlanName.

Related Links

802.1ab Port dot1 tables on page 350

802.1ab Port dot3 tables

Port dot3 tables are presented in the content pane after you select the device node in the 802.1ab/ Port dot3 folder in the navigation tree.

You can configure the 802.1ab Port dot3 parameters on the following devices:

- ERS 4500 v5.1.0 and above
- ERS 55xx v5.0.0 and above
- ERS 8300 v3.0 and above

- VSP 7000 v10.2 and above

The sections list and describe the 802.1ab Port dot3 tables.

Related Links

Management of Auto Detection and Auto Configuration on the Avaya Switch on page 336
Power tables on page 353
Link table on page 354

Power tables

The following table describes the 802.1ab Port dot3 Power tables.

Table 118: Power tables

Table	Details	
Local PoE	PortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
	PowerPortClass	The value that identifies the port Class of the given port associated with the local system.
	PowerMDI Supported	The truth-value that indicates if the MDI power is supported on the given port associated with the local system.
	PowerMDIEnabled	The truth-value that identifies if MDI power is enabled on the given port associated with the local system.
	PowerPair Controlable	Contains the value of the pethPsePortPowerPairs object, as defined in IETF RFC 3621, associated with the given port on the local system.
	PowerPairs	Contains the value of the pethPsePortPowerPairs object, as defined in IETF RFC 3621, associated with the given port on the local system.
	PowerClass	Contains the value of the pethPsePortPowerClassifications object, as defined in IETF RFC 3621, associated with the given port on the local system.
Local Max Frame	PortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
	MaxFrameSize	An integer value that indicates the maximum supported frame size in octets on the given port of the local system.

Related Links

802.1ab Port dot3 tables on page 352

Link table

The following table describes the 802.1ab Port dot3 Link table.

Table 119: Local Link aggregate table

Part	Details
PortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
LinkAggStatus	The bitmap value contains the link aggregation capabilities and the current aggregation status of the link.
LinkAggPortId	Contains the IEEE 802.3 aggregated port identifier, aAggPortID (IEEE 802.3-2002, 30.7.2.1.1), derived from the ifNumber of the ifIndex for the port component in link aggregation.

Related Links

802.1ab Port dot3 tables on page 352

802.1ab Port med tables

Port med tables are presented in the content pane after you select the device node in the 802.1ab, Port med folder in the navigation tree.

You can configure the 802.1ab Port med parameters on the following devices:

- ERS 55xx v5.0.0 and above
- ERS 8300 v3.0 and above
- VSP 7000 v10.2 and above
- ERS 35xx v.5.1 and above
- ERS 4000 v5.6 and above

The following sections list and describe the 802.1ab Port med tables.

Related Links

Management of Auto Detection and Auto Configuration on the Avaya Switch on page 336
Policy table on page 355
Location table on page 356
PoE PSE table on page 356
Capabilities table on page 357
Inventory table on page 357

Policy table

The following table describes the Policy table.

Table 120: Policy table

Table	Details	
Local Policy	PortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
	PolicyVlanID	An extension of the VLAN Identifier for the port, as defined in IEEE 802.1P-1998. A value of 1 through 4094 defines a valid PVID.
	PolicyPriority	Contains the value of the 802.1p priority, which is associated with the given port on the local system.
	PolicyDscp	Contains the value of the Differentiated Service Code Point (DSCP), as defined in IETF RFC 2474 and RFC 2475, which is associated with the given port on the local system.
	PolicyUnknown	Indicates whether or not the network policy for the specified application type is currently unknown. The values are: • True (1)—indicates that the network policy for the specified application type is currently unknown. • False (2)—indicates that the network policy is defined. If the value is True (1), COM ignores the VLAN ID, the layer 2 priority, and the DSCP value fields.
	PolicyTagged	Indicates whether or not the application is using a tagged VLAN. The values are: • True (1)—indicates that it is using a tagged VLAN. • False (2)—indicates that for the specific application the device either is using an untagged VLAN, or does not support port based VLAN operation. If the value is False (2), COM ignores the VLAN ID and the Layer 2 priority fields, and only the DSCP value has relevance.
Local Location	PortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
	LocationSubtype	The location subtype advertised by the local device.
	LocationInfo	The location information. Parsing of the location information is dependent upon the location subtype, as defined by the value of the LocationSubtype.

Related Links

802.1ab Port med tables on page 354

Location table

The following table describes the Location table.

Table 121: Location table

Part	Details
PortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
LocationSubtype	The location subtype advertised by the local device.
LocationInfo	The location information. Parsing of the location information is dependent upon the location subtype, as defined by the value of the LocationSubtype.

Related Links

802.1ab Port med tables on page 354

PoE PSE table

The following table describes the PoE PSE table.

Table 122: PoE PSE table

Part	Details
PortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
PSEPortPowerAv	Contains the value of the power available from the PSE from this port, expressed in units of 0.1 watts.
PSEPortPDPriority	Reflects the PD power priority that is advertised on this PSE port. The values are: • unknown - 1 • critical - 2 • high - 3 • low - 4

Related Links

802.1ab Port med tables on page 354

Capabilities table

The following table describes the Capabilities table.

Table 123: Capabilities table

Part	Details
TimeMark	A TimeFilter for this entry. For more information, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry. The lldpRemLocalPortNum identifies the port on which the remote system information is received.
Index	Represents an arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated remote system.
CapSupported	A bitmap value that includes the MED organizationally defined set of LLDP TLVs that can transmit on the LLDP agent of the remote device connected to the port. Each bit in the bitmap corresponds to an LLDP-MED subtype associated with a specific TIA TR41.4 MED optional TLV. If the bit is set, the agent has the capability to support the corresponding TLV.
CapCurrent	A bitmap value that includes the MED organizationally defined set of LLDP TLVs that can transmit on the LLDP agent of the remote device connected to this port. Each bit in the bitmap corresponds to an LLDP-MED subtype associated with a specific TIA TR41.4 MED optional TLV. If the bit is set, the agent currently supports the corresponding TLV.
DeviceClass	Device Class as advertised by the device remotely connected to the port.

Related Links

802.1ab Port med tables on page 354

Inventory table

The following table describes the Inventory table.

Table 124: Inventory table

Part	Details
TimeMark	A TimeFilter for the entry. For more information, see the TimeFilter textual convention in IETF RFC 2021.
LocalPortNum	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry. LocalPortNum identifies the port on which the remote system information is received.

Part	Details
Index	Represents an arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated remote system.
HardwareRev	The vendor-specific hardware revision string as advertised by the remote endpoint.
FirmwareRev	The vendor-specific firmware revision string as advertised by the remote endpoint.
SoftwareRev	The vendor-specific software revision string as advertised by the remote endpoint.
SerialNum	The vendor-specific serial number as advertised by the remote endpoint.
MfgName	The vendor-specific manufacturer name as advertised by the remote endpoint.
ModelName	The vendor-specific model name as advertised by the remote endpoint.
AssetID	The vendor-specific asset tracking identifier as advertised by the remote endpoint.

Related Links

802.1ab Port med tables on page 354

Chapter 14: Inventory Manager

With the Inventory Manager you can manage the hardware and software configurations for different devices. Use the Inventory Manager to perform the following actions.

- 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

About the Inventory Manager

Inventory Manager has two primary functions—file management and inventory management. This section describes the capabilities provided by those functions.

File management features

The file management features of 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 Inventory Manager to perform 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 Inventory Manager.

Table 125: Inventory Manager file management capabilities

Device family	Operation	Multiple devices	File types
ERS 8000 VSP 9xxx VSP 7xxx VSP 4xxx v3.1 VSP 8xxx	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
	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

Device family	Operation	Multiple devices	File types
	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* * 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

Device family	Operation	Multiple devices	File types
	Restore	Yes	Configuration
	Archive	Yes	Configuration
	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 the 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 the Inventory Manager

Perform the following procedure to start the Inventory Manager.

- The administrator must assign the Inventory Manager in the MultiElementManager Assignment tab.

Procedure steps

1. Select **Devices** from **Configuration and Orchestration Manager**, and then click the **Inventory Manager** iIcon.

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**, the 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 **Inventory Manager** dialog box appears.

   Important:

   Discovery process does not include devices without proper credentials assigned to them.

Using the Inventory Manager window

The following figure shows the Inventory Manager window.

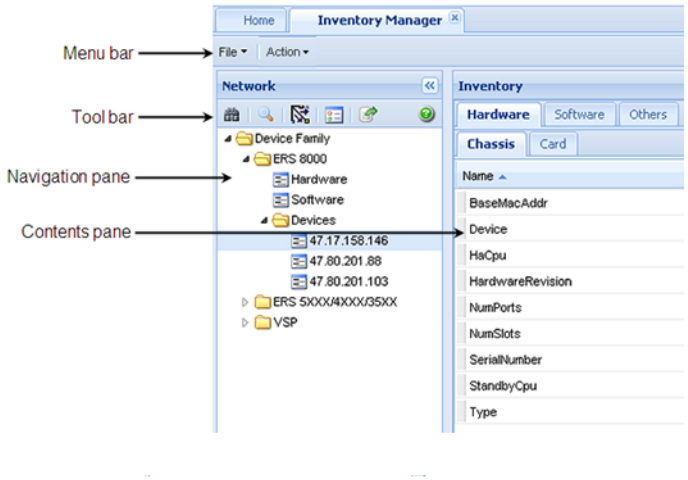


Figure 14: Inventory Manager window

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

Table 126: Parts of the Inventory Manager window

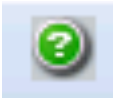
Part	Description
Menu bar	Provides access to all Inventory commands. For more information, see Menu bar commands on page 364.
Tool bar	Provides quick access to commonly used Inventory commands. For more information, see Tool bar commands on page 364.

Part	Description
Navigation pane	Allows you to navigate Inventory elements for devices discovered on the network. For more information, see Navigation pane on page 365.
Contents pane	Displays file and inventory information for the element selected on the Navigation pane. For more information, see Contents pane on page 367.

Tool bar commands

The following table describes the Inventory Manager tool bar commands.

Table 127: Inventory Manager tool bar commands

Command	Tool bar button	Description
Reload / Discover		Rediscovers the inventory information and reloads the Inventory Manager with the latest information.
Find		Finds matching text strings in the navigation or contents panes.
Highlight on topology		Highlights devices of the selected family on the Configuration and Orchestration Manager topology map.
Preferences		Filters devices based on Family or Capabilities.
Export		Exports inventory information displayed in content panel grid in to a text file.
Help		Opens online Help for the current folder or tab.

Menu bar commands

The following table describes the Inventory Manager menu bar commands for the File menu and the Action menu.

Table 128: Inventory Manager menu bar commands for the File menu and the Action menu

Command	Menu	Description
Reload	File	Use to reload the manager from the Device Inventory View.
Save Inventory Info	File	Use to save inventory files that you can load again later.
Open Inventory File	File	Use to load saved inventory files.
Save Inventory in tab delimited text file	File	Use to save network inventory information in a tab-delimited text file.
Download file to Device(s)	Action	Use to download configuration or image files or both to devices.
Upload file from Device(s)	Action	Use to upload configuration or image files or both from devices.
Backup Config File	Action	Use to create backup files that can be restored to devices in the event of a network.
Save Backed Up Config Files to Local	Action	Use to view, download, or copy files from the COM server to your local desktop or PC. The backup files are always on the COM server. From a remote browser connection you can view the device files, or copy the device files locally.
Restore Config File	Action	Use to restore the configuration for the target device(s).
Archive Config File	Action	Use to archive the configuration for the target device(s).
Synchronize Config File	Action	Use to synchronize the configuration for the target device(s).
Device Upgrade	Action	Use to update the software for the specified device(s).
Device Upgrade Wizard	Action	Displays the Auto Upgrade form.
Compare Runtime Config With Existing Config	Action	Use to compare the runtime configuration for the specified device(s) with the external configuration file.

Navigation pane

The Inventory Manager Navigation pane enables you to navigate file and 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.

The following is an example of the Inventory Manager Navigation pane.

Figure 15: Parts of the Inventory Manager Navigation pane

The following table describes the Navigation pane. The Navigation pane shows only the device families that are available in COM.

Table 129: 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 folder	Displays the information specific to ERS 8xxx devices.
ERS 5XXX/4XXX/35XX folder	Displays the information specific to ERS 5xxxx, 4xxxx, and 35xx devices.
Legacy ERS 1424/16xx folder	Displays the information specific to ERS 1424 and 16xx devices.
VSP folder	Displays the following subfolders: • VSP7024XLS — Displays the information specific to VSP 7024XLS devices. • VSP9012 — Displays the information specific to VSP 9012 devices. • VSP4000 — Displays the information specific to VSP 4000 devices. • VSP8000 — Displays the information specific to VSP 8000 devices.
Legacy BayStack folder	Displays the information specific to legacy baystack.
ERS 16XX folder	Displays the information specific to ERS 16XX devices.
Ethernet Switch/ERS 25XX folder	Displays the information specific to Ethernet Switch and ERS 25XX devices.
Alteon folder	Displays the information specific to Alteon devices.
Passport 1000 folder	Displays the information specific to Passport 1000 devices.
WLAN AP folder	Displays the information specific to WLAN AP devices.
WC 8180 folder	Displays the information specific to WC 8180 devices.

Part	Description
Hardware	Displays all hardware information for the discovered devices.
Software	Displays all software information for the discovered devices.
Devices folder	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 Inventory Manager navigation tree

The following figure is an example of the Inventory Manager navigation tree. Depending on the devices that are discovered, the Inventory Manager window may show folders that are not listed here, and may not show folders that are listed.

Figure 16: Understanding the Inventory Manager navigation tree

The following sections describe the tab contents of Device Family folders.

ERS 5XXX/4XXX/35XX folder

Use the ERS 5XXX/4XXX/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 5XXX/4XXX/35XX folder.

Table 130: Parts of the ERS 5XXX/4XXX/35XX folder

Part	Description
ERS 5XXX/4XXX/35XX Hardware table on page 368	Shows information about Ethernet Routing Switch 5XXX, 4XXX, and 35XX device hardware in the network inventory.

Part	Description
ERS 5XXX/4XXX/35XX Software table on page 369	Shows information about software running on Ethernet Routing Switch 5XXX, 4XXX, and 35XX devices in the network inventory.
ERS 5XXX/4XXX/35XX Devices folder on page 370	Shows information about each of the Ethernet Routing Switch 5XXX, 4XXX, and 35XX devices discovered on the network.

ERS 5XXX/4XXX/35XX Hardware table

Use the ERS 5XXX/4XXX/35XX Hardware table to view information about Ethernet Routing Switch 5XXX, 4XXX, and 35XX device hardware in the network inventory.

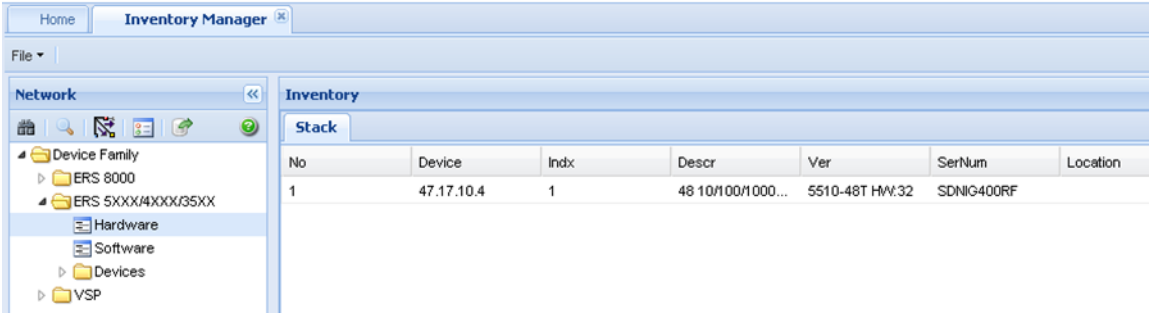
The following table describes the parts of the ERS 5XXX/4XXX/35XX Hardware table.

Table 131: Parts of the ERS 5XXX/4XXX/35XX Hardware table

Part	Description
Stack tab on page 368	Shows information about Ethernet Routing Switch 5XXX, 4XXX, and 35XX stack.

Stack tab

Use the Stack of the ERS 5XXX/4XXX/35XX folder to view information about Ethernet Routing Switch 5XXX, 4XXX, and 35XX stack.



The following table describes the parts of the Stack tab.

Table 132: Parts of the stack tab of the ERS 5XXX/4XXX/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.
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.

ERS 5XXX/4XXX/35XX Software table

Use the ERS 5XXX/4XXX/35XX Software table to view information about software running on Ethernet Routing Switch 5XXX, 4XXX, and 35XX devices in the network inventory.

The following table describes the parts of the ERS 5XXX/4XXX/35XX Software table.

Table 133: Parts of the ERS 5XXX/4XXX/35XX Software table

Part	Description
General tab on page 369	Shows general information about software running on Ethernet Routing Switch (legacy) 5XXX, 4XXX, and 35XX devices in the network inventory.
Image/Config tab on page 369	Shows information about software configuration settings.

General tab

Use the General tab of the ERS 5XXX/4XXX/35XX Software table on page 369 to view general information about the software running on Ethernet Routing Switch 5XXX, 4XXX, and 35XX devices.

The following table describes the parts of the General tab.

Table 134: Parts of the General tab of the ERS 5XXX/4XXX/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 5XXX/4XXX/35XX Software table on page 369 to view information about image and configuration files loaded on the Ethernet Routing Switch 5XXX, 4XXX, and 35XX devices.

The following table describes the parts of the Image/Config tab.

Table 135: Parts of the Image/Config tab of the ERS 5XXX/4XXX/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.

Part	Description
CfgFname	Shows the filename of the last configuration file downloaded to or uploaded from the device.

ERS 5XXX/4XXX/35XX Devices folder

Use the ERS 5XXX/4XXX/35XX Devices folder to view information about each of the Ethernet Routing Switch 5XXX, 4XXX, and 35XX devices discovered on the network.

For each device in the Devices folder, the Inventory Manager displays the following tabs in the contents pane

Table 136: Parts of the ERS 5XXX/4XXX/35XX Devices folder

Tab	Part	Description
Hardware tab	Stack tab on page 370	Shows information about Ethernet Routing Switch 5XXX, 4XXX, and 35XX stack.
	Gbic tab on page 371	Shows information about the system that Ethernet Routing Switch 5XXX, 4XXX, and 35XX use to determine the device capabilities.
Software tab	General tab on page 371	Shows general information about software running on Ethernet Routing Switch 5XXX, 4XXX, and 35XX devices in the network inventory.
	Image/Config tab on page 371	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.

Stack tab

Use the Stack tab of the ERS 5XXX/4XXX/35XX Devices folder on page 370 to view information about Ethernet Routing Switch 5XXX, 4XXX, and 35XX Stack.

The following table describes the parts of the Stack tab.

Table 137: Parts of the stack tab of the ERS 5XXX/4XXX/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	Shows the location of the device.

Gbic tab

Use the Gbic tab of the ERS 5XXX/4XXX/35XX Devices folder on page 370 to view information about the system that Ethernet Routing Switch 5XXX, 4XXX, and 35XX use to determine the device capabilities.

The following table describes the parts of the Gbic tab.

Table 138: Parts of the Gbic tab of the ERS 5XXX/4XXX/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.
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 5XXX/4XXX/35XX Devices folder on page 370 to view general information about the selected Ethernet Routing Switch 5XXX, 4XXX, and 35XX device.

The following table describes the parts of the General tab.

Table 139: Parts of the General tab of the Devices folder

Part	Description
Contact	Shows the administrative contact for the device.
Description	Shows a description of the device.
Device	Shows the IP address of the device.
Location	Shows the location of the device.
SysName	Shows the system name of the device.
Type	Shows the type of 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 5XXX/4XXX/35XX Devices folder on page 370 to view information about image and configuration files loaded on the device.

The following table describes the parts of the Image/Config tab.

Table 140: Parts of the Image/Config tab of the ERS 5XXX/4XXX/35XX Devices folder

Part	Description
CfgFname	Shows the filename of the last configuration file downloaded to or uploaded from the device.
Device	Shows the IP address of the device.
ImgFname	Shows the filename of the last image or firmware file downloaded to the device.

ERS 8000 folder

Use the ERS 8000 folder to view information about Ethernet Routing Switch 8000 hardware, software, and devices in the network inventory.

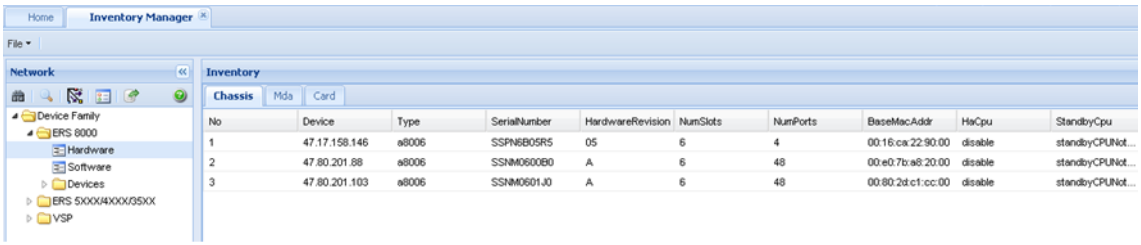
The following table describes the parts of the ERS 8000 folder.

Table 141: Parts of the ERS 8000 folder

Part	Description
ERS 8000 Hardware table on page 372	Shows information about Ethernet Routing Switch 8000 device hardware in the network inventory.
ERS 8000 Software table on page 375	Shows information about software running on Ethernet Routing Switch 8000 devices in the network inventory.
ERS 8000 Devices folder on page 376	Shows information about each of the Ethernet Routing Switch 8000 devices discovered on the network.

ERS 8000 Hardware table

Use the ERS 8000 Hardware table to view information about Ethernet Routing Switch 8000 device hardware in the network inventory.



The following table describes the parts of the ERS 8000 Hardware table.

Table 142: Parts of the ERS 8000 Hardware table

Part	Description
Chassis tab on page 373	Shows information about Ethernet Routing Switch 8000 family chassis.
Mda tab on page 373	Shows information about MDAs installed in Ethernet Routing Switch 8000 family chassis.

Part	Description
Card tab on page 374	Shows information about cards installed in Ethernet Routing Switch 8000 family chassis.

Chassis tab

Use the Chassis tab of the ERS 8000 Hardware table on page 372 to view information about Ethernet Routing Switch 8000 family chassis.

The following table describes the parts of the Chassis tab.

Table 143: Parts of the Chassis tab of the ERS 8000 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: • hotStandbyCPU • warmStandbyCPU • standbyCPUNotPresent

Mda tab

Use the Mda tab of the ERS 8000 Hardware table on page 372 to view information about MDA installed in Ethernet Routing Switch 8000 family devices in the network inventory.

The following table describes the parts of the Mda tab.

Table 144: Parts of the Mda tab of the ERS 8000 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.

Part	Description
Description	Shows the MDA description. Possible values include: • OC-3c SMF MDA—Dual port OC-3c SMF • OC-3c MMF MDA—Dual port OC-3c MMF • OC-12c SMF MDA—Single Port OC-12c SMF • OC-12c MMF MDA—Single Port OC-12c MMF
NumPorts	Shows the number of ports on the MDA.

Card tab

Use the Card tab of the ERS 8000 Hardware table on page 372 to view information about cards installed in Ethernet Routing Switch 8000 series chassis.

The following table describes the parts of the Card tab.

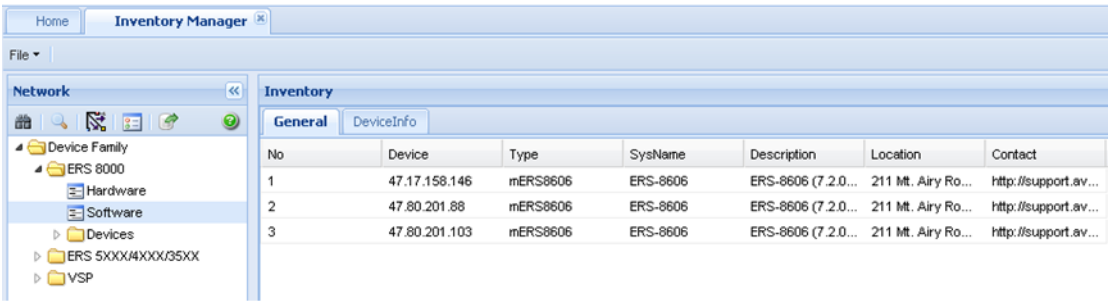
Table 145: Parts of the Card tab of the ERS 8000 Hardware table

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 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: • rc2kBackplane • rc2kSFM • rc2kBFM0 • rc2kBFM2 • rc2kBFM3 • rc2kBFM6 • rc2kBFM8 • rc2kMGSFM • other
BackDescription	Shows the back description for the card.

Part	Description
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.

ERS 8000 Software table

Use the ERS 8000 Software table to view information about software running on Ethernet Routing Switch 8000 devices in the network inventory.



The following table describes the parts of the ERS 8000 Software table.

Table 146: Parts of the ERS 8000 Software table

Part	Description
General tab on page 375	Shows general information about software running on Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices in the network inventory.
DeviceInfo tab on page 376	Shows information about the device.

General tab

Use the General tab of the ERS 8000 Software table on page 375 to view general information about software running on Ethernet Routing Switch 8000 family devices on the network.

The following table describes the parts of the General tab.

Table 147: Parts of the General tab of the ERS 8000 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.

Part	Description
Contact	Shows the administrative contact for the device.

DeviceInfo tab

Use the DeviceInfo tab of the ERS 8000 Software table on page 375 to view information about the device in the Ethernet Routing Switch 8000 family chassis.

The following table describes the parts of the DeviceInfo tab.

Table 148: Parts of the DeviceInfo tab of the ERS 8000 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.
FlashBytesFree	Shows the number of bytes available in the system configuration flash device.
FlashNumFiles	Shows the number of files available in the system configuration flash device.
PcmciaBytesUsed	Shows the number of bytes used by pcmcia device in the system.
PcmciaBytesFree	Shows the number of bytes available in the system pcmcia device.
PcmciaNumFiles	Shows the number of files available in the system pcmcia device.

ERS 8000 Devices folder

Use the ERS 8000 Devices folder to view information about the Ethernet Routing Switch 8000 devices discovered on the network.

The following table describes the parts of the ERS 8000 Devices folder.

Table 149: Parts of the ERS 8000 Devices folder

Tab	Part	Description
Hardware	Chassis tab on page 376	Shows information about the Ethernet Routing Switch 8000 family chassis.
	Card tab on page 377	Shows information about cards installed in the Ethernet Routing Switch 8000 series chassis.
Software	General tab on page 378	Shows general information about software running on Ethernet Routing Switch 8000 family devices in the network inventory.
Others	PcmciaFiles tab on page 378	Shows information about the PcmciaFiles.

Chassis tab

Use the Chassis tab of the ERS 8000 Devices folder on page 376 to view information about the Ethernet Routing Switch 8000 device chassis.

The following table describes the parts of the Chassis tab.

Table 150: Parts of the Chassis tab of the ERS 8000 Devices folder

Part	Description
BaseMacAddr	Shows the starting point of the block of MAC addresses used by the switch for logical and physical interfaces.
Device	Shows the IP address or host name for the device.
HaCpu	Shows you whether the L2 redundancy on the master CPU is enabled or disabled.
HardwareRevision	Shows the current hardware revision of the device chassis.
NumPorts	Shows the number of ports currently on this device.
NumSlots	Shows the number of slots (or cards) this device can contain.
SerialNumber	Shows the serial number for the device.
Type	Shows you whether the L2 Redundancy is enabled on the standby CPU. The possible states are: • hotStandbyCPU • warmStandbyCPU • standbyCPUNotPresent
StandbyCpu	Shows the module type.

Card tab

Use the Card tab of the ERS 8000 Devices folder on page 376 to view information about cards installed in Ethernet Routing Switch 8000 series chassis.

The following table describes the parts of the Card tab.

Table 151: Parts of the Card tab of the ERS 8000 Devices folder

Part	Description
No	Shows the row number of the table entry.
Device	Shows the IP address or host name for the device.
SlotNum	Shows the slot numbers of cards installed in the chassis.
FrontType	Indicates the card types in Ethernet Routing Switch 8000 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 • rc2kBackplane

Part	Description
	• rc2kSFM • rc2kBFM0 • rc2kBFM2 • rc2kBFM3 • rc2kBFM6 • rc2kBFM8 • rc2kMGSFM • 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.

General tab

Use the General tab of the ERS 8000 Devices folder on page 376 to view general information about software running on Ethernet Routing Switch 8000 family devices on the network.

The following table describes the parts of the General tab.

Table 152: Parts of the General tab of the ERS 8000 Devices folder

Part	Description
Contact	Shows the administrative contact for the device.
Description	Shows a description of the device.
Device	Shows the IP address or host name for the device.
Location	Shows the location of the device.
SysName	Shows the system name of the device.
Type	Shows the type of the device.
UpTime	Shows the elapsed time since the last restart of the device.

PcmciaFiles tab

Use the PmciaFiles tab of the ERS 8000 Devices folder on page 376 to view pcmcia file information of the selected Ethernet Routing Switch 8000 device.

The following table describes the parts of the PcmciaFiles tab.

Table 153: Parts of the PcmciaFiles tab of the ERS 8000 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.

VSP folder

The VSP folder contains information about hardware, software, and devices in the network inventory for Virtual Services Platform (VSP) 9xxx, VSP 7xxxx, VSP 8xxx, and VSP 4xxx.

VSP 9XXX folder

Use the VSP 9XXX folder to view information about Virtual Services Platform (VSP) 9XXX hardware, software, and devices in the network inventory.

The following table describes the parts of the VSP 9XXX folder.

Table 154: Parts of the VSP 9XXX folder

Part	Description
VSP 9XXX Hardware table on page 379	Shows information about Virtual Services Platform 9XXX device hardware in the network inventory.
VSP 9XXX Software table on page 381	Shows information about software running on Virtual Services Platform 9XXX devices in the network inventory.
VSP 9XXX Devices folder on page 382	Shows information about each of the Virtual Services Platform 9XXX devices discovered on the network.

VSP 9XXX Hardware table

Use the VSP 9XXX Hardware table to view information about Virtual Services Platform 9XXX device hardware in the network inventory.

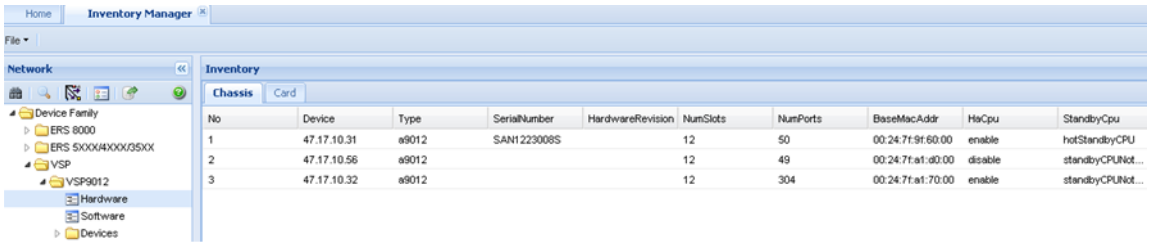


Figure 17: Example of the Inventory Manager VSP 9XXX hardware table

The following table describes the parts of the VSP 9XXX Hardware table.

Table 155: Parts of the VSP 9XXX Hardware table

Part	Description
Chassis tab on page 384	Shows information about the Virtual Services Platform 9XXX family chassis.
Card tab on page 380	Shows information about cards installed in the Virtual Services Platform 9XXX family chassis.

Card tab

Use the Card tab of the VSP 9XXX Hardware table to view information about cards installed in the Virtual Services Platform 9XXX series chassis.

The following table describes the parts of the Card tab.

Table 156: Parts of the Card tab of the 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 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: • rc2kBackplane • rc2kSFM • rc2kBFM0 • rc2kBFM2 • rc2kBFM3 • rc2kBFM6 • rc2kBFM8 • rc2kMGSFM • other
BackDescription	Shows the back description for the card.
BackSerialNum	Shows the back serial number for the card.

Part	Description
BackHwVersion	Shows the back hardware version for the card.
BackPartNumber	Shows the back part number for the card.
BlackDateCode	Shows the back date code for the card.
BackDeviations	Shows the back deviations for the card.

VSP 9XXX Software table

Use the VSP 9XXX Software table to view information about software running on the Virtual Services Platform 9XXX devices in the network inventory.

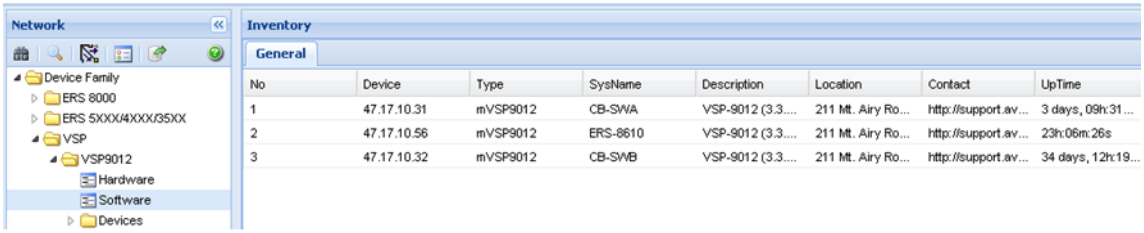


Figure 18: Example of the VSP 9XXX Software table

The following table describes the parts of the VSP 9XXX Software table.

Table 157: Parts of the VSP 9XXX Software table

Part	Description
General tab on page 381	Shows general information about software running on Virtual Services Platform 9XXX family devices in the network inventory.

General tab

Use the General tab of VSP 9XXX Software table to view general information about software running on Virtual Services Platform 9XXX family devices on the network.

Table 158: Parts of the General tab of the 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.
UpTime	Shows the elapsed time since the last restart of the device.

VSP 9XXX Devices folder

Use the VSP 9XXX Devices folder to view information about Virtual Services Platform 9XXX devices discovered on the network.

The following table describes the parts of the VSP 9XXX Devices folder.

Table 159: Parts of the VSP 9XXX Devices folder

Tab	Part	Description
Hardware	Chassis tab on page 382	Shows information about the Virtual Services Platform 9XXX family chassis.
	Card tab on page 383	Shows information about cards installed in the Virtual Services Platform 9XXX series chassis.
Software	General tab on page 384	Shows general information about software running on Virtual Services Platform 9XXX family devices in the network inventory.
Others	FlashFiles tab on page 385	Shows information about the files in the flash memory of Virtual Services Platform 9XXX family devices.

Chassis tab

Use the Chassis tab of the VSP 9XXX Devices folder to view information about the Virtual Services Platform 9XXX device chassis.

The following table describes the parts of the Chassis tab.

Table 160: Parts of the Chassis tab of the VSP 9XXX Devices folder

Part	Description
BaseMacAddr	Shows the starting point of the block of MAC addresses used by the switch for logical and physical interfaces.
Device	Shows the IP address or host name of the device.
HaCpu	Shows you whether the L2 redundancy on the master CPU is enabled or disabled.
HardwareRevision	Shows the current hardware revision of the device chassis.
NumPorts	Shows the number of ports currently on this device.
NumSlots	Shows the number of slots (or cards) this device can contain.
SerialNumber	Shows the serial number for the device.
StandbyCpu	Shows you whether the L2 Redundancy is enabled on the standby CPU. The possible states are: • hotStandbyCPU • warmStandbyCPU • standbyCPUNotPresent
Type	Shows the module type.

Card tab

Use the Card tab of the VSP 9XXX Devices folder to view information about cards installed in the Virtual Services Platform 9XXX series chassis.

The following table describes the parts of the Card tab.

Table 161: Parts of the Card tab of the 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.
SlotNum	Shows the slot numbers of cards installed in the chassis.
FrontType	Indicates the card types in 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: • rc2kBackplane • rc2kSFM • rc2kBFM0 • rc2kBFM2 • rc2kBFM3 • rc2kBFM6 • rc2kBFM8 • rc2kMGSFM • 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.

General tab

Use the General tab of the VSP 9XXX Devices folder to view general information about software running on Virtual Services Platform 9XXX family devices on the network.

The following table describes the parts of the General tab.

Table 162: Parts of the General tab of the VSP 9XXX Devices folder

Part	Description
Contact	Shows the administrative contact for the device.
Description	Shows a description of the device.
Device	Shows the device.
Location	Shows the location of the device.
SysName	Shows the system name of the device.
Type	Shows the type of the device.
UpTime	Shows the elapsed time since the last restart of the device.

Chassis tab

Use the Chassis tab of VSP 9XXX Hardware table to view information about the Virtual Services Platform 9XXX family chassis.

The following tables describes the parts of the Chassis tab.

Table 163: Parts of the Chassis tab of the 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.
HardwareRevision	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: • hotStandbyCPU • warmStandbyCPU • standbyCPUNotPresent

FlashFiles tab

Use the FlashFiles tab of the VSP 9XXX Devices folder to view information about the files in the flash memory of the selected Virtual Services Platform 9XXX device.

The following table describes the parts of the Flash Files tab.

Table 164: Parts of the FlashFiles tab of the 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.

VSP7XXX folder

Use the VSP7XXX folder to view information about Virtual Services Platform (VSP) 7XXX hardware, software, and devices in the network inventory.

The following table describes the parts of the VSP7XXX folder.

Table 165: Parts of the VSP7XXX folder

Part	Description
VSP 7XXX Hardware table on page 385	Shows information about VSP 7XXX device hardware in the network inventory.
VSP 7XXX Software table on page 387	Shows information about software running on VSP 7XXX devices in the network inventory.
VSP 7XXX Devices folder on page 388	Shows information about each of the VSP 7XXX devices discovered on the network.

VSP 7XXX Hardware table

Use the following VSP 7XXX Hardware table to view information about VSP 7XXX device hardware in the network inventory.

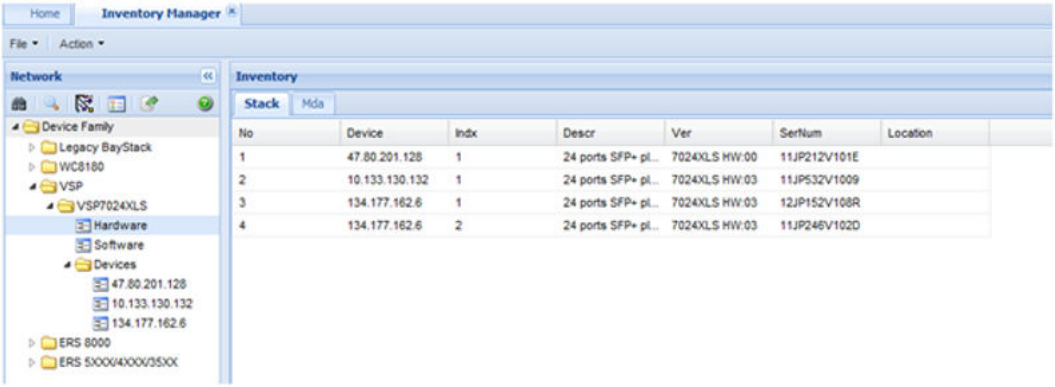


Figure 19: Example of the VSP 7XXX Hardware table

Table 166: Parts of the VSP 7XXX Hardware table

Part	Description
Stack tab on page 386	Shows information about the Virtual Services Platform 7XXX stacks.
Mda tab on page 386	Shows information about the Virtual Services Platform 7XXX Mda.

Stack tab

Use the Stack tab of the VSP 7XXX Devices folder to view information about the stacks.

The following table describes the parts of the Stack tab.

Table 167: Parts of the Stack tab of the VSP 7XXX 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 a description of the device.
Ver	Shows the version number of the device.
SerNum	Shows the serial number for the device.
Location	Shows the location of the device.

Mda tab

The following table describes the parts of the Mda tab.

Table 168: Parts of the Mda tab of the VSP 7XXX Devices folder

Part	Description
No	Shows the row number of the table entry.

Part	Description
Device	Shows the IP address or host name for the device.
Indx	Shows the index number of the device.
Descr	Shows a description of the device.

VSP7XXX Software table

Use the VSP7XXX Software table to view information about software running on the Virtual Services Platform 7XXX devices in the network inventory.

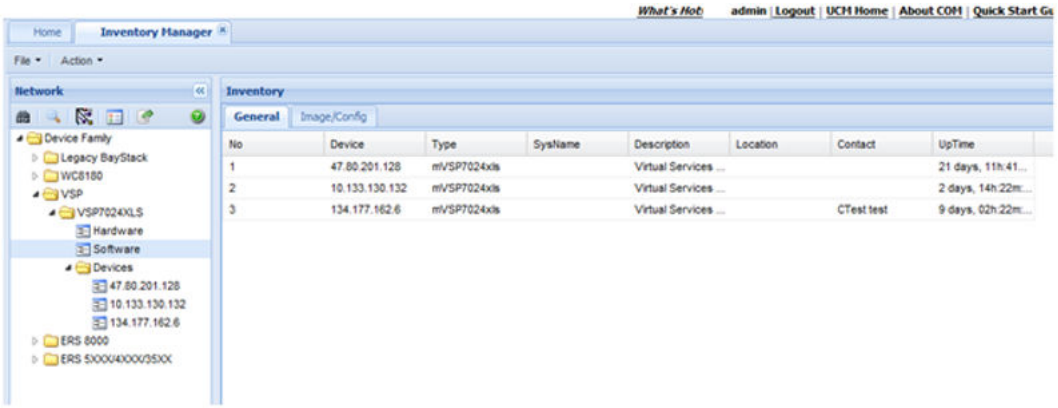


Figure 20: Example of the VSP 7XXX Software table

The following table describes the parts of the VSP 7XXX Software table.

Table 169: Parts of the VSP 7XXX Software table

Part	Description
General Tab on page 387	Shows general information about software running on Virtual Services Platform 7XXX family devices in the network inventory.
Image Config Tab on page 388	Shows information about image and configuration files loaded on VSP 7XXX devices in the network inventory.

General tab

Use the General tab of the VSP 7XXX Software table to view general information about software running on the VSP 7XXX family of devices on the network.

Table 170: Parts of the General tab of the VSP 7XXX 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.

Part	Description
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 VSP 7XXX Software table to view information about image and configuration files loaded on VSP 7XXX devices.

The following table describes the parts of the VSP 7XXX Software table Image/Config tab.

Table 171: Parts of the Image/Config tab of the VSP 7XXX 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.

VSP 7XXX Devices folder

Use the VSP 7XXX Devices folder to view information about Virtual Services Platform 7XXX devices discovered on the network.

For each device in the Devices folder, the Inventory Manager displays the following tabs in the Contents pane.

Table 172: Parts of the VSP 7XXX Devices folder

Tab	Part	Description
Hardware Tab	Stack tab on page 386	Shows information about the VSP 7XXX stack.
	Mda tab on page 386	Shows information about MDA installed in VSP 7XXX devices.
Software tab	General Tab on page 387	Shows general information about software running on VSP 7XXX devices in the network inventory.
	Image Config Tab on page 388	Shows information about software configuration settings.

Important:

The Contents pane displays the tabs described in the preceding table only after you select a device from the device folder.

Setting Inventory Manager preferences

You can set preferences for displaying and managing devices on the Inventory Manager. This section contains information about setting the following preferences:

- Setting device management preferences on page 389

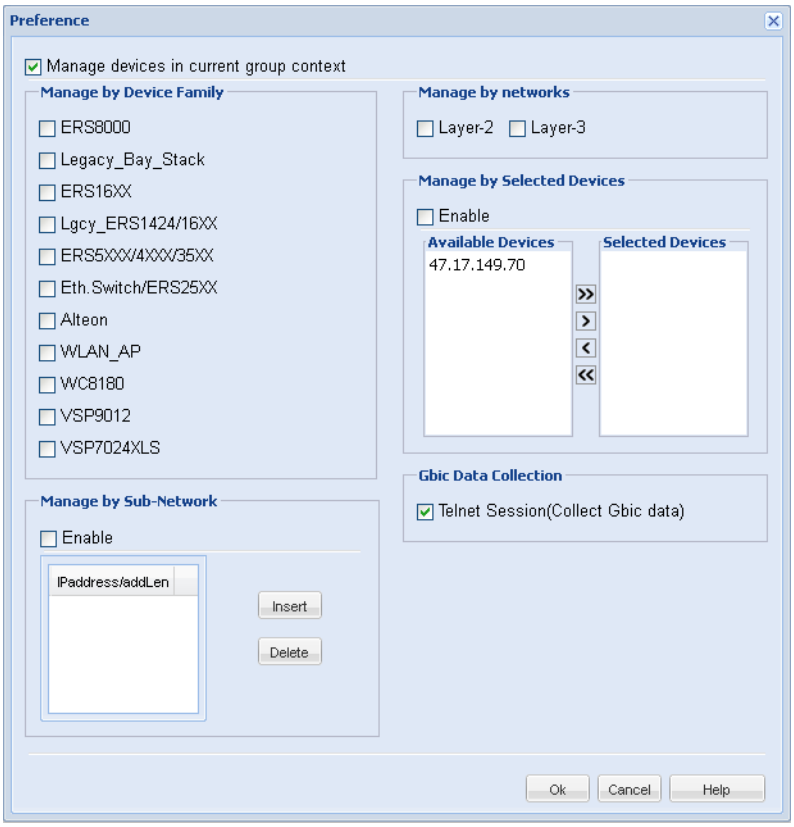
Setting device management preferences

Perform the following procedure to set the preferences for managing devices using the Inventory Manager.

Procedure steps

1. Open the 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: ERS8000, Legacy_Bay_Stack, ERS16XX, Lgcy_ERS1424/16XX, ERS5XXX/4XXX/35XX, Eth. Switch /ERS25XX, Alteon, WLAN_AP, WC8180, VSP9012, and VSP7024XLS.

- **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 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.

Chapter 15: Management of Traps and Logs

This chapter describes how to manage traps and logs in your network.

Configuration of Audit log

All the managers including Topology and Discovery send log messages to audit and debug logs.

The following sections contain information about how to configure and use the audit log feature.

Launching the audit log

Perform the following procedure to start the audit log.

Procedure steps

1. From the Navigation pane, expand the Admin panel.
2. Click the **Audit Log** icon.

   The Audit Log window displays the audit log listings.

Audit Log Report Viewer tabs

The following table describes the Audit Log Report Viewer tabs.

Table 173: Audit Log Report Viewer tabs

Tab	Description
Date Time	The date and time at which the event occurred.
Audit Level	The audit level of the audit message, for example INFO, ERROR, or WARNING.
User	The COM user name.
Access Type	The type of access to the device, for example read or write.
Source	The module name from which the log messages originate, for example, MultiLink Trunking Manager, Multicast Manager, Multimedia Manager, Routing Manager, Security Manager, Trap/Log Inventory, VLAN Manager, VPN Manager, Virtual Routing Manager, BCM, and COM.

Tab	Description
Device IP	The corresponding IP address of the device.
Message	The audit message.

Audit log management

This section provides information about audit log management.

Exporting audit logs

Perform the following procedure to export the audit logs.

Procedure steps

1. From the Navigation pane, expand the Admin panel, and then click **Audit Log**.

   The Audit Log dialog box appears.
2. Click **Export**.

   The Export drop-down menu appears.
3. Select the **Export to CSV** or **Export to TXT**.

   The File Download dialog box appears.
4. Click **Save** .

   The Save As dialog box appears.
5. In the Save in field, browse to the directory where you want to save the audit log file.
6. In the File name field, type a name for the audit log file.
7. Click **Save**.

Filtering audit logs

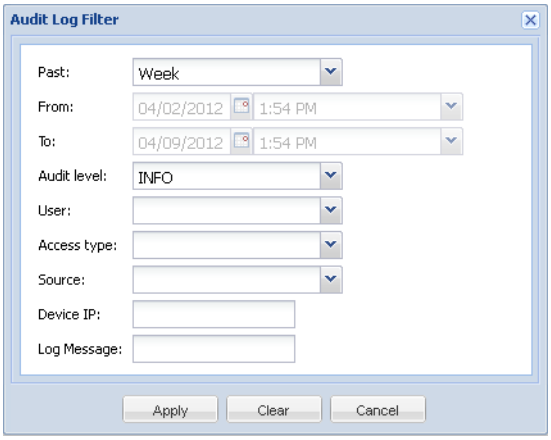
Perform the following procedure to filter audit logs.

Procedure steps

1. From the Navigation pane, expand the Admin panel, and then click **Audit Log**.

   The Audit Log dialog box appears.
2. Click **Show Filter**.

   The Audit Log Filter dialog box appears.



3. Enter all the fields in the Audit Log Filter dialog box as appropriate.
4. Click **Apply** to commit the changes or click **Cancel** to discard the changes.

   The audit log data displays according to the selected filters.

Audit Log Filter dialog box fields

The following table describes the fields of the Audit Log Filter dialog box.

Table 174: Audit Log Filter dialog box fields

Field	Description
Past	Specifies the duration for which audit log messages are fetched. Settings are: Hour, Day, Week, Month, and Specific.
From Date	Specifies the start date for fetching audit log messages. This setting is enabled when the Past field is set to Specific.
From Time	Specifies the start time for fetching audit log messages. This setting is enabled when the Past field is set to Specific.
To Date	Specifies the end date for fetching audit log messages. This setting is enabled when the Past field is set to Specific.
To Time	Specifies the end time for fetching audit log messages. This setting is enabled when the Past field is set to Specific.
Audit level	Specifies the type of audit level to be filtered.
User	Specifies the user name to be used for filtering data.
Access type	Specifies the access type to be filtered.
Source	Specifies the source or module from which to fetch audit log messages.
Device IP	Specifies the filter for log messages based on a device IP address.
Log Message	Specifies a filter based on audit log message contents.

Refreshing audit logs

Perform the following procedure to refresh the audit logs.

Procedure steps

1. From the Navigation pane, expand the Admin panel, and then click **Audit Log**.

   The Audit Log dialog box appears.

2. Click **Refresh**.

   The audit log details are refreshed.

Generating Audit Log reports

Perform the following procedure to generate audit log reports.

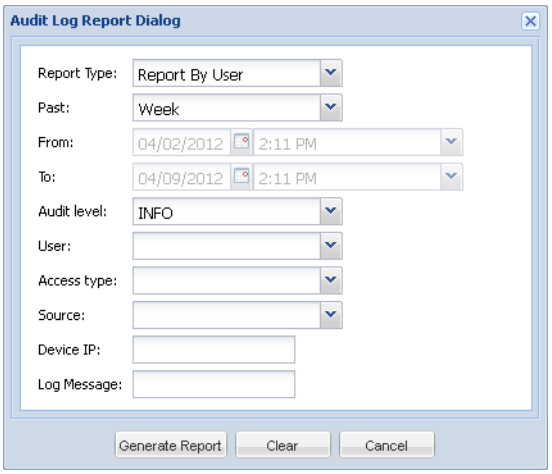
Procedure steps

1. From the Navigation pane, expand the Admin panel, and then click **Audit Log**.

   The Audit Log dialog box displays.

2. In the Audit Log dialog box, click the **Report** icon.

   The Audit Log Report Dialog box displays.



3. Select the required options in the Audit Log Report Dialog box.
4. Click **Generate Report**.

   The BIRT Report Viewer displays the generated report . The report can contain a maximum of 50 entries.

5. To navigate through the report, type a page number in the **Go to page** field, or click the forward and back buttons.

Next steps

After you generate an audit log report, you can perform the following actions from the Audit Log Report tool bar.

- Toggle table of contents—click to open or close the table of contents
- Run report—click to enter the parameters required to run the audit log report.
- Export data—click to export data from the audit log report in csv format.

- Export report—click to export the audit log report in Excel, postscript, PDF, Word, OpenDocument Presentation, OpenDocument Spreadsheet, OpenDocumen Text, or Power Point.
- Print report—click to print the audit log report in HTML or PDF format.
- Print report on the server—click to print the audit log report on the server.

Audit Log Report dialog box fields

The following table describes the fields of the Audit Log Report dialog box.

Table 175: Audit Log Report dialog box fields

Field	Description
Report Type	Specifies the type of report to be generated. The available reports are: • Report By User • Report By Device • Report By Date
Past	Specifies the time frame during which audit log messages are fetched. The available options are: • Hour • Day • Week • Month • Specific
From Date	Specifies the start date for audit log message collection. This field is enabled only if the Past field is set to Specific.
From Time	Specifies the start time for audit log message collection. This field is enabled only if the Past field is set to Specific.
To Date	Specifies the end date for audit log message collection. This field is enabled only if the Past field is set to Specific.
To Time	Specifies the end time for audit log message collection. This field is enabled only if the Past field is set to Specific.
Audit Level	Specifies the type of audit level to be filtered.
User	Filters the audit log messages by user.
Access type	Specifies the access type to be filtered.
Source	Specifies whether audit log messages are to be filtered by a specific source or module.
Device IP	Specifies whether audit log messages are to be filtered by a specific device IP address.

Field	Description
Log Message	Specifies whether audit log messages are to be filtered based on message contents.

Archiving audit logs

COM is configured by default to perform a database cleanup of audit log data every Sunday at 5:00 a.m. You can control the length of time audit logs are retained in the database by configuring the logging settings in the Preferences window. You can also configure the settings to archive the audit logs or to delete them permanently after they exceed the retention limit.

The archived files are saved in cvs format.

Procedure steps

1. From the Navigation pane, expand the Admin panel, and then click **Preferences**.

   The Preferences dialog box displays in the contents pane.

2. Click **Logging**.

   The Logging dialog box displays.

3. In the **Purge audit logs older than** field, select the retention limit for the audit logs by selecting the number of weeks or months in the combo boxes.

4. Select **Archive audit logs before purging to**.

   The audit logs are automatically saved to the following location.

   - For Windows: `C:/Avaya/SMGR/COM/log/Audit_Archives`
   - For Linux: `/opt/avaya/smgr/com/log/Audit_Archives`

5. Click **Archive audit logs now**

   A confirmation dialog box displays.

6. Click **OK**.

7. Click **Save Preferences**.

8. A dialog box displays indicating that the changes were saved.

9. Click **OK**.

Deleting audit logs

The COM application is configured by default to perform a database cleanup of audit log data every Sunday at 5:00 a.m. You can control the length of time audit logs are retained in the database by configuring the logging settings in the Preferences window. You can also configure the settings to permanently delete audit logs that have exceeded the retention limit.

Procedure steps

1. From the Navigation pane, expand the Admin panel and then click **Preferences**.

   The Preferences dialog box displays in the Contents pane.

2. Click the **Logging** tab.

The Logging dialog box displays.

3. In the **Purge audit logs older than** field, select the retention limit for the audit logs by selecting the number of weeks or months in the combo boxes.
4. Select **Delete Permanently**.
5. Click **Save Preferences**.

   A confirmation dialog box displays indicating that the changes were saved successfully.
6. Click **OK**.

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.

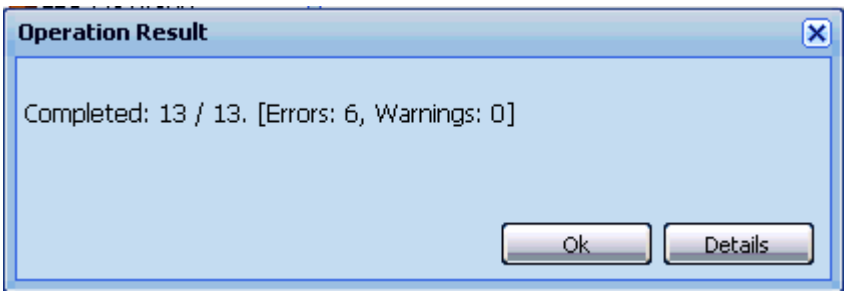
Starting Trap/Log Manager

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.

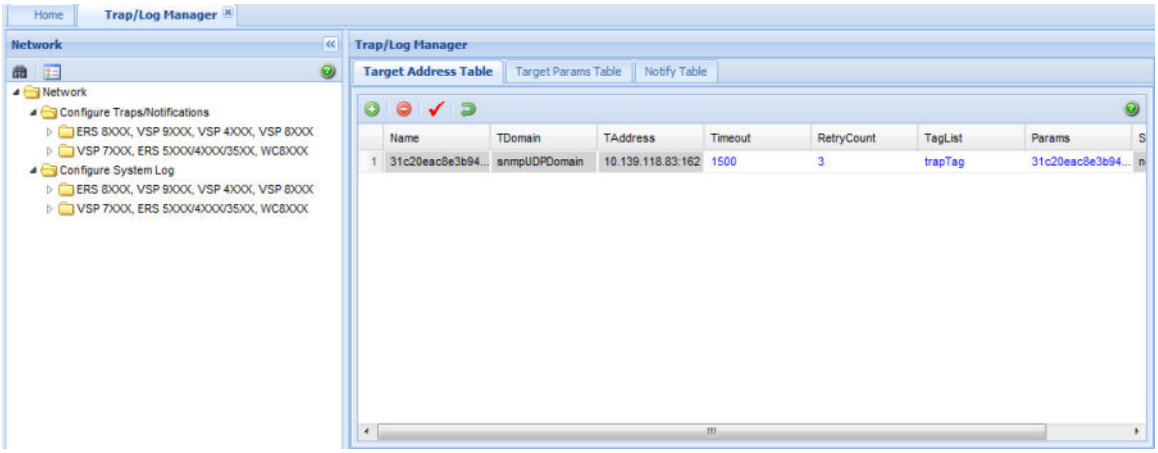
   OR

   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.



The following table describes the parts of the Trap/Log Manager window.

Table 176: 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 399.
Navigation pane	Allows you to navigate to the settings for the current network devices. For more information, see Navigation pane on page 399.
Contents pane	Displays details of the folder selected on the navigation pane. For more information, see Contents pane on page 399.

Tool bar buttons

The following table describes the Trap/Log Manager tool bar buttons.

Table 177: 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.

Contents pane

The contents pane displays detailed information for the element selected in the navigation pane.

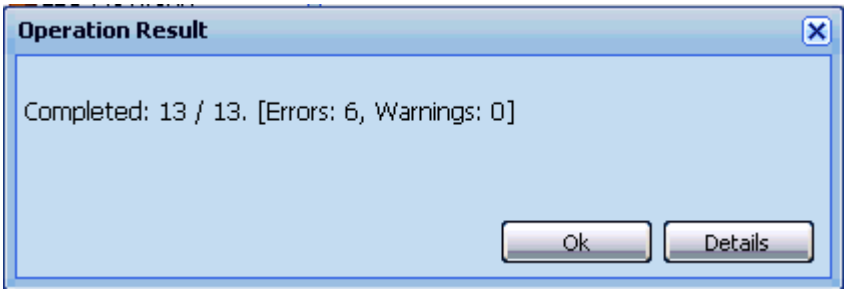
Discovering devices

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

1. 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.

1. Click **Preferences** in the tool bar. The Trap/Log Manager preferences dialog box displays.

For more information on editing the Preferences, see Setting Inventory Manager preferences on page 389.

Configuring Traps

The following sections provide instructions on configuring traps for ERS, VSP, and WC devices.

Configuring Trap Receivers for ERS and WC devices

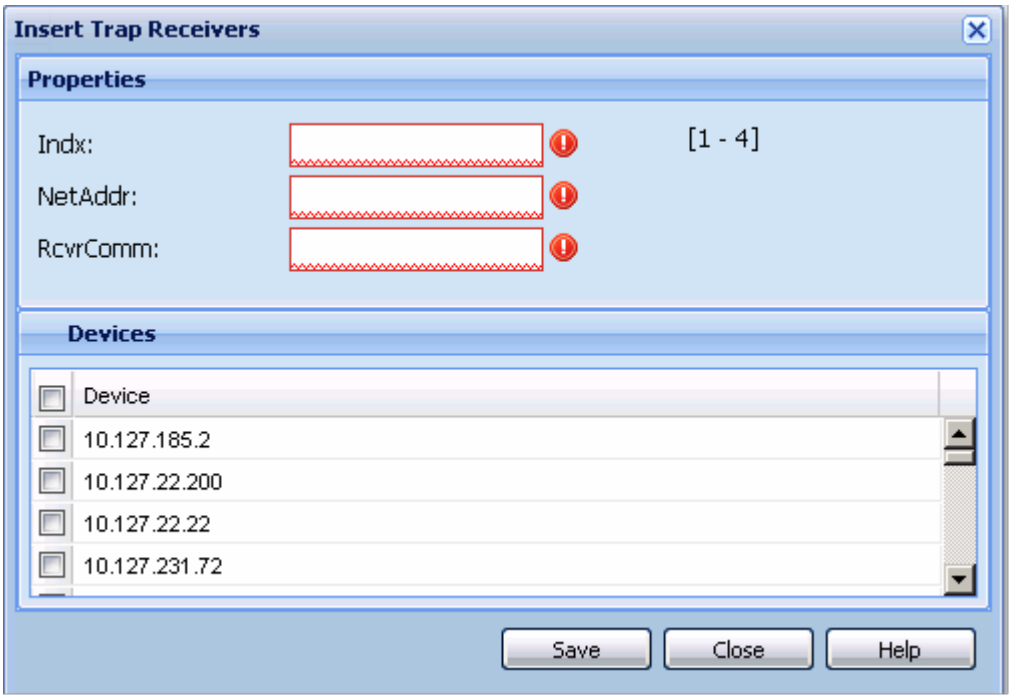
Perform the following procedure to configure trap/logs for the following devices:

- ERS 8xxx
- ERS 5xxx/4xxx/3xxx
- Ethernet Switch/ERS 25xx
- VSP 9xxx, VSP 7xxx, VSP 4xxx, VSP 8xxx
- 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 **Add** in the tool bar.

   The Insert Trap Receiver dialog box displays.



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:

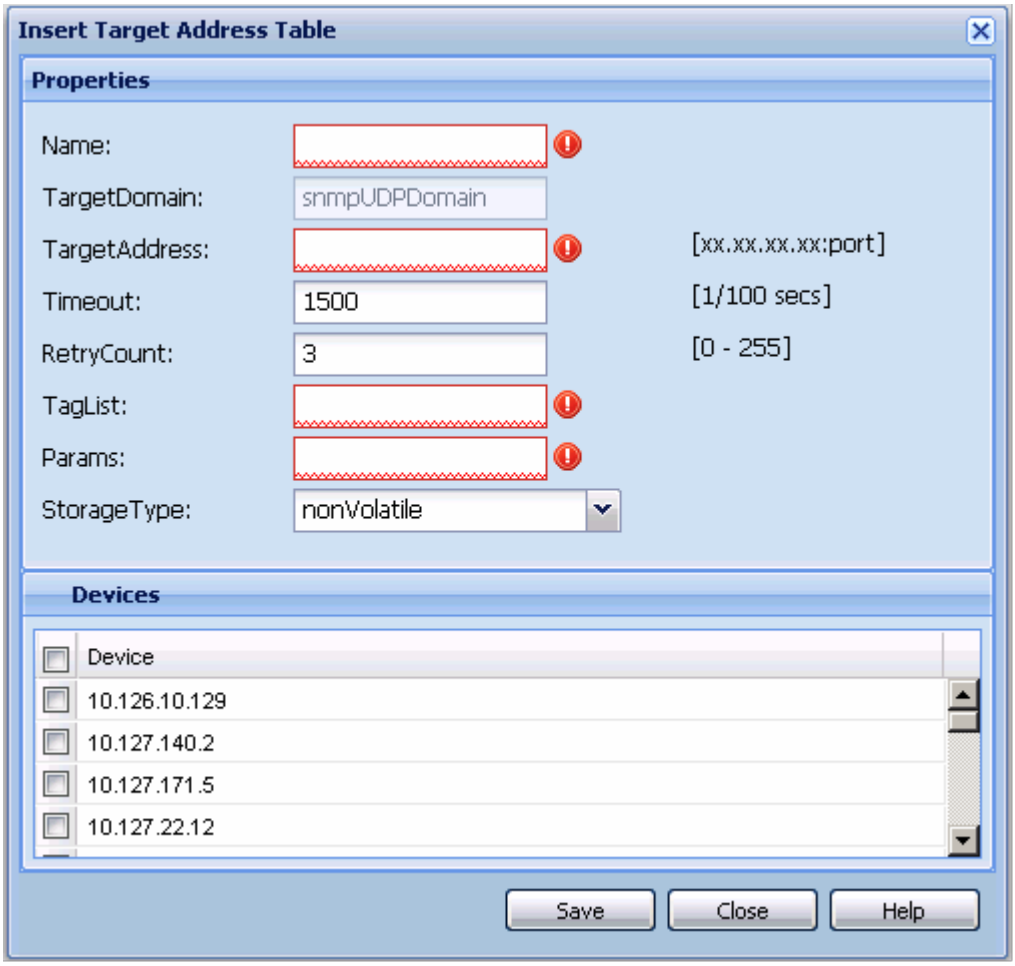
- ERS 1424/16xx
- ERS 25xx
- ERS 8xxx
- ERS 5xxx/4xxx/35xx
- VSP 9xxx, VSP 7xxx, VSP 8xxx, VSP 4xxx
- WC 8xxx

Procedure steps

1. In the Trap/Log Manager navigation tree, click **Configure Traps/Notifications**.
2. Choose the switch for which you want to configure target addresses.
3. In the contents pane, click the **Target Address Table** tab.

   By default, the Target Address Table tab displays.
4. To add a target address entry for a device, click **Add** in the tool bar.

   The Insert Target Address Table dialog box displays.



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.
TAddress	The IP address and the host of the target and the UDP port number.

Part	Definition
	Important: 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

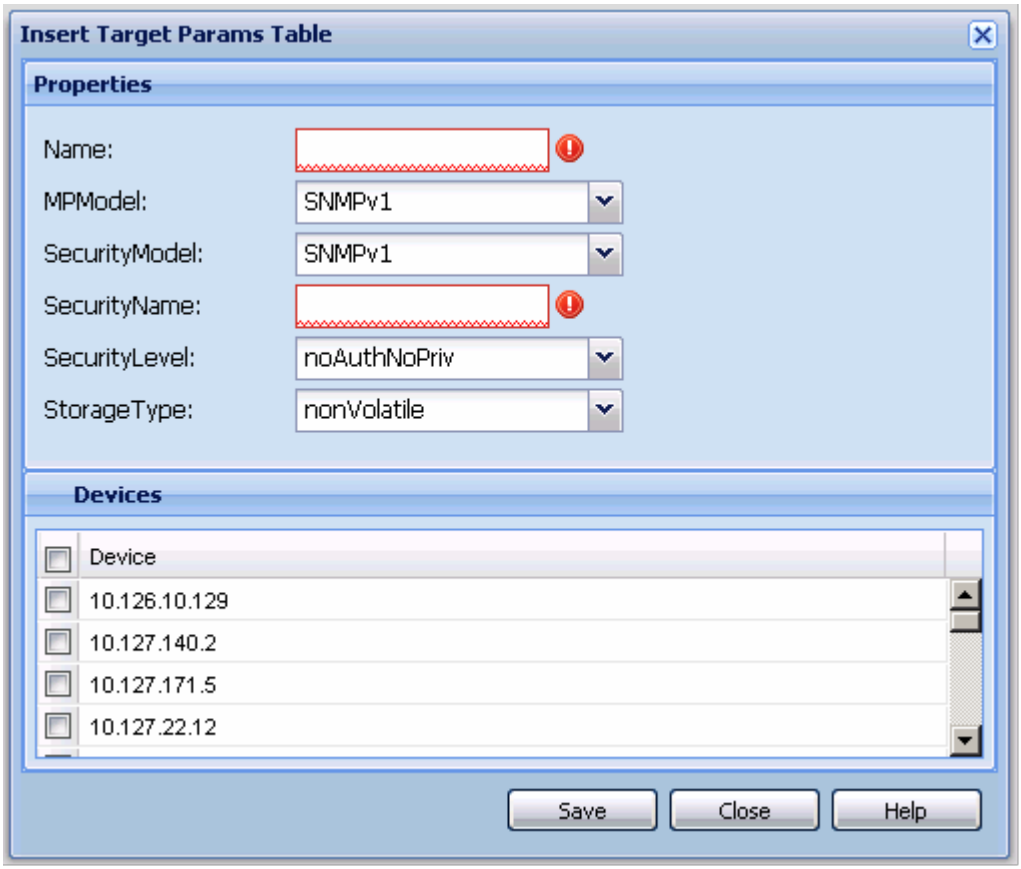
Perform the following procedure to configure Target Params Table for the following devices:

- ERS 1424/16xx
- ERS 25xx
- ERS 8xxx
- ERS 5xxx/4xxx/35xx
- VSP 9xxx, VSP 7xxx, VSP 8xxx, VSP 4xxx
- 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 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 displays.



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.
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.

Part	definition
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

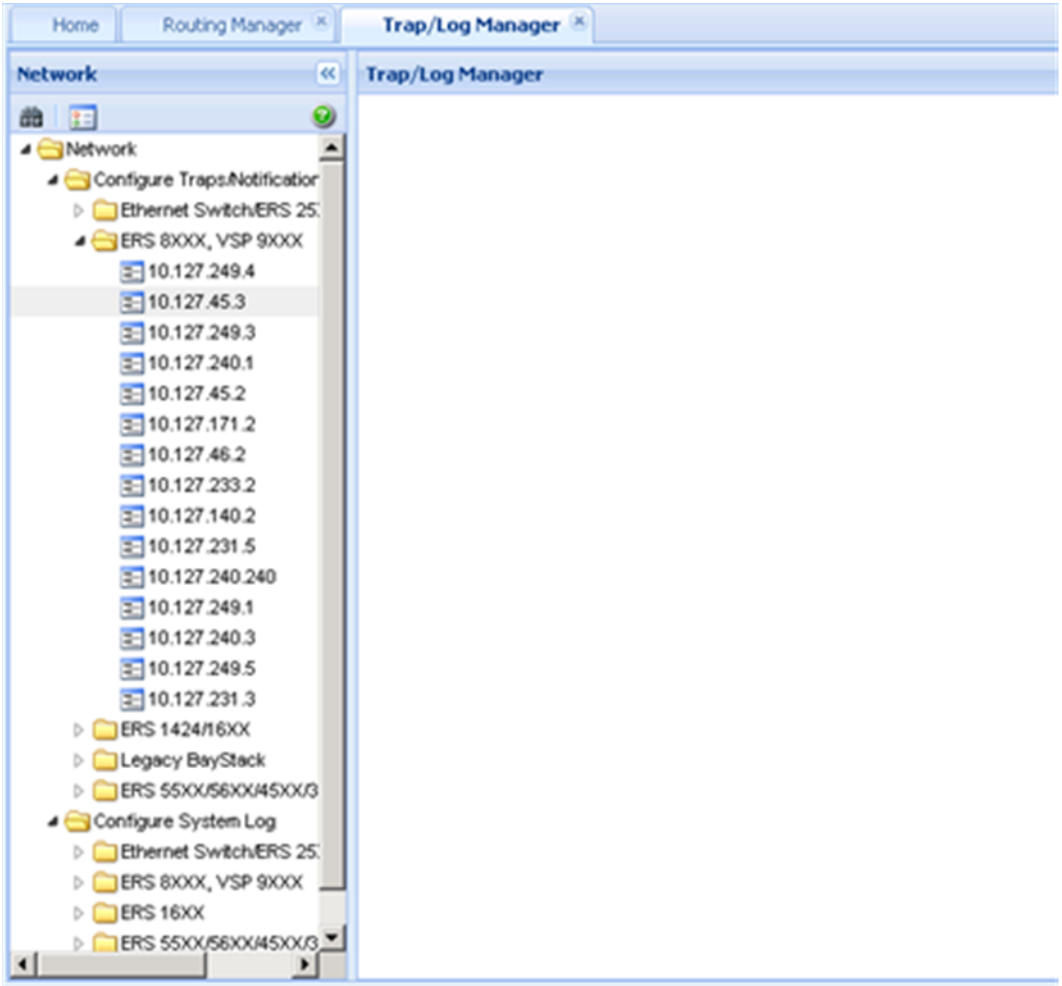
Perform the following procedure to configure Notify Table for the following devices:

- ERS 1424/16xx
- ERS 25xx
- ERS 8xxx
- ERS 5xxx/4xxx/35xx
- VSP 9xxx, VSP 7xxx, VSP 8xxx, VSP 4xxx
- WC 8xxx

Procedure steps

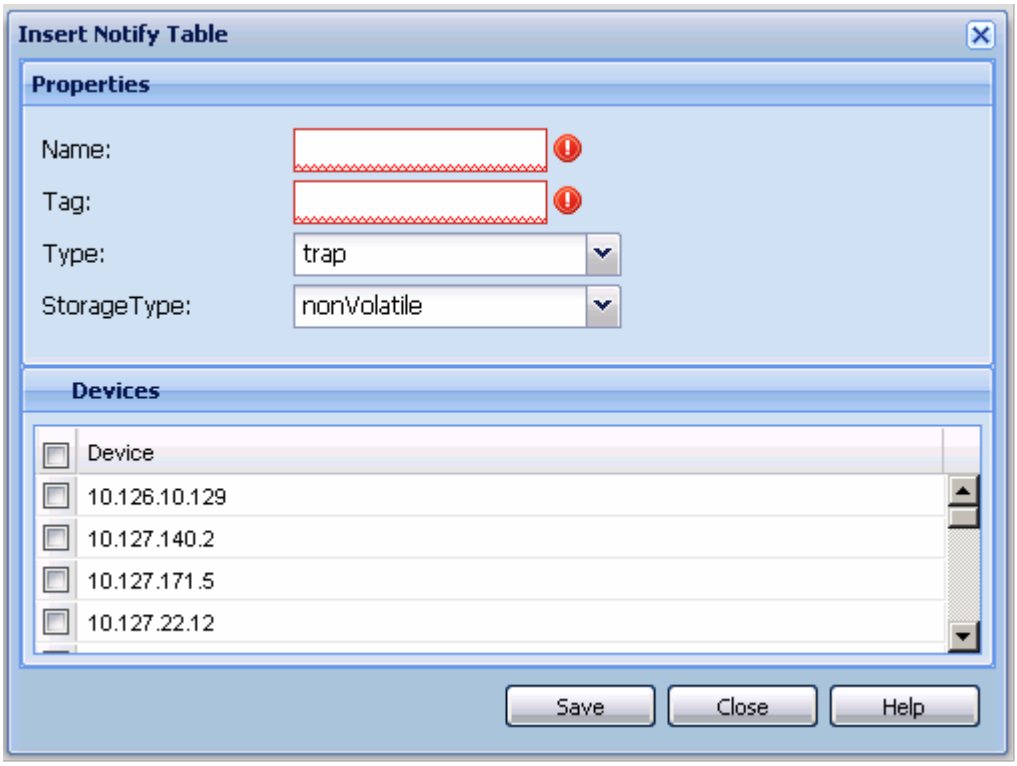
1. In the **Trap/Log Manager** navigation tree, click **Configure Traps/Notifications**.
2. Choose the switch for which you want to configure notifications.
3. In the contents pane, click the **Notify Table** tab.

   The Notify Table window displays.



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. If the value of this object is inform, then any messages generated for selected rows contain Inform PDUs.

Part	definition
	Important: 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.

Configuring System Log for ERS and VSP devices

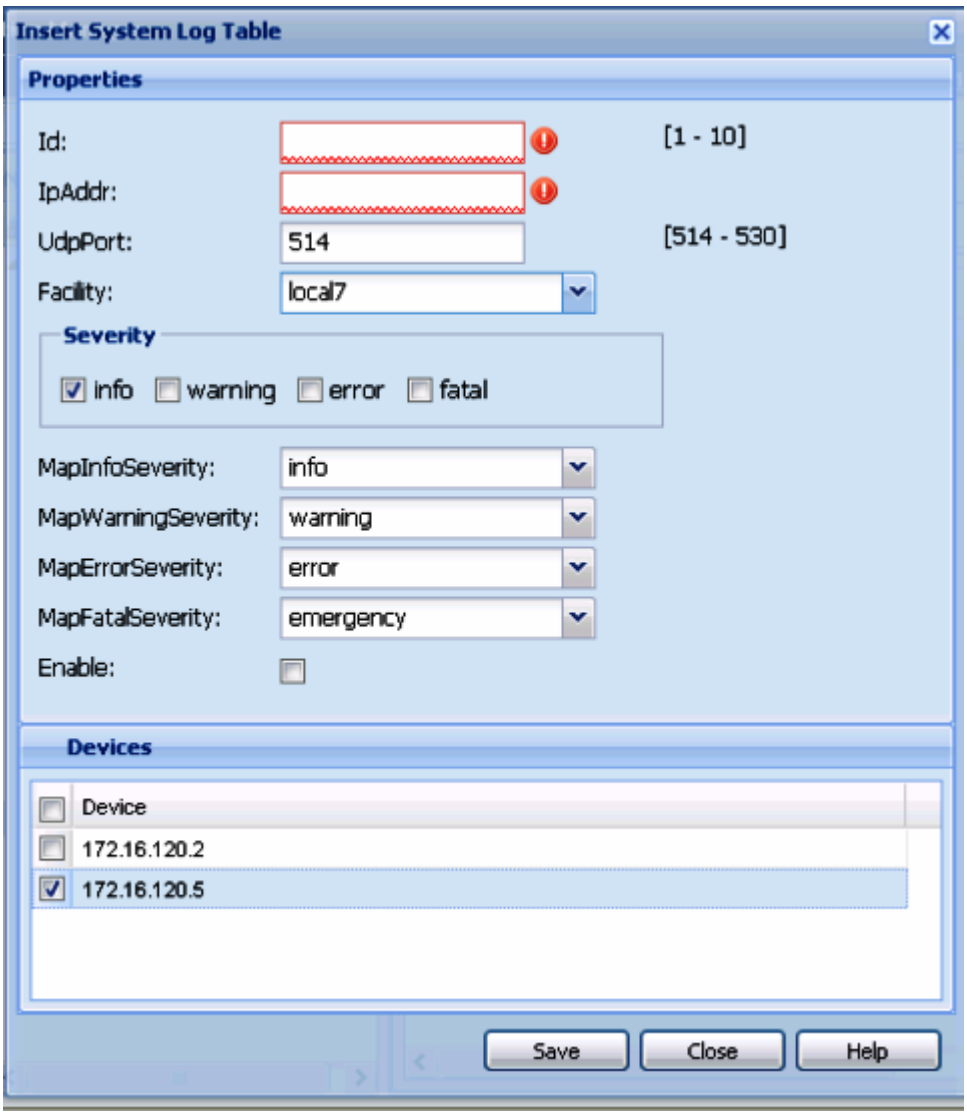
Perform the following procedure to create a system log for the following devices:

- ERS 8000
- Ethernet Switch/ERS 25xx
- ERS 1424/16xx
- VSP 9xxx, VSP 7xxx, VSP 8xxx, VSP 4xxx
- ERS 5xxx/4xxx/35xx
- WC8xxx

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.
UdpPort	The UDP port to use to send messages to the syslog host (514 to 530). Default value is 514.

Part	Definition
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 1424/16xx
- ERS 25xx
- ERS 8000
- ERS 5xxx/4xxx/35xx
- VSP 9xxx, VSP 7xxx, VSP 4xxx, VSP 8xxx
- WC 8xxx

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.

Configuration of trap parsers

You can use the **Trap Viewer** tab to configure trap parsers and to assign colors to trapped OID values in the COM database. The color that you assign to an OID value represent its importance in the trap grid listings. You can visually manage the network by setting severities for network events or statuses according to OID values.

For example, you can specify that a trap containing a specific OID should be considered a high priority trap and should be highlighted in red. When configured correctly, the COM application displays the trapped OID value in red in the trap grid.

Using the right click menu option, you also can use the trap parser configuration tool to highlight devices on a topology map. This map highlighting feature gives you a visual indication of the origin of the high priority trap. You can access the **Trap Viewer** tab by selecting the **Trap Viewer** icon in the Configuration and Orchestration Manager Navigation tree.

The **Trap Viewer** tab displays the following information about traps from devices:

- Time — The time that the trap was received.
- Device — The IP of the device in the trap.
- Trap Type — Lists one of the following two trap types for the device: LinkUp and LinkDown. These trap types determine whether any of the management station device links is functional or not functional.
- Message Text — The list of varbind (oid/value) pairs that detail information on the trap. The message text consists of an OID header value, then a varbind list value which gives detailed information about device issues. For example, an OID header value could be `powerSupplyFailed` and the varbind value could be `powerSupplyTemp=tooHigh`.

Starting the Trap Viewer

You launch the trap parser tool to gain access to the trap configuration options. In the trap parser configuration tool you perform the following actions: create a trap parser object and enable e-mail trap notifications. You also can use the trap parser configuration tool to highlight devices on a topology map.

You use trap parser objects to assign colors to trapped OID values in the COM database. The colors that you assign to an OID value represent its importance in the trap grid listings.

Complete the following steps to start the trap parser configuration tool.

Procedure

1. In the Configuration and Orchestration Manager Navigation tree, expand Managers.
2. Click the **Trap Viewer** icon.

   The Trap Viewer window displays the trapped devices.

Trap Viewer toolbar options

You can use the toolbar options on the **Trap Viewer** tab to manage trap parser objects and listed trap values. For example, you can create a trap parser object, filter trap values, and export values from the trap grid.

You use a parser object to assign the following properties to a particular trap or OID: severity, color, auto highlight, and e-mail. The colors that you assign to an OID value represent its importance in the trap grid listings. .

The traps are displayed on the **Trap Viewer** tab. If you have assigned a color to a trap, the trap is highlighted on the **Trap Viewer** tab in your chosen color. You can access the **Trap Viewer** tab by selecting the **Trap Viewer** icon in the Configuration and Orchestration Manager Navigation tree.

The following table lists and describes the Trap Viewer toolbar options available for your use:

Table 178: Trap Viewer toolbar options

Option	Description
Filter	Use this option to filter trapped grid listings based on on the following values: • Date • Device IP • Trap type • Message text
Forwarder	Use this option to manage trap forwarding rules according to source IP, destination IP, and port values. You have the option to add or to delete a listed forwarding rule.
Refresh	Use this option to refresh the trap grid view. The COM application communicates with the server to get the latest list of trap parser objects.
Print	Use this option to print the values that are displayed in the trap grid view.
Trap Parser	Use this option to create a trap parser object. In the Trap Parser Configuration window, you have the ability to specify the parser name and OID, varbind filter, and severity level values of the trap parser object.
Export	Use this option to export trapped grid values into xml and csv files.
Highlight on topology	Use this option to highlight the originating device of the high priority trap.

Trap parser object management

This section provides information about trap parser object management.

Creating a trap parser object

You can create a trap parser object to associate an OID and OID group with a parser. You also can create a trap parser object to associate a color with the trap severity. The color that you assign to a parser object represents its importance in the trap grid listings. When you work with trap colors, you can set severities for network events or statuses according to OID values.

When you create a trap parser object, you have the ability to specify trap filters through the varbind filtering list. You can set the trap parser object to trap general events through the OID field setting only. You also can set the trap parser object to trap specific events through the OID and varbind list field settings.

Use the toolbar buttons on the **General** and **Varbind Filter** tabs in the Trap Parser configuration Properties window to select, add, delete, and clear OID values on the trap parser object.

Perform the following procedure to create a trap parser object.

Procedure

1. On the Trap viewer tab, select the **Trap Parser** toolbar button.

   The Trap Parser Configuration window displays.
2. On the **General** tab, enter values in the following fields:
   - **Parser Name** — The name that identifies the trap parser object.
   - **OID** — The OID value that uniquely identifies the trap associated with the parser.
   - **Description** — The description for the trap parser object.
3. On the **Varbind Filter** tab, enter values in the following fields:
   - **OID** — The OID value that uniquely identifies the varbind filter value list.
   - **Value** — The specific varbind value that is used for the system uses to filter a trap.
   - **OID Value List** — The value list of one or more varbind OIDs.
4. On the **Severity Assignment** tab, select a severity level value from the **Severity Level** drop down list.
5. Click **Save**.

Next steps

You can enable a trap parser to allow the COM application to start processing the trap object.

Configuring the e-mail alert settings

Before you can use any e-mail alert function in COM, you must configure the e-mail alert settings. You can work with the e-mail server preferences to set up the SMTP values for your e-mail server. You also can use the COM preferences to enable or disable the e-mail alert function.

Perform the following procedure to configure an e-mail alert.

Procedure

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

   The Preferences window displays.

2. In the Email Server section on the **General** tab, enter values in the following fields:

   - SMTP Host
   - SMTP User Name
   - SMTP Password
   - From User (optional)
   - To Recipient (optional)
   - Port

   In the Preferences tool, if you enter values in the From User and To Recipient fields, and then configure a backup task, SVU task, or trap parser, the From User and To Recipient fields from the tasks are automatically populated with the corresponding information from the Preferences tool. However, you can override the preference information in the task creation.

3. Specify whether you want to enable the e-mail alert function.

Option	Enable E-mail
Enabled	Selected
Disabled	Cleared

4. Click **Save Preferences**.
5. **(Optional)** Select the **Test Email** button to test the e-mail function.

E-mailing a trap

You can use the **email icon** on the **Trap Viewer** tab to set up the trap e-mail notifications. Using an activated trap parser, you an configure the COM application to send information about trap OID and device traps. When you configure the e-mail settings, you have the option to specify one or more e-mail recipients along with textual descriptions.

Perform the following procedure to e-mail a trap.

Procedure

1. From the COM Navigation panel, open **Admin**, and then click **Preferences**.
2. Click the **General** tab.
3. Scroll down to the EMail Server section, and enter the following account information:
   a. SMTP Host
   b. SMTP User Name
   c. SMTP Password

d. From User
e. To Recipient
f. Port

4. Select **Enable Email**.
5. Click **Save Preferences**.

Next steps

After you access the Trap Parser from the Trap View tool bar, you can click the Severity Assignment tab to overwrite the information in the **From User** and **To Recipient** fields defined in the General Preferences. After you open the Severity Assignment tab, click **Enable Email**, and either enter new **Email Details** or accept the General Preferences information. To save the updated information, click **Save**.

For more information about trap parser configuration, see Configuration of trap parsers on page 411.

Job aid

The following table describes the EMail Server Preferences fields.

Table 179: EMail Server Preferences field descriptions

Attribute	Format	Description
SMTP Host	<textbox>	The host COM uses to set up a connection to the corporate e-mail server.
SMTP User Name	<textbox>	The user name COM uses to set up a connection to the corporate e-mail server.
SMTP Password	<textbox>	The password that permits COM to set up a connection to the corporate e-mail server.
From User	<textbox>	The default e-mail target address of the sender that identifies the sender of the e-mail to the recipient. For example: COM_TRAP@avaya.com
To Recipient	<textbox>	The default e-mail target of the recipient that identifies the location where COM sends e-mails and trap e-mails. For example: SYS_ADMIN@acme.com
Port	<numeric>	Identifies the port number.
Enable Email	Check box	If checked, enables the e-mail function.
Test Email	Context-sensitive button	Tests the connection to the corporate e-mail server.

Highlighting the originating device on the topology map

You can use the **Highlight on Topology** button to highlight devices on a topology map from the received trap in the trap viewer. You can work with the highlighted rows on the **Trap View** tab to further highlight the originating device of the trap.

Before you begin

To ensure that a trap is available for selection on the **Trap Viewer** tab, you first must enable a trap parser object.

Procedure

1. On the **Trap View** tab, select the trap grid row that you would like to
2. Select the **Highlight on Topology** toolbar button.

   The system highlights the originating device on the topology map.

Using the Syslog Viewer

The Syslog Viewer is a Configuration Orchestration Manager (COM) tool that permits you to view the system log.

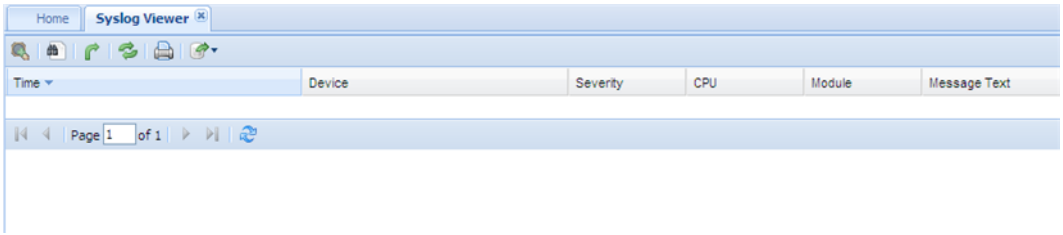
Viewing System Log

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. The CSV format permits you to read the trap information in a spreadsheet. The XML format permits you to read the trap information in other applications.

Chapter 16: Configuration of wizards and templates

Configuring 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.

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.

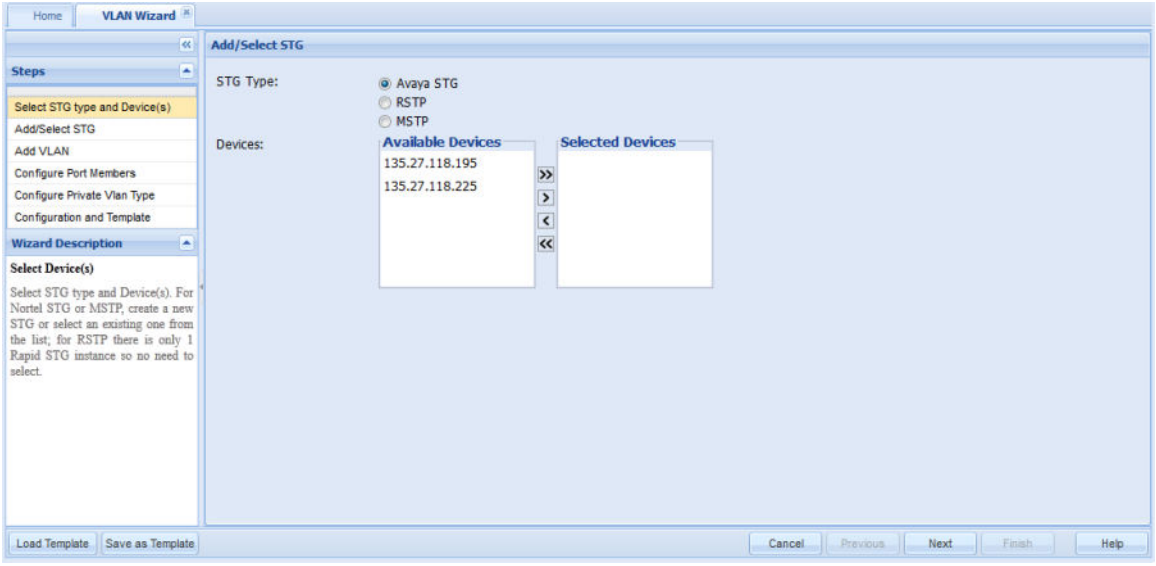


Figure 21: VLAN Wizard

VLAN wizard functionality

VLAN wizard can be used to configure spanning tree groups (STG) – Avaya STG and MSTP, and Switched UNI VLANs in multiple devices.

Note:

Switched UNI VLAN is supported on VSP 7000 v10.2 and above and ERS 4800 v5.7 only.

VLAN wizard provides the following functionalities:

- Select STG type and Device(s)
- Add/select an STG
- Add one or multiple VLANs or Switched UNI 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 180: 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.

Button	Description
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 420
- Adding or selecting an STG on page 421
- Adding a VLAN on page 421
- Configuring port members on page 424
- Saving the VLAN configuration on page 425

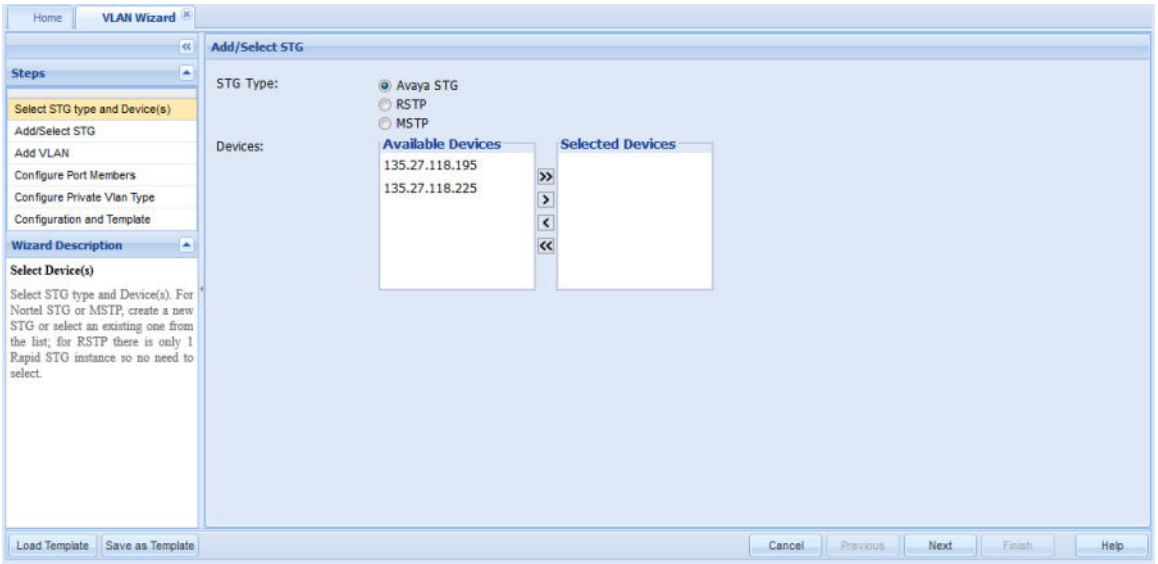
Selecting STG type and devices

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 displays.



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

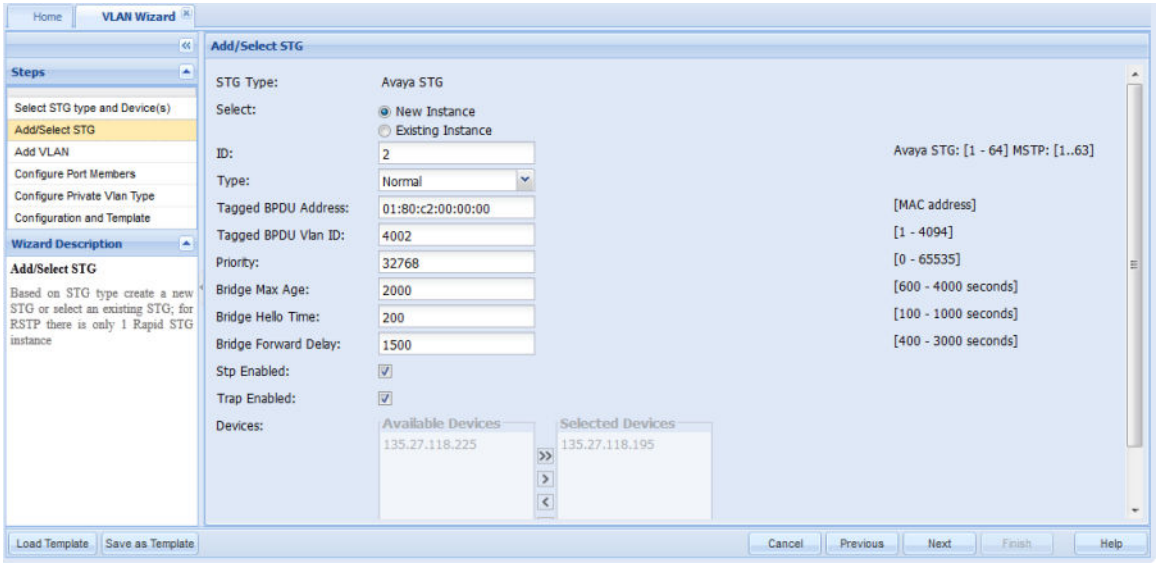
- In the Configuration and Orchestration Manager (COM) select VLAN Wizard.
- Perform the procedure for selecting STG type and devices.

Note:

The STG/MSTP id is not used in case of spbm-bvlan for VSP 7000.

Procedure steps

1. To add a new MSTP instance, choose **New Instance** in the **Select** field.
   - **OR**
   - To select an exiting STG, choose **Existing Instance** 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

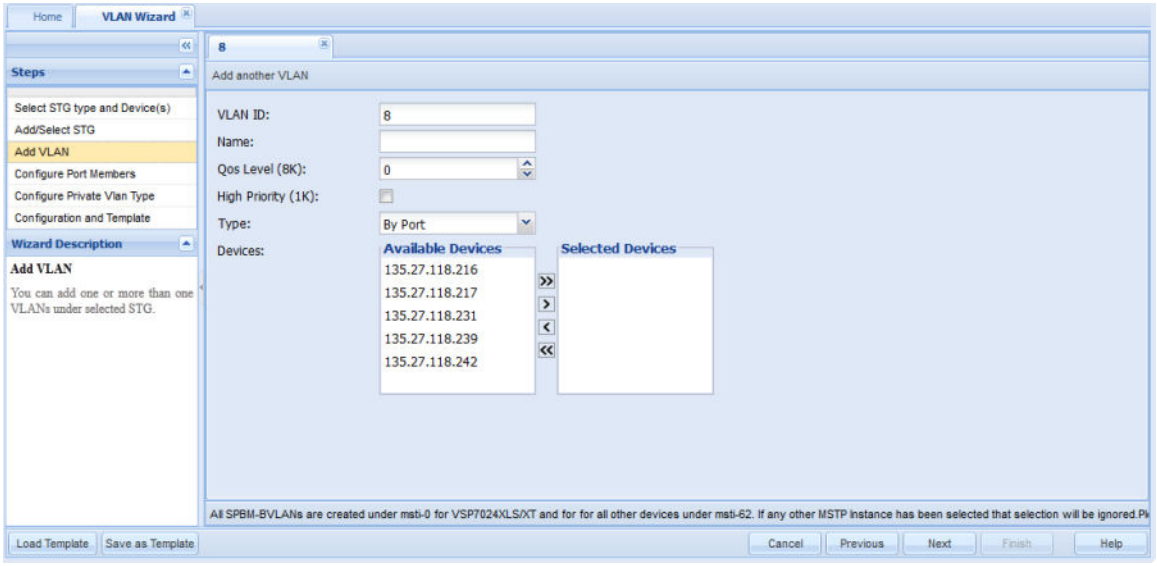
Perform the following procedure to add a VLAN in the wizard.

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 another 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 **Next** to move on Configure Port Members page.

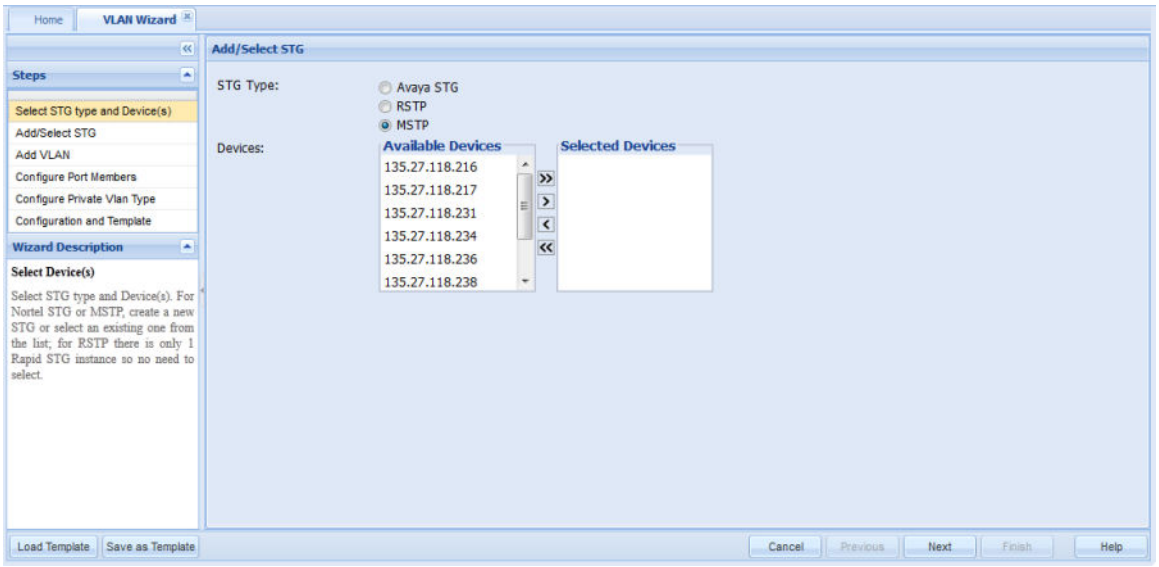
Selecting MTSP or RSTP type and devices

Perform the following procedure to select MSTP or RSTP 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 displays.
2. In the Add/Select STG dialog box, select the MSTP or RSTP type.



3. Select the devices.

4. To move to the Add/Select STG page, click **Next**.

Adding or selecting an MSTP or RSTP

Perform the following procedure to add or select an MSTP or RSTP in the VLAN wizard.

Prerequisites

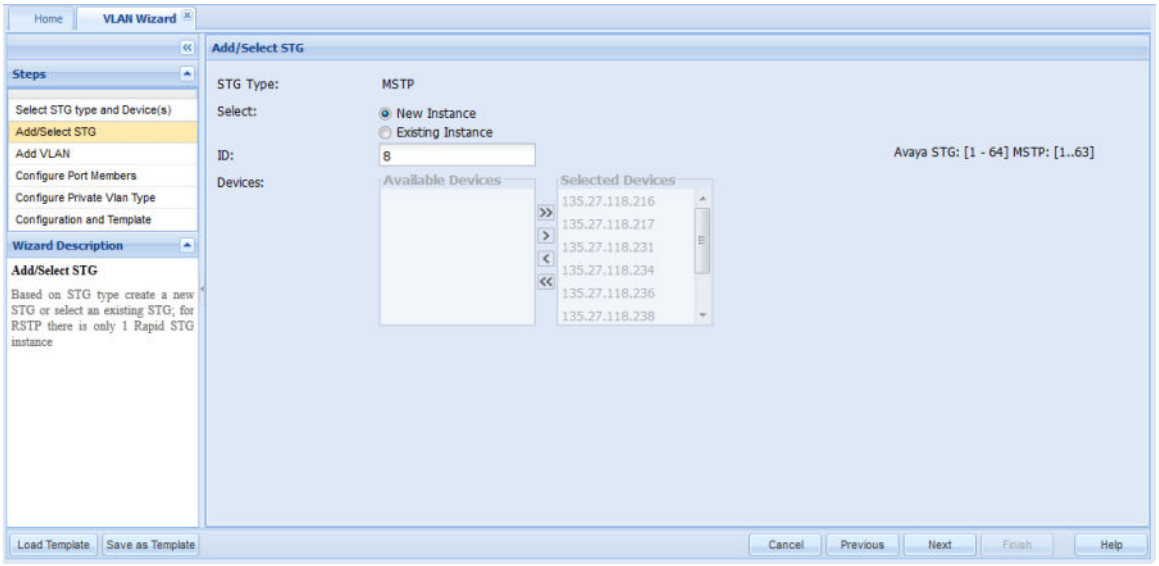
- In the Configuration and Orchestration Manager (COM) select VLAN Wizard.
- Perform the procedure for selecting MSTP or RSTP type and devices.

Note:

The STG/MSTP id is not used in case of spbm-bvlan for VSP 7000.

Procedure steps

1. To add a new MSTP instance, choose **New Instance** in the **Select** field.
   - **OR**
   - To select an exiting STG, choose **Existing MSTP** in the **Select** field.



2. Select the devices.
3. Click **Next** to move on Add VLAN page.

Adding a private VLAN

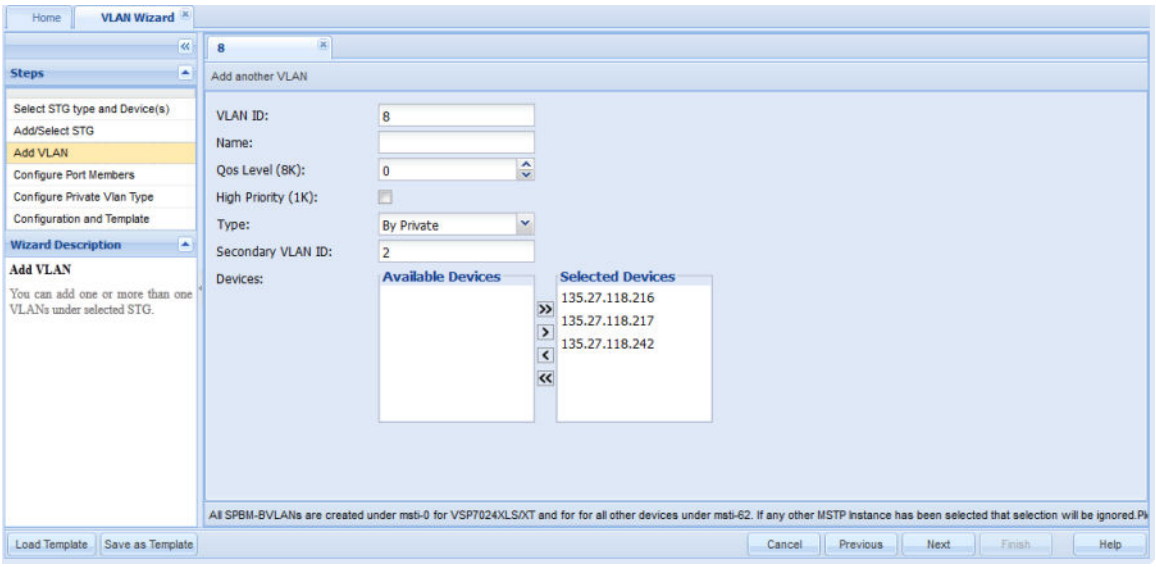
Perform the following procedure to add a private VLAN in the wizard.

Prerequisites

- In the Configuration and Orchestration Manager (COM), select VLAN Wizard.
- Perform the procedure for selecting MSTP or RSTP type and devices.
- Perform the procedure for adding or selecting an MSTP or RSTP.

Procedure steps

1. In the **Add another VLAN** page, enter information in all the fields to add a VLAN in the wizard.



2. Select **By Private**.
3. Enter the secondary VLAN ID.
4. 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.
5. Click **Next** to move on Configure Port Members page.

Configuring port members

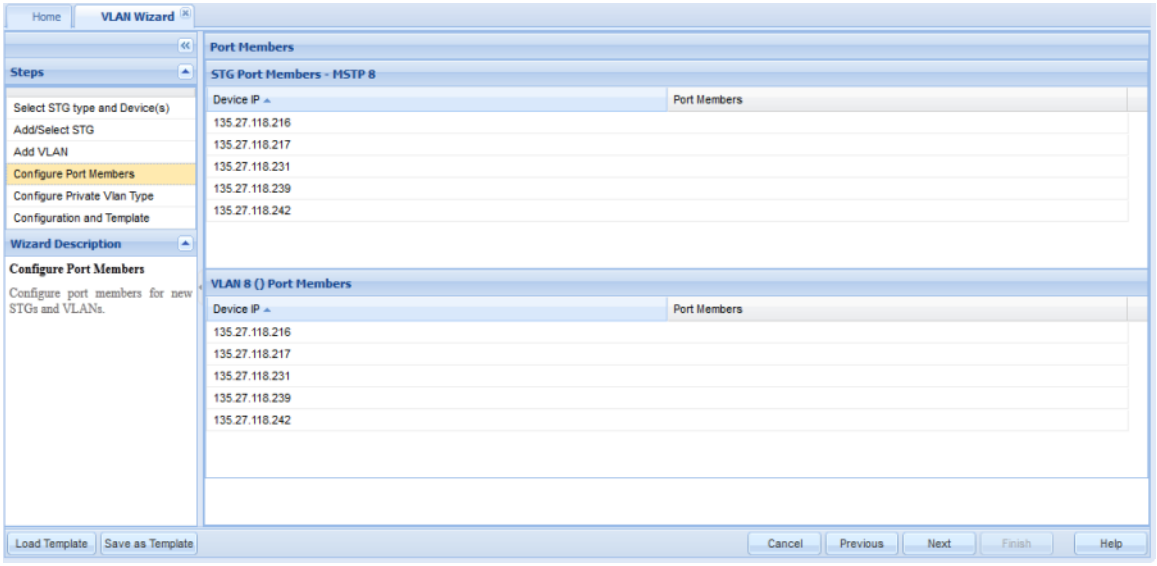
Perform he following procedure to view the configured port members.

Prerequisites

- In the Configuration and Orchestration Manager (COM), select VLAN Wizard.
- Perform the procedure for selecting STG, MSTP or RSTP type and devices.
- Perform the procedure for adding or selecting an STG, MSTP or RSTP.
- Perform the procedure for adding a VLAN.

Procedure steps

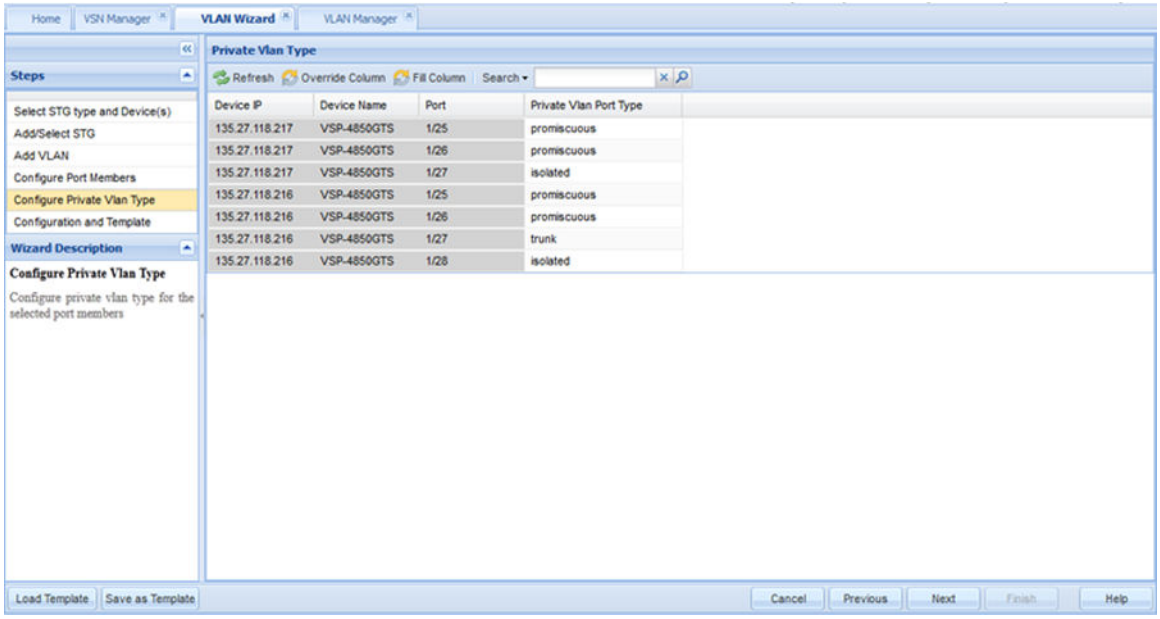
1. In the Port Members page, click **Next** to move to the Configuration and Template page.



Configuring Private VLAN Type

When the ports members are added to the VLAN, this step aids in identifying each selected port to be either isolated, promiscuous, or trunk.

This step is required when the added VLAN type is private.



Saving the VLAN configuration

Perform the following procedure to save the configuration as a template.

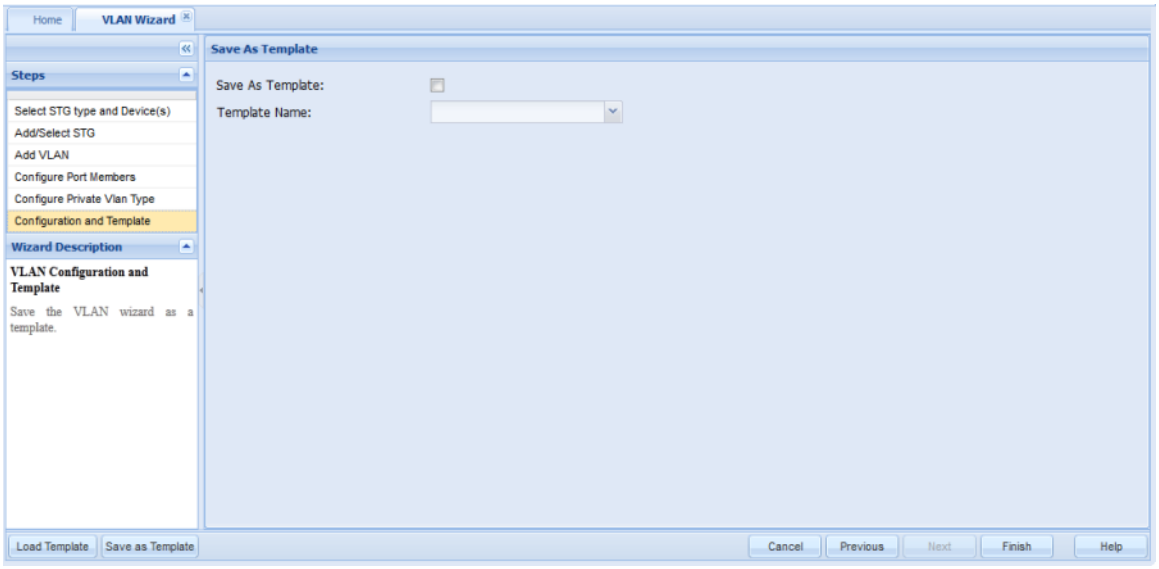
Procedure steps

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 displays.



3. Select **Save As Template** 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 displays.

Loading a template

Perform the following procedure to load a template.

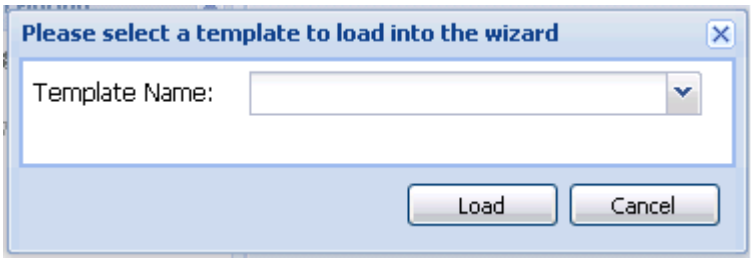
Procedure steps

1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizards**, and then click the **VLAN Wizard** icon.

   The VLAN Wizard dialog box displays.

2. Click **Load Template**.

   The Please select a template to load into the wizard dialog box displays.



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.

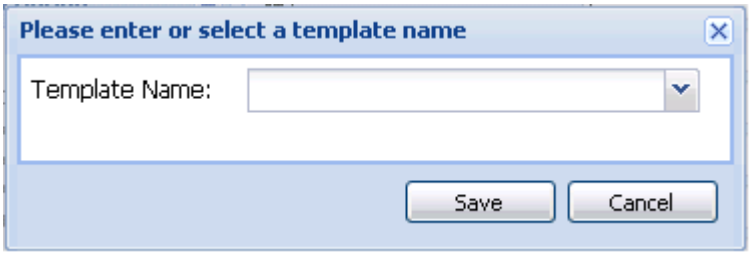
Procedure steps

1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizards**, and then click the **VLAN Wizard** icon.

   The VLAN Wizard dialog box displays.

2. Click **Save as Template**.

   The Please enter or select a template name dialog box displays.



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.

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

Job aid

The following table describes the fields of Truck properties screen:

Table 181: Trunk properties

Field	Description
SMLT Access Ports	Specifies the SMLT access port.
SMLT MLT Number	Specifies the SMLT MLT number.
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.

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.

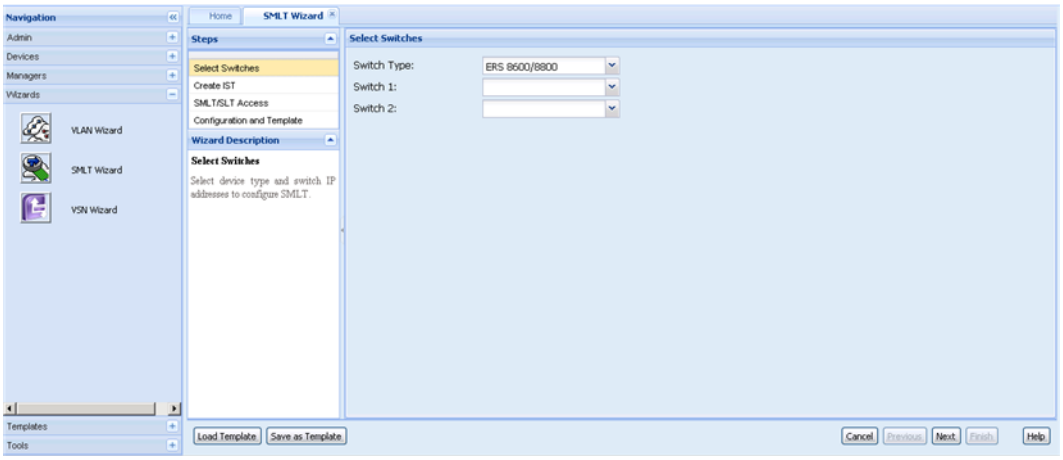
Note:

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

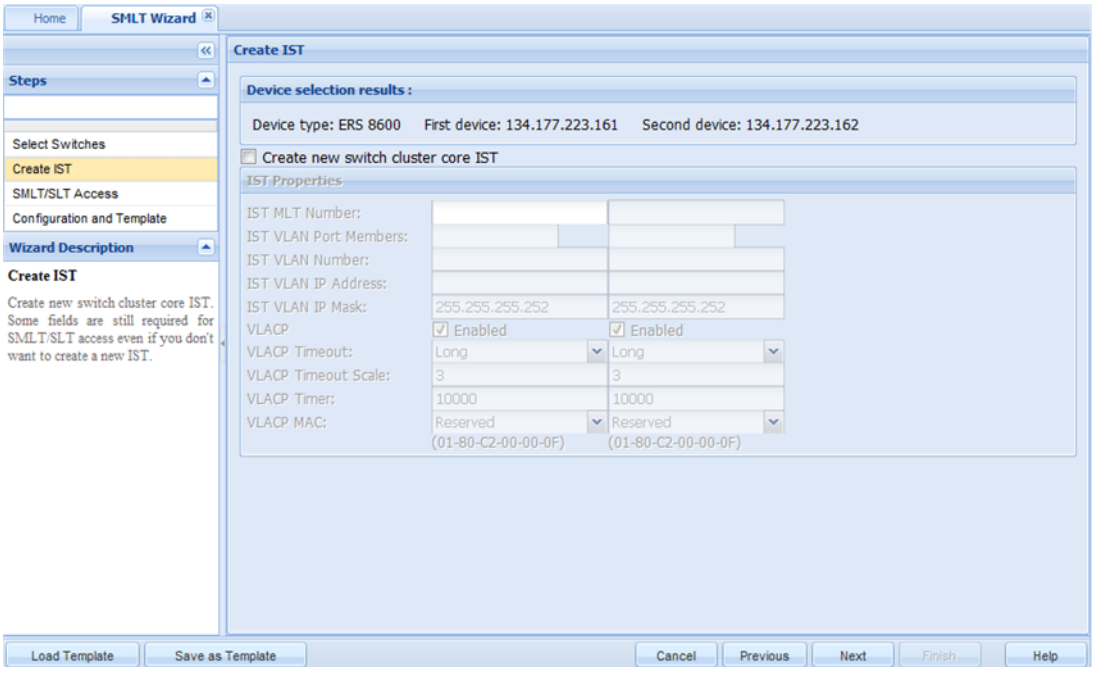
1. From the **Configuration and Orchestration Manager** navigation pane, select **Wizards**, and then click the **SMLT Wizard** icon.

   The SMLT Wizard dialog box displays.



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 displays.



5. Select the **Create new switch cluster core IST** check box.
6. Enter the values for creating the IST in the fields provided.

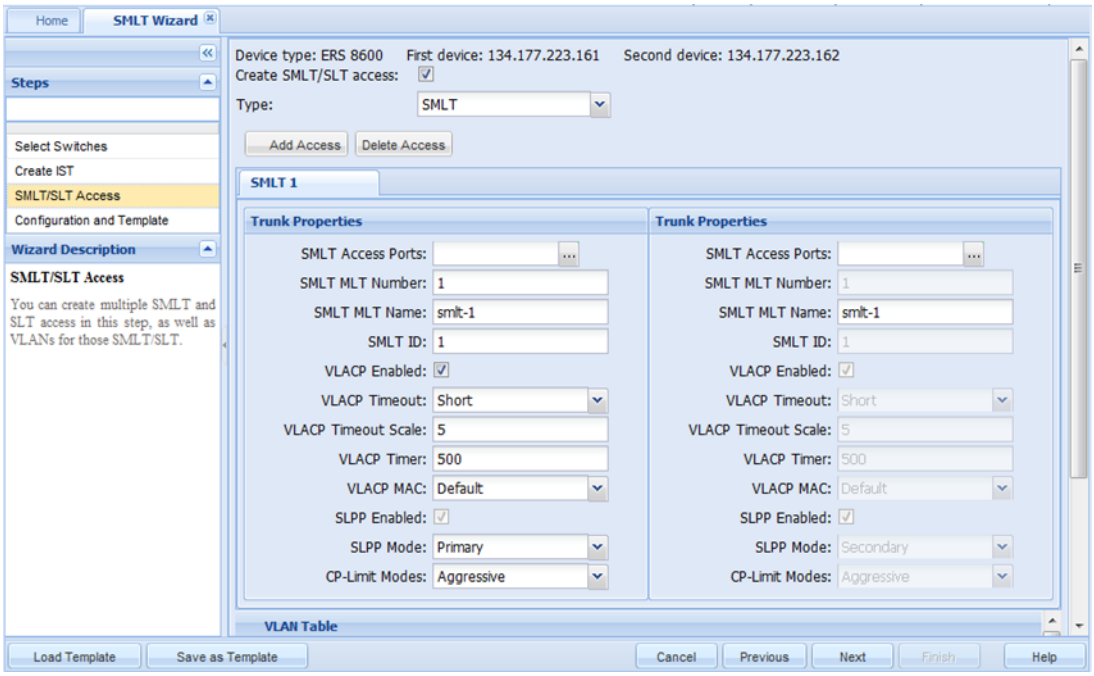
Some of the fields are common for both the switches. For the second switch, the value of the common fields are filled automatically as you enter the value for the first switch.

Important:

Prepopulated values are available in some fields.

7. Click **Next**.

   The SMLT/SLT access dialog box displays.



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.

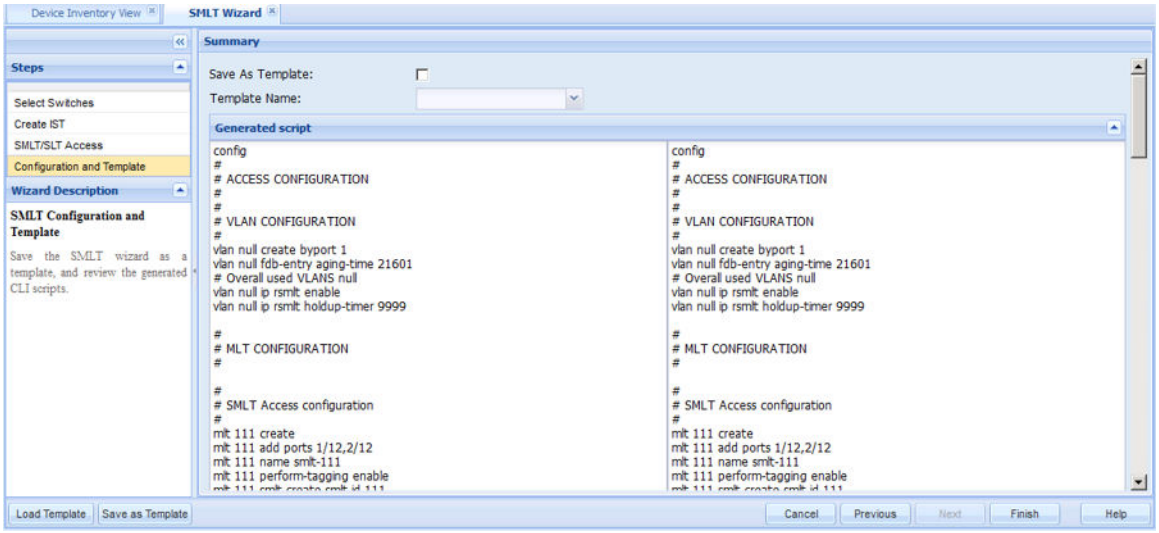
    The SMLT/SLT Access form includes

    - 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 Summary page (SMLT Configuration and Template) displays. This page reviews the generated CLI scripts and has option to Save the SMLT wizard as a template and provides the template name.



17. Select the **Save as Template** check box to save the current SMLT wizard Configuration as a template. When this check box is selected, the Template Name drop down text box enables.
18. Provide a valid Template name or select the existing Template name if the selected template needs to be overwritten.
19. Click **Finish** 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 VLAN table.

Table 182: 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.

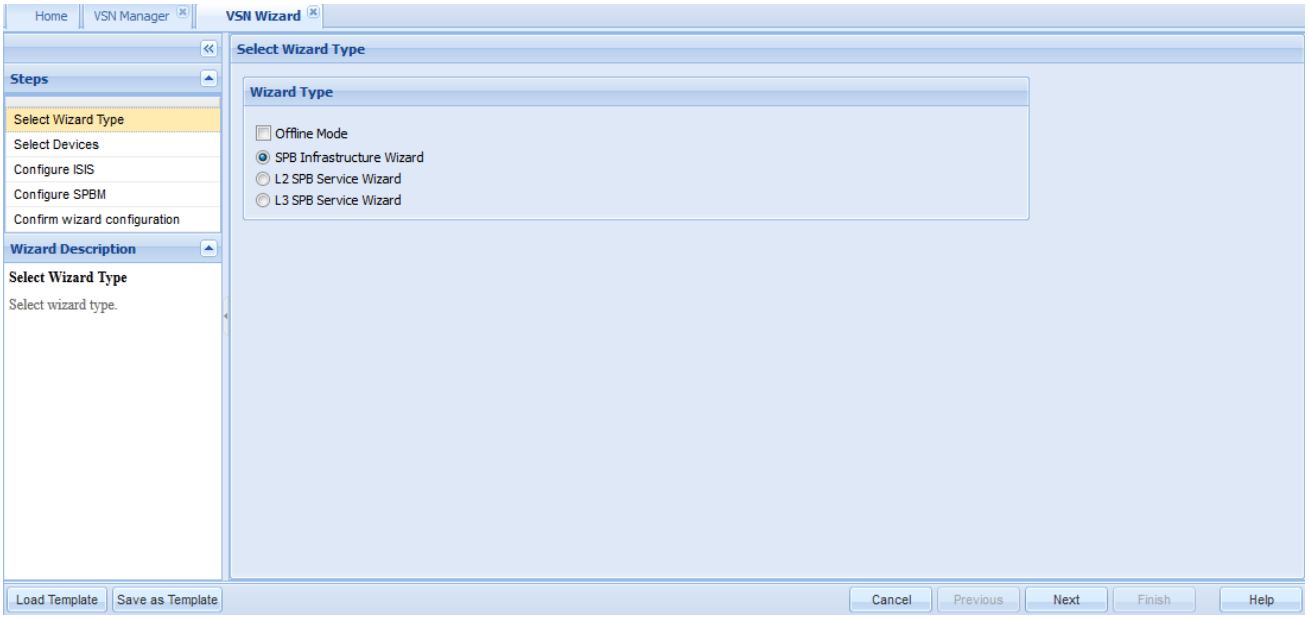
You can modify the value of VLAN Table entries using in-line edit modes.

VSN wizard

VSN wizard has the following two sections:

- 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 following table outlines the supported device list for the VSN wizard.

Supported device for VSN wizard	Version	Wizard type supported
ERS 8600 and ERS 8800	v7.1, v 7.1.3, v7.2.0, v7.2.10	• SPB Infrastructure Wizard • L2 SPB Service Wizard • L3 SPB Service Wizard
VSP 4000	v3.0.1, v 3.1	• SPB Infrastructure Wizard • L2 SPB Service Wizard
VSP 7000	v10.1, v10.2, v10.3, v10.3.1[1]	• SPB Infrastructure Wizard • L2 SPB Service Wizard - L2 SPB Service Wizard C Vlan UNI - L2 SPB Service Wizard Switched UNI

Supported device for VSN wizard	Version	Wizard type supported
		- L2 SPB Service Wizard Transparent UNI • L3 SPB Service Wizard
VSP 8000	4.0	• SPB Infrastructure Wizard • L2 SPB Service Wizard
VSP 9000	v 3.2, v 3.3, v3.4, v4.0	• SPB Infrastructure Wizard • L2 SPB Service Wizard • L3 SPB Service Wizard

1 — SPB Infrastructure and L2 SPB Service support only

VSN wizard functionality

The VSN wizard has the following 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 449.

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 supported devices 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
   - Source/CLIP Address
   - CLIP Mask
   - ISIS Interfaces
     a. In the ISIS interfaces column, click on **Please specify**.

        The ISIS Interfaces dialog box appears.

     b. Enter the values.
     c. 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. The required parameters are: <System ID> = System ID {xxxx.xxxx.xxxx - 6 bytes} The command syntax is : system-id <System ID> 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.
Source/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.
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. The required parameters are: <instance-id> = plsb instance-id (1..100) {1..100} 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. The required parameters are: <enable|disable> = isis spbm ip shortcut state {disable|enable} The command syntax is: ip<enable|disable>

Field	Description
	The states are enable and disable. The default is disable.

Using the L2 SPB Service Wizard

In the L2 SPB Service Wizard, you can configure C-VLAN UNI, Switched UNI, and Transpartent UNI Vlans.

Note:

Switched UNI Vlans can be configured for VSP 7000 v10.2 and v10.3 and ERS 4800 v5.7 devices only.

Note:

Transparent UNI Vlans can be configured for VSP 4000 v3.1 devices only.

Adding an L2 ISID with C-VLAN UNI type

About this task

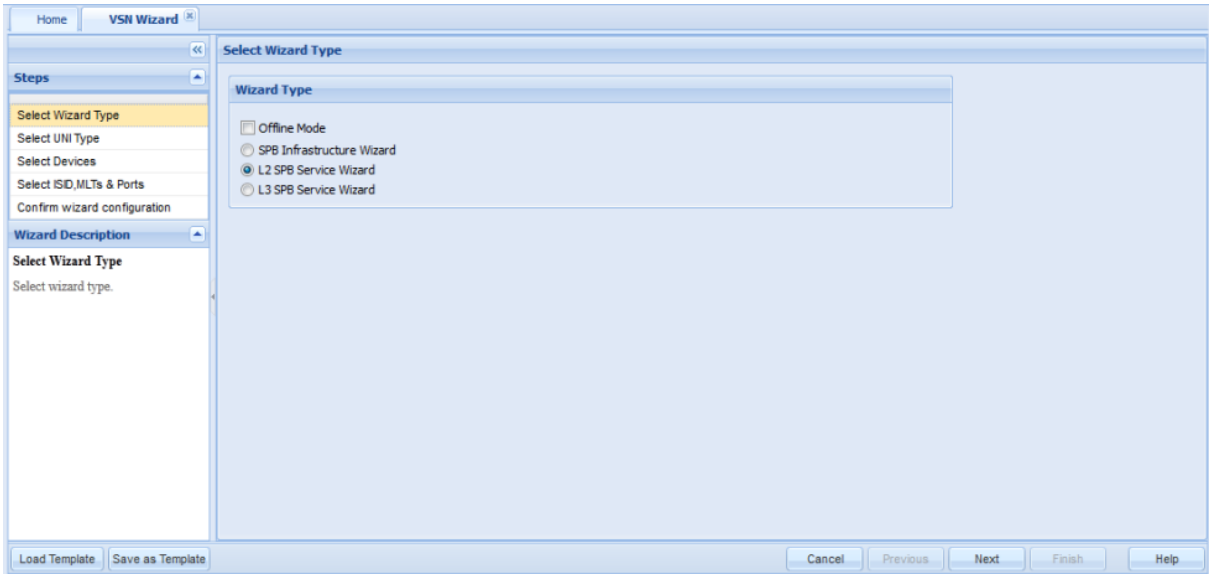
Perform the following procedure to add an L2 ISID with CVLAN UNI type.

Procedure

1. From the **COM** navigation pane, select **Wizards**, and click the **VSN Wizard** icon.

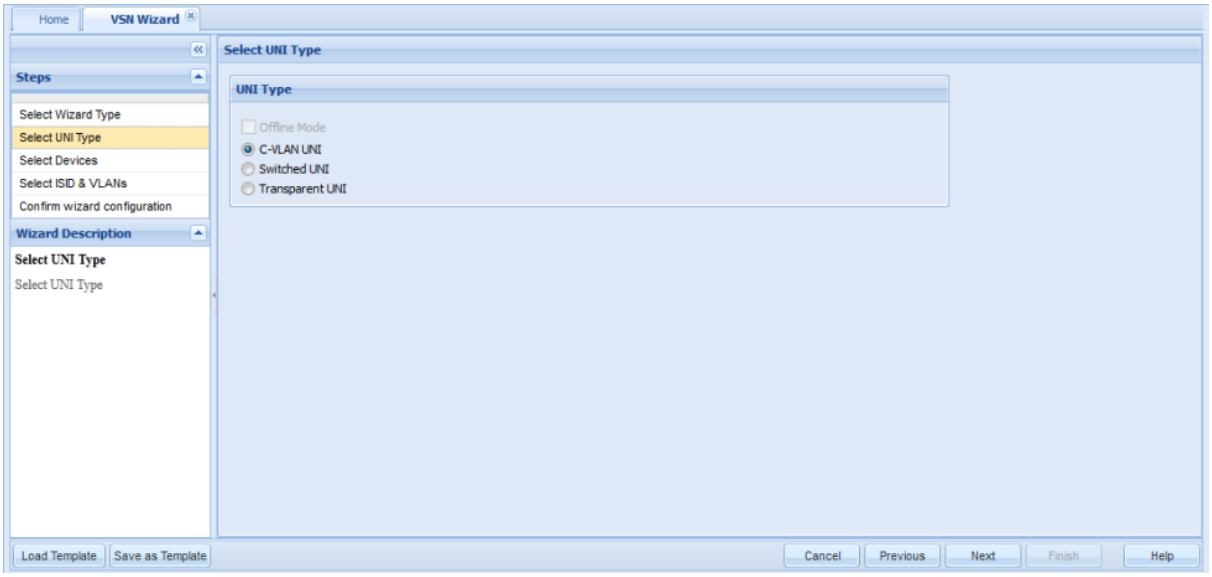
   The VSN Wizard tab opens.

2. In the Select Wizard Type area in the Contents pane, select **L2 SPB Service Wizard**.



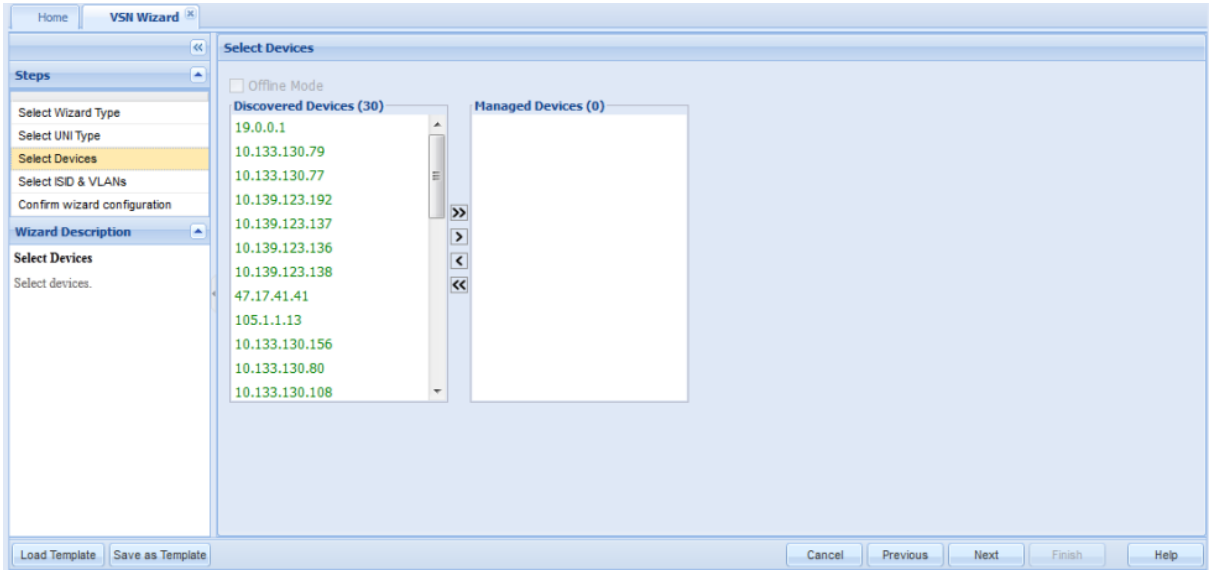
3. Click **Next**.

   The Select UNI Type window displays.



4. From the Select UNI Type window, select **C-VLAN UNI** .
5. Click **Next**.

   The Select Devices window displays.



6. From the Discovered Devices section, select the device(s).
   - 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 >**.
   - To move all devices from the Available Devices list to the Selected Devices list, click **Select All >>**.

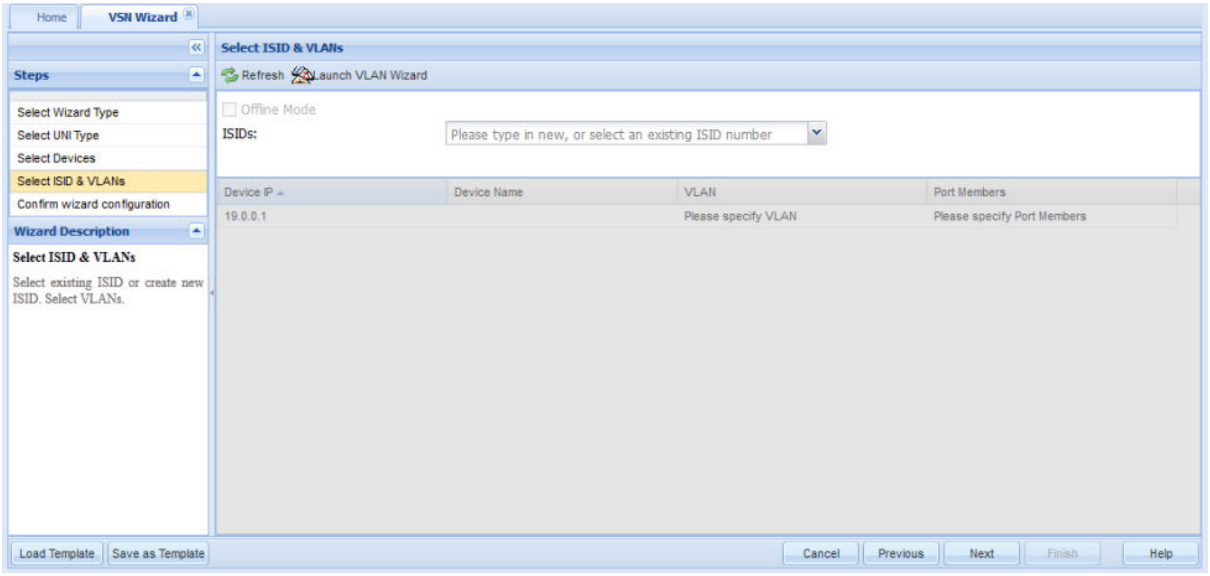
   To unselect a device, from the Selected Devices table, select the required item and click **< Unselect** . To unselect all devices, click **<< Unselect All** .

7. Click **Next**.

   COM performs a VSN discovery and the Operation Completed box displays the results of the VSN discovery.

8. Click **OK**.

   The Select ISID & VLANs page displays.



9. In **ISID** field, enter an ISID number.
10. From the **VLAN** column drop-down box, select a VLAN.

    If there are no VLANs for a device, then you must add a VLAN.

11. Click **Launch the VLAN Wizard**.
12. After you complete the procedure for adding a VLAN, click the **VSN Wizard** tab.
13. Click **Refresh** and select the VLAN.
14. To view the information or make changes to the port currently mapped to the VLANs, in the **Port Members** column, double-click on a cell for a specific device.

    The Port Members window displays.

15. Add or remove ports, then click **Save**.
16. In the wizard frame, click **Next**.
17. Click **Finish** or if you choose to save the wizard configuration as a template, perform the following steps:

    a. Check the **Save as Template** check box.

    b. Enter a Template name.

    c. Click **Finish**.

Adding L2 ISID with Switched UNI type

About this task

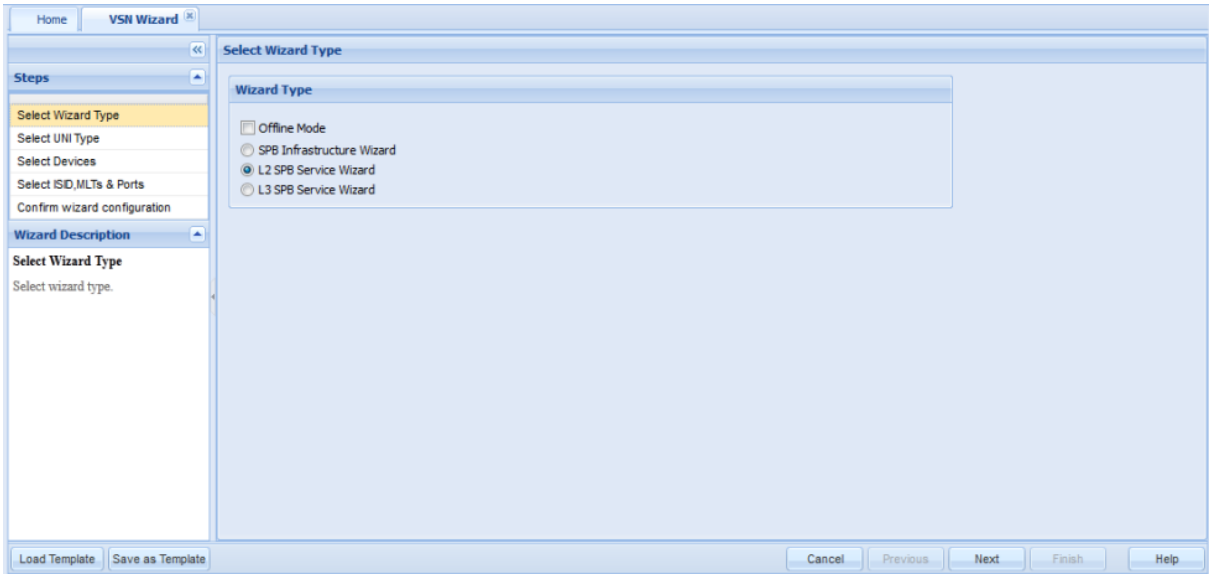
Perform the following procedure to add an L2 ISID with Switched UNI type.

Procedure

1. From the **COM** navigation pane, select **Wizards**, and click the **VSN Wizard** icon.

   The VSN Wizard tab opens.

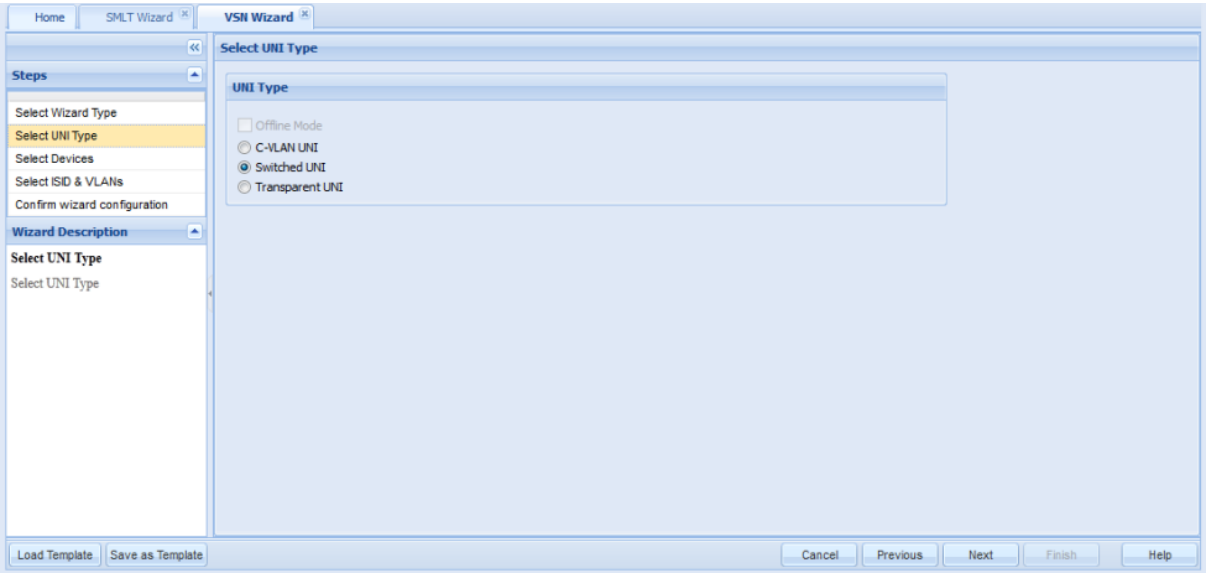
2. In the Select Wizard Type area in the Contents pane, select **L2 SPB Service Wizard**.



3. Click **Next**.

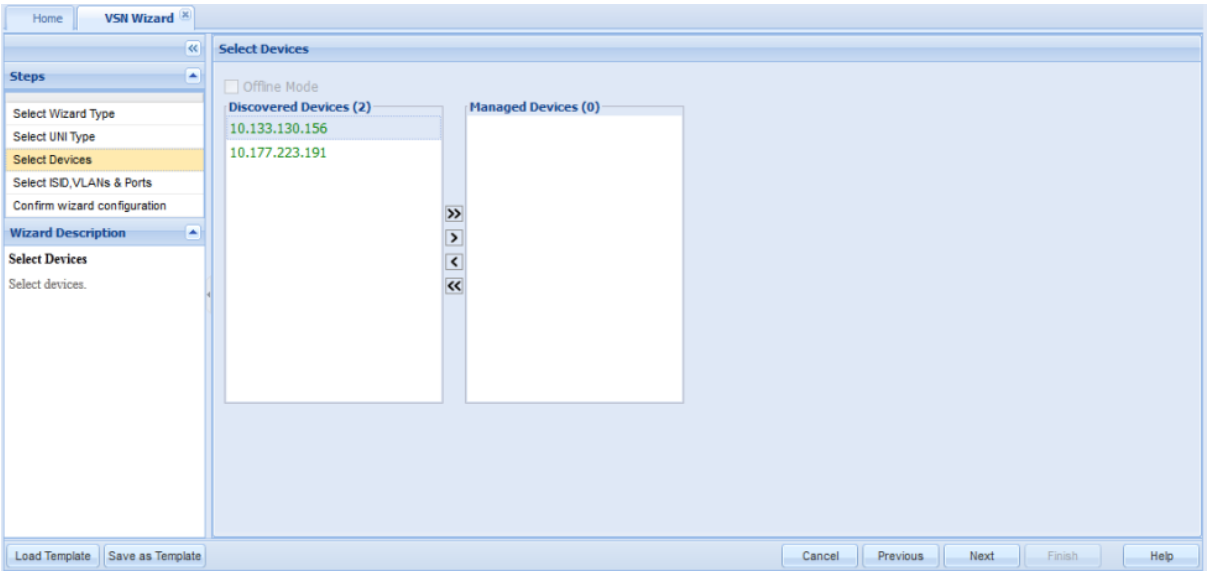
   The Select UNI Type window displays.

4. Select **Switched UNI** .



5. Click **Next**.

   The Select Devices window displays.



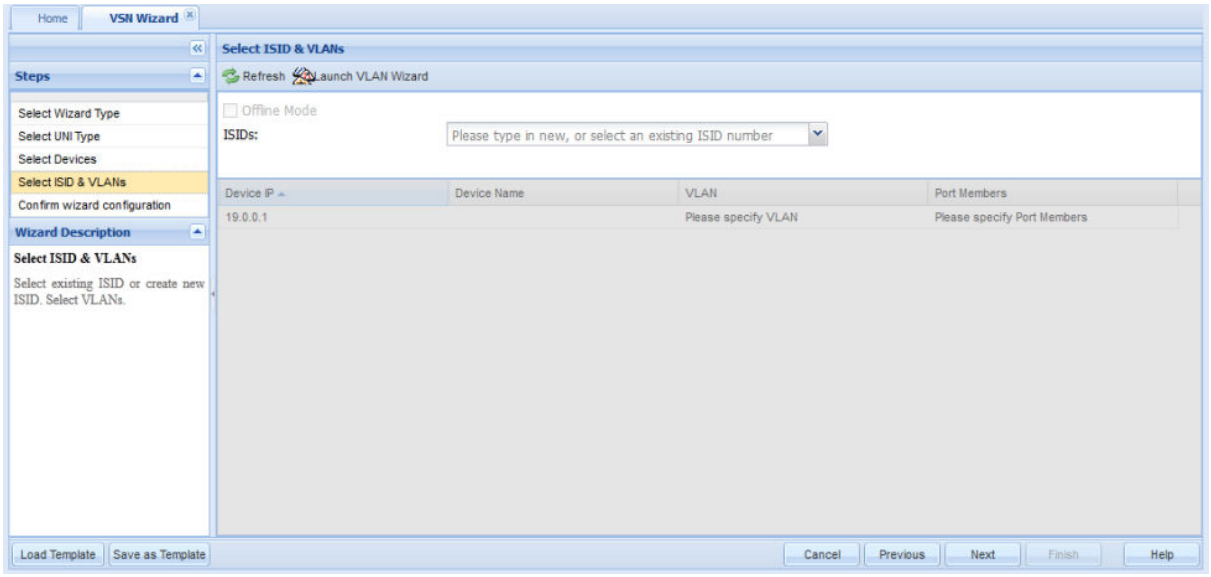
6. From the Discovered Devices section, select the device(s).
   - To move a device from the Available Devices list to the Selected Devices list, from the Available Devices list, select the corresponding row, and click **Select >**.
   - To move all devices from the Available Devices list to the Selected Devices list, click **Select All >>**.

   To unselect a device, from the Selected Devices table, select the required item and click **< Unselect** . To unselect all devices, click **<< Unselect All** .
7. Click **Next**.

COM performs a VSN discovery and the Operation Completed box displays the results of the VSN discovery.

8. Click **OK**.

   The Select ISID & VLANs page displays.



9. In **ISID** field, enter an ISID number.
10. From the **VLAN** column drop-down box, select a VLAN.

    If there are no VLANs for a device, then you must add a VLAN.
11. Click**Launch the VLAN Wizard**.
12. After you complete the procedure for adding a VLAN, click the **VSN Wizard** tab.
13. Click **Refresh** and select the VLAN.
14. To view the information or make changes to the port currently mapped to the VLANs, in the **Port Members** column, double-click on a cell for a specific device.

    The Port Members window displays.
15. Add or remove ports, then click **Save**.
16. In the wizard frame, click **Next**.
17. Click **Finish** or if you choose to save the wizard configuration as a template, perform the following steps:
    a. Check the **Save as Template** check box.
    b. Enter a Template name.
    c. Click **Finish**.

Adding an L2 ISID with Transparent UNI type

About this task

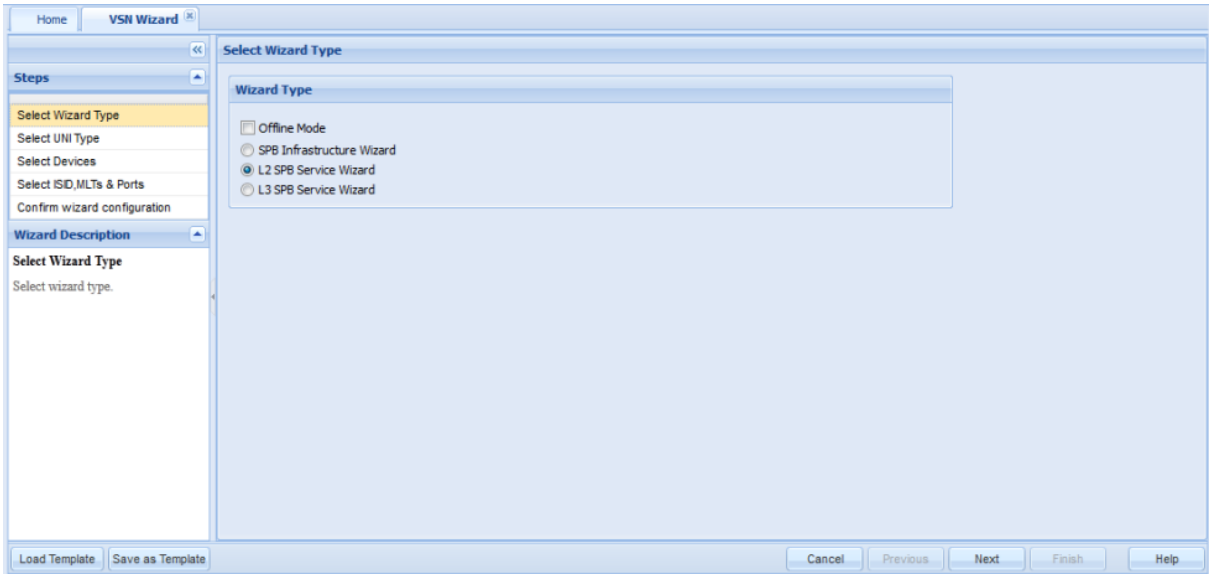
Perform the following procedure to add an L2 ISID with Transparent UNI type.

Procedure

1. From the **COM** navigation pane, select **Wizards**, and click the **VSN Wizard** icon.

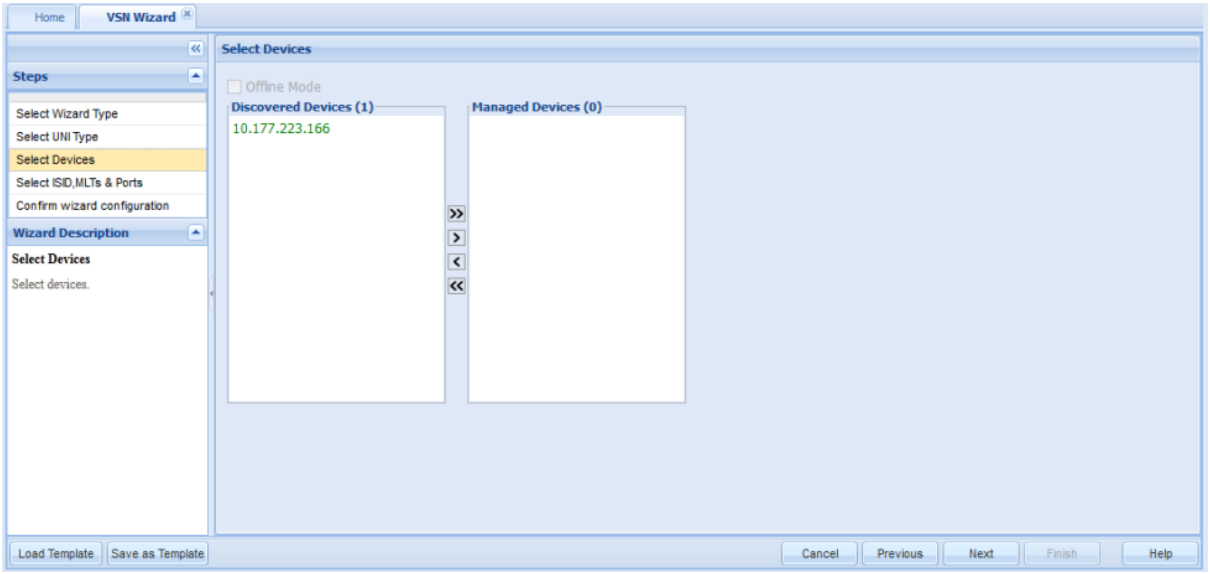
   The VSN Wizard tab opens.

2. In the Select Wizard Type area in the Contents pane, select **L2 SPB Service Wizard**.

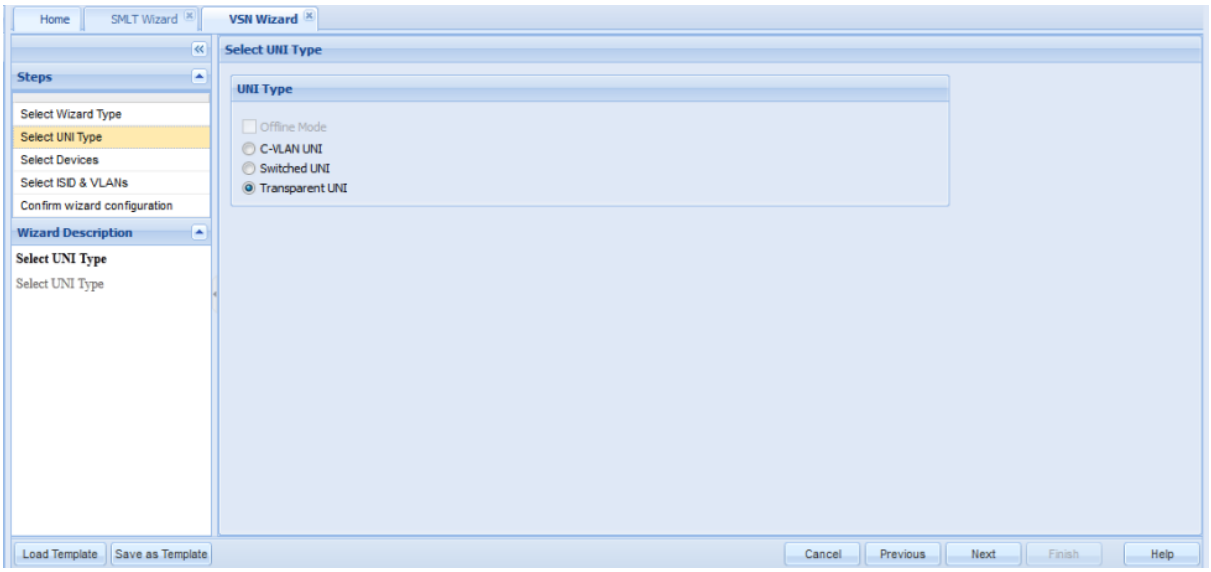


3. Click **Next**.

   The Select UNI Type window displays.

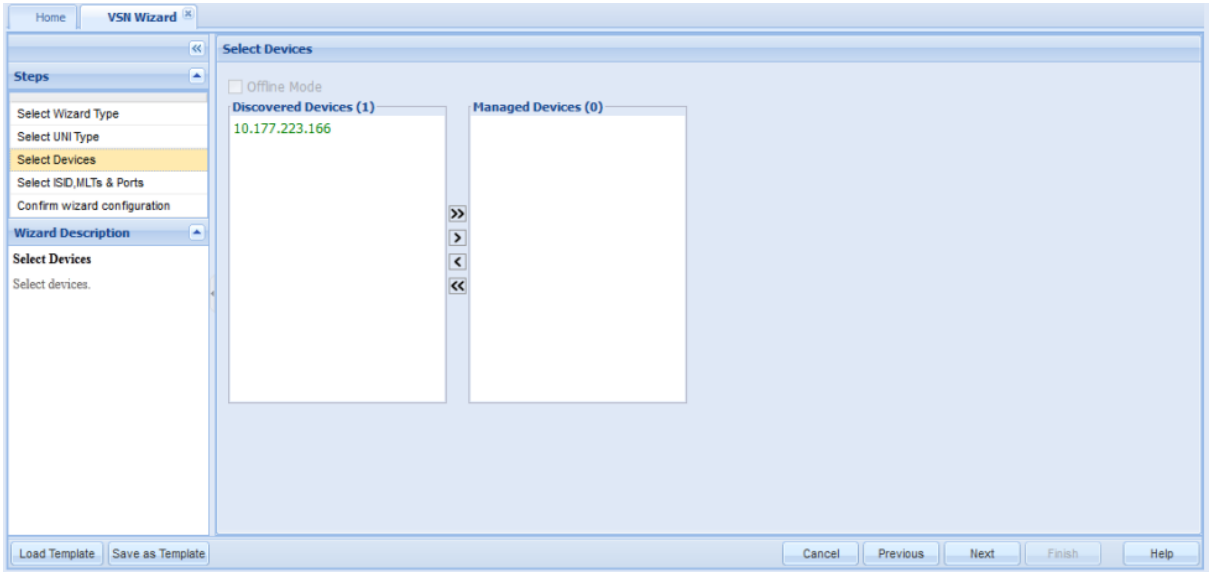


4. Select **Transparent UNI**.



5. Click **Next**.

   The Select Devices window displays.



6. From the Discovered Devices section, select the device(s).

   - 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 >**.
   - To move all devices from the Available Devices list to the Selected Devices list, click **Select All >>**.

   To unselect a device, from the Selected Devices table, select the required item and click **< Unselect** . To unselect all devices, click **<< Unselect All** .

7. Click **Next**.

   COM performs a VSN discovery and the Operation Completed box displays the results of the VSN discovery.

8. Click **OK**.

   The Select ISID, MLTs & Ports page displays.

9. In **ISID** field, enter an ISID number.
10. **Allow Ports/MLTs belonging to Vlans to be selected** is selected by default. You can clear this selection if you do not want to allow Ports/MLTs belonging to Vlans to be selected.
11. From the **VLAN** column drop-down box, select a VLAN.

    If there are no VLANs for a device, then you must add a VLAN.

12. Click **Launch the VLAN Wizard**.
13. After you complete the procedure for adding a VLAN, click the **VSN Wizard** tab.
14. Click **Refresh** and select the VLAN.
15. To view the information or make changes to the port currently mapped to the VLANs, in the **Port Members** column, double-click on a cell for a specific device.

    The Port Members window displays.

16. Add or remove ports, then click **Save**.
17. In the wizard frame, click **Next**.
18. Click **Finish** or if you choose to save the wizard configuration as a template, perform the following steps:
    a. Check the **Save as Template** check box.
    b. Enter a Template name.
    c. 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

Field	Description
	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 displays.

2. In the **Select Wizard Type** dialog box, select **L3 SPB Service Wizard**.

Note:

For information about working offline, see Offline mode on page 449

3. Click **Next**.

   The Select Devices screen displays.

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 supported versions of ERS 8600, ERS 8800 and VSP9000 display 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 Completed box displays the results of the VSN discovery.

6. Click **OK**.

   The Select ISID & VRFs screen displays.

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 displays.

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 displays.

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.
Route Source	Redistributes routes from the protocols you select into ISIS. You can select one or more of the following protocols: • Direct • Static

Field	Description
	• OSPF • RIP • BGP • Delete Unselected Redistributes 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: • ip vrf <vrfName> isis redistribute direct create • ip vrf <vrfName> isis redistribute direct enable • ip vrf <vrfName> isis redistribute direct apply 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: • ip vrf {vrfName} isis redistribute static delete • ip vrf {vrfName} isis redistribute ospf delete • ip vrf {vrfName} isis redistribute rip delete • ip vrf {vrfName} isis redistribute bgp delete 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. Refresh after the VLAN Manager updates.
Launch VRF Manager	Launches a pop-up window to create a VRF for the required device. 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 VSN 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 the VSN 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 450.

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 451.

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

Starting Templates Manager

Perform the following procedure to start the Templates Manager.

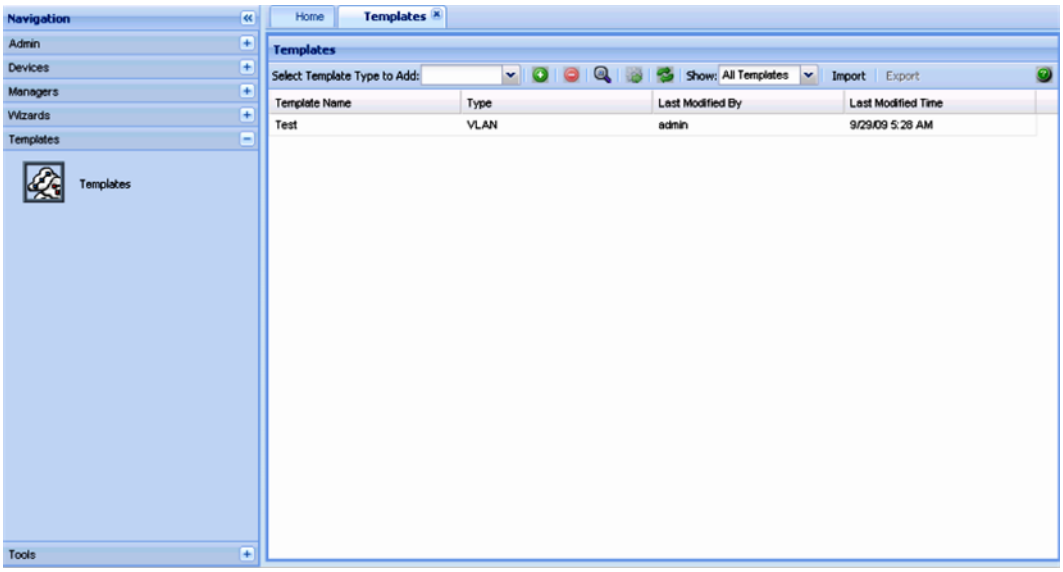
Procedure steps

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.

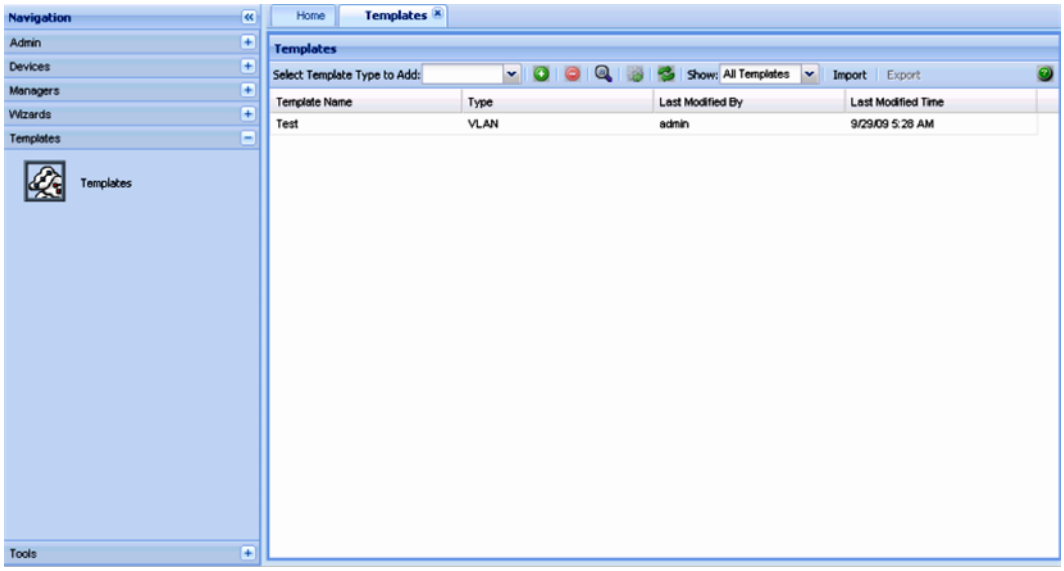


Figure 22: Templates Window

The following table explains the parts of the Templates window:

Table 183: Parts of the Templates window

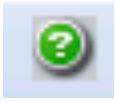
Part	Description
Tool bar	Provides quick access to commonly used Template commands. For more information, see Tool bar buttons on page 452.
Contents pane	Displays details of the templates. For more information, see Contents pane on page 453.

Tool bar buttons

The following table explains the different buttons on the tool bar.

Table 184: 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.
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.

Command	Tool bar button	Description
Show		Displays the templates depending on the value selected. The available values are as follows: • All Templates • VLAN only • 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.

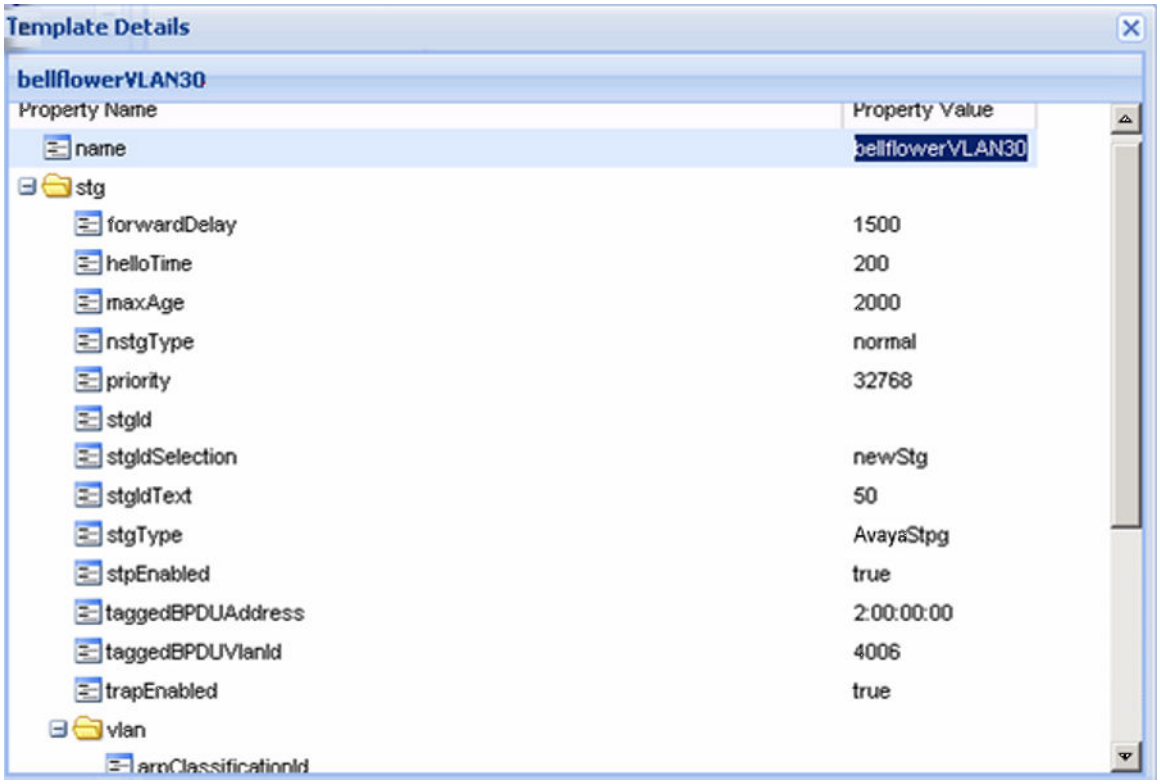


Figure 23: Template Details dialog box

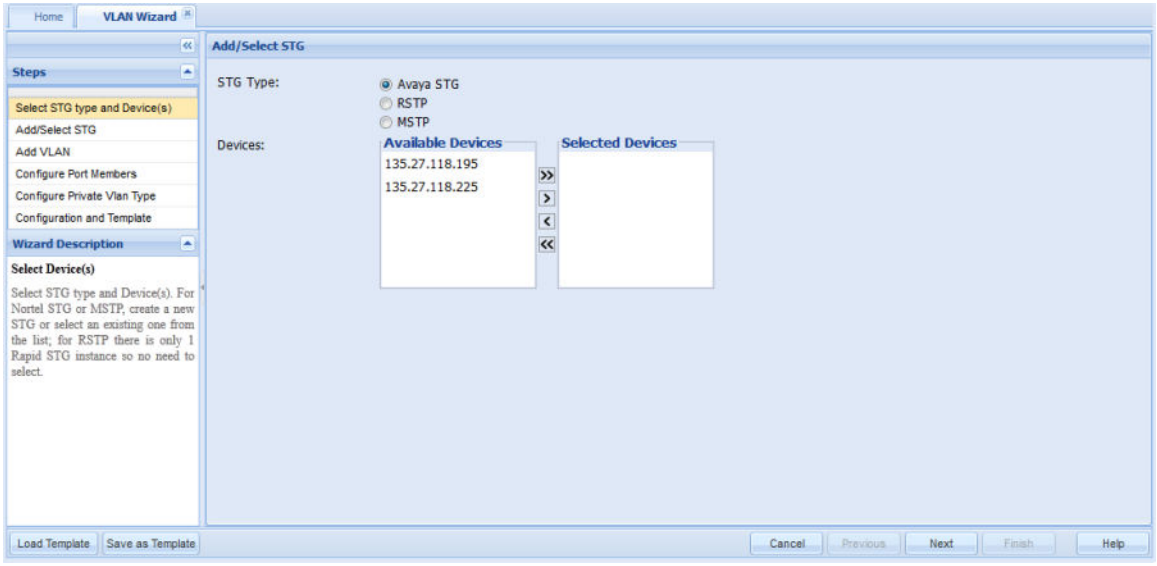
Adding a VLAN template

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 **Add new template using wizard** [(+) sign].

   The VLAN Wizard discovery occurs, and a Loading wizard data message displays. After the VLAN wizard discovery is complete, the VLAN Wizard window displays.



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 Configure Private VLAN page to view configuration details.

    This step is required when the added VLAN type is private.
12. Click **Next** to move on Configuration and Template page.
13. 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 420.
14. From the Template window, click **Refresh** to view the newly added template.

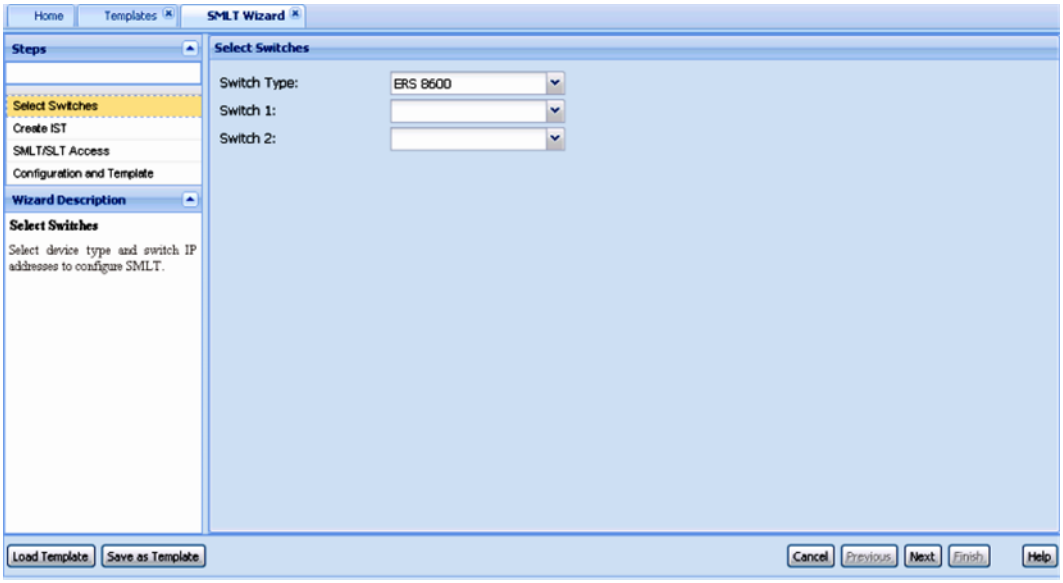
Adding a SMLT template

Perform the following procedure to add a SMLT template.

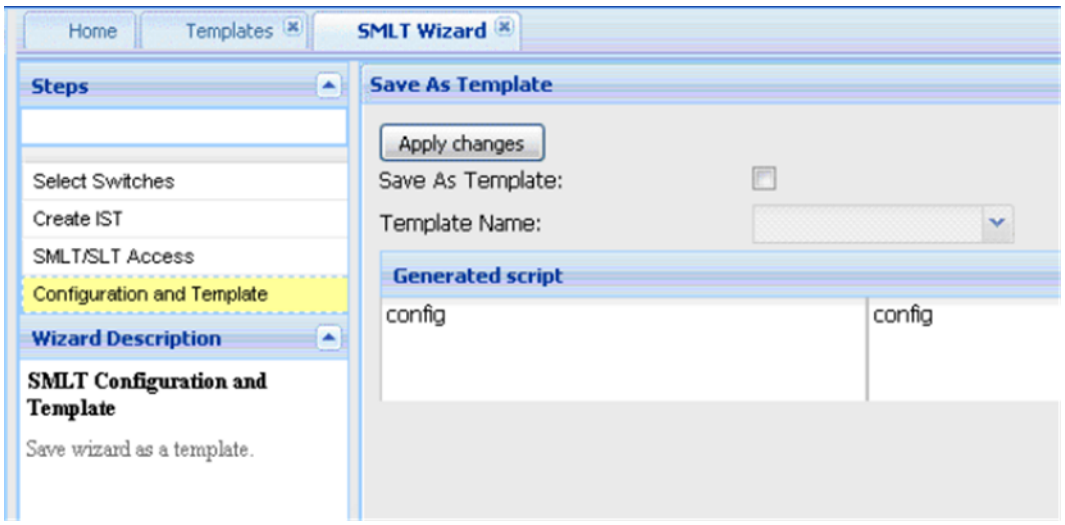
Procedure steps

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 427.

Adding a VSN template

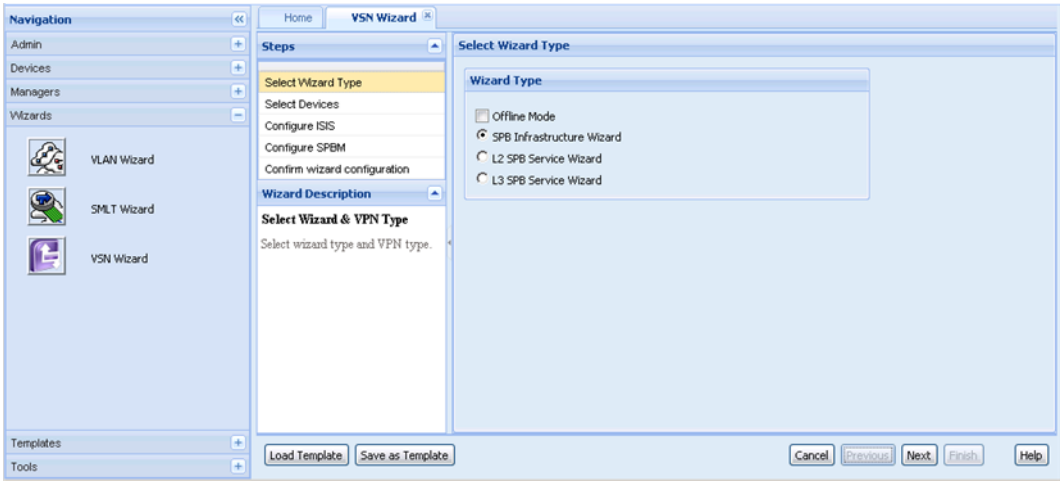
Perform the following procedure to add a VSN template.

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 displays.



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 433.

If you select the L2 SPB Service Wizard, see Using the L2 SPB Service Wizard on page 436.

If you select the L3 SPB Service Wizard, see Using the L3 SPB Service Wizard on page 445.

Deleting an existing template

Perform the following procedure to delete an existing template.

Procedure steps

1. 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.

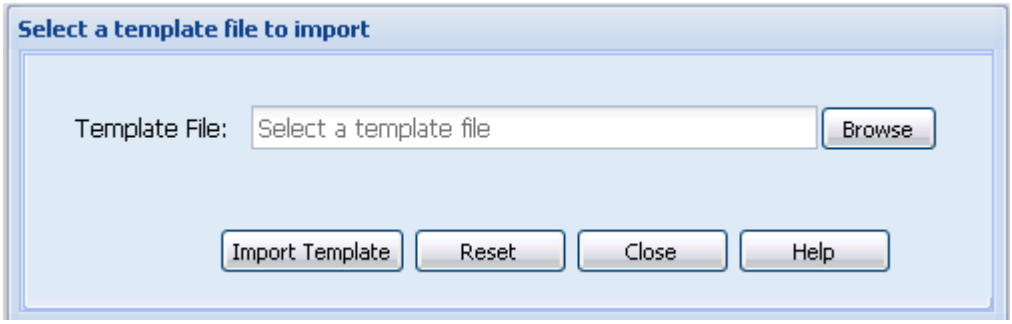
Importing a template

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.

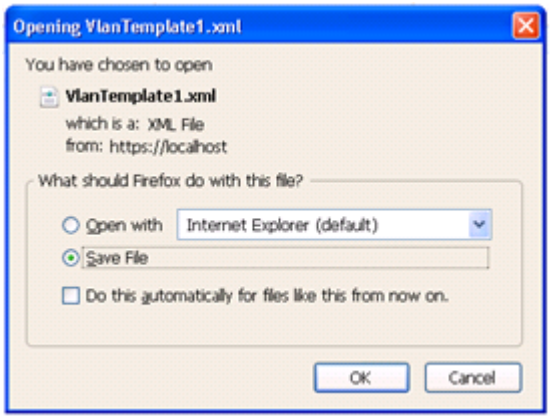
Exporting a template

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.