

ExtremeManagement™

Network Configuration using Extreme Fabric Orchestrator

Release 1.2
NN48100-501
Issue 03.01
December 2017

© 2017, Extreme Networks, 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, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. 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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks 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 or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks' 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

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks 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. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks' standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: <http://www.extremenetworks.com/support> under the link "Policies" or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

"Hosted Service" means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU

REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS 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 EXTREME NETWORKS INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE ("EXTREME NETWORKS").

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. 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 computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) 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.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks 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 Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Extreme Networks, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Extreme Networks' prior consent and payment of an upgrade fee.

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 Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks 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 Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

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 products, Documentation or on Extreme Networks' website at: <http://www.extremenetworks.com/support/policies/software-licensing> or such successor site as designated by Extreme Networks. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS

AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Extreme Networks product is used.

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.

Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at <https://gtacknowledge.extremenetworks.com/>.

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: <http://documentation.extremenetworks.com>, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

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

Contact Avaya Support

See the Avaya Support website: <https://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: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks 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 Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

For additional information on Extreme Networks trademarks, please see: <http://www.extremenetworks.com/company/legal/>

Contents

Chapter 1: Preface	11
Purpose.....	11
Training.....	11
Providing Feedback to Us.....	11
Getting Help.....	12
Extreme Networks Documentation.....	13
Subscribing to service notifications.....	13
Chapter 2: New in this document	14
Chapter 3: Network Configuration overview	15
Overview.....	15
VLAN.....	20
MLT.....	21
Routing.....	21
VRF.....	21
Multicast.....	22
Fabric Connect.....	22
Fabric Extend.....	23
Multimedia.....	24
Trap Log Registration	24
Security.....	24
Device Groups.....	25
File Inventory.....	25
Port channelization.....	26
Chapter 4: Managing access to configuration features using Role-based Access Control	27
About access to configuration features.....	27
Creating a custom role for configuration features.....	27
Chapter 5: Using Network Map	30
About Network Map.....	30
Understanding the topology map.....	31
Network Map contents pane.....	31
Managing the discovered devices.....	31
Discovery results.....	36
Working with multiple topologies.....	40
Chapter 6: Managing Device Groups	43
About Device Groups.....	43
Launching Device Groups.....	43
Device Groups tool bar options.....	44
Creating a device group.....	45

Editing a device group.....	46
Assigning device groups to a user.....	46
Editing device group assignments.....	47
Chapter 7: Using Network Table.....	49
About Network Table.....	49
Launching the Network Table.....	49
Network Table toolbar.....	49
Launching an Element Manager.....	50
Importing devices.....	51
Exporting devices.....	51
Chapter 8: Managing VLAN.....	52
About VLAN.....	52
VLAN.....	52
VLAN features.....	52
Spanning Tree Protocol.....	53
VLAN configuration.....	54
Starting VLAN view.....	55
VLAN view.....	56
Configuring Avaya Spanning Tree Groups.....	58
Create and configure VLANs for an Avaya STG.....	62
Managing Rapid Spanning Tree Protocol.....	68
Create and configure VLANs for RSTP.....	69
MSTP configuration.....	70
VLANs configuration for MSTP.....	71
Private VLAN.....	73
Configuring port members.....	74
Configuring routing on a VLAN interface.....	76
STG and VLAN information.....	77
Domain synchronization.....	86
Domain synchronization procedures.....	92
Chapter 9: Managing MultiLink Trunking.....	96
About MultiLink Trunking.....	96
Create and manage MultiLink Trunks.....	96
MultiLink Trunks in different switch types.....	97
MultiLink Trunking view features.....	98
Starting MLT view.....	98
MLT view.....	98
MLT management.....	104
MLT configurations.....	110
SMLT configuration.....	116
Chapter 10: Managing Routing.....	122
About Routing.....	122
Starting Routing view.....	122

Viewing Routing folder contents.....	125
Discover Routing.....	126
Adding devices.....	126
Setting Routing Manager preferences.....	127
Routing view features.....	128
Supported devices for Routing view.....	128
Viewing and configuring IPv4 routing.....	130
View and configure IPv6 routing.....	149
Chapter 11: Managing Virtual Routing and Forwarding.....	164
About Virtual Routing and Forwarding.....	164
VRF view.....	165
Starting VRF view.....	165
Adding VRF on a device or multiple devices.....	166
Setting VRF content for devices.....	168
Viewing VRF details.....	168
Editing a single or multiple VRF configurations.....	168
Deleting a VRF configuration from a device.....	169
VRF enhancement—VLAN and routing.....	169
Chapter 12: Managing Multicast.....	170
About Multicast.....	170
Multicast view.....	171
Starting Multicast view.....	171
Actions.....	171
Navigation tree structure.....	174
Using tables to change device configuration.....	174
IGMP and IGMP Snoop.....	174
DVMRP protocol folder.....	192
PIM SM protocol folder.....	198
MSDP Protocol folder.....	205
Multicast Route protocol folder.....	209
Policy folder.....	214
Highlight multicast data in the topology map.....	220
Chapter 13: Managing Fabric Connect.....	222
About Fabric Connect.....	222
Launching the Fabric Connect view.....	225
Fabric Connect view.....	225
Private VLAN overview.....	233
Etree overview.....	235
Editing Global Routing Table — IP Shortcuts.....	237
L2 SPBm functionality.....	238
L3 SPBm functionality.....	245
BGP-VPN.....	249
SPBm Multicast Route table.....	252

CFM Globals.....	252
Fabric topology.....	253
Fabric Attach.....	259
Chapter 14: Managing Fabric Extend.....	273
About Fabric Extend.....	273
Overview.....	273
Fabric Extend view.....	277
Chapter 15: Managing VXLAN.....	299
About VXLAN.....	299
VXLAN Network.....	300
VXLAN view navigation pane toolbar.....	302
VXLAN contents pane.....	302
Starting VXLAN view.....	303
VXLAN Manager view.....	303
Adding a CLIP interface.....	305
VXLAN Manager non Avaya device view.....	306
Adding a non Avaya VTEP.....	307
Viewing a remote VTEP.....	307
Adding a remote VTEP.....	308
Viewing VTEP VNI ELAN end points.....	309
Viewing a VNI.....	309
Adding a VNID on a device.....	309
Deleting a VNID from a device.....	310
Viewing VNID configured devices.....	310
Adding an Avaya device to a VNID.....	311
Deleting an Avaya VTEP from a VNID.....	312
Adding a non Avaya VTEP to a VNID.....	312
Deleting a non Avaya VTEP device from a VNID.....	312
Viewing VNID ELAN end points.....	313
Adding ELAN end points to the VNID.....	313
Deleting an ELAN from a VNID.....	314
Chapter 16: Managing Multimedia.....	315
About Multimedia.....	315
Multimedia view.....	315
Starting the Multimedia.....	316
Actions.....	316
Navigation tree structure.....	319
Using tables to change device configuration.....	319
ADAC tables.....	319
802.1ab LLDP tables.....	325
802.1ab Port dot1 tables.....	329
802.1ab Port dot3 tables.....	331
802.1ab Port med tables.....	334

Chapter 17: Managing Trap and Log Registration	339
About Trap/Log Registration.....	339
Starting Trap/Log Registration.....	339
Trap/Log Registration view.....	339
Discovering devices.....	341
Displaying Preferences.....	342
Traps configuration.....	342
Chapter 18: Managing Security	351
About Security.....	351
Supported devices for Security view.....	351
Starting Security view.....	353
Security view.....	353
Create and manage security groups.....	356
Configuring the authentication method.....	359
Configuring management access.....	364
Chapter 19: Managing File Inventory	391
About File Inventory.....	391
File management features.....	391
Inventory management features.....	394
Starting File Inventory view.....	394
Using the File Inventory view.....	395
Understanding the File Inventory navigation tree.....	399
Reloading Inventory Manager.....	433
Saving inventory information.....	434
Opening an inventory file.....	434
Saving inventory file in a tab delimited text file.....	435
Downloading files to devices.....	435
Uploading file from device.....	436
Backing up the configuration file.....	436
Saving backed up Config files locally.....	437
Restoring the configuration file.....	437
Archiving the configuration file.....	438
Synchronizing the configuration file.....	438
Performing a device upgrade.....	439
Using the Device Upgrade Wizard.....	439
Comparing Runtime configuration file.....	440
Setting File Inventory preferences.....	441
Chapter 20: Viewing Audit Logs	442
About Audit Logs.....	442
Audit Logs toolbar.....	442
Launching the Audit Log view.....	443
Audit log management.....	443
Chapter 21: Wizard	450

Contents

Wizard.....	450
VLAN wizard.....	450
SMLT wizard.....	456
Fabric wizard.....	464
Offline mode.....	481
Template support.....	481
Configuration of Templates.....	482
Chapter 22: Tools	490
Tools.....	490
Starting SmartDiff Tool.....	490
MIB Browser.....	491
MIB Query.....	495
Accessing the Port Scanner.....	495
Device Save Configuration Tool.....	499
ISID Name Management.....	499
Appendix A: Recommendations	503
Recommendations.....	503
Rediscovery of devices.....	503
Internet browser settings.....	503

Chapter 1: Preface

Purpose

This document provides information on configuring and managing the network using Extreme Fabric Orchestrator (EFO).

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

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

Product purchased from Extreme Networks

If you purchased your product from Extreme Networks, use the following support contact information to get help.

If you require assistance, contact Extreme Networks using one of the following methods:

- [GTAC \(Global Technical Assistance Center\) for Immediate Support](#)
 - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- [GTAC Knowledge](#) – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- [The Hub](#) – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- [Support Portal](#) – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Product purchased from Avaya

If you purchased your product from Avaya, use the following support contact information to get help.

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.

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for previous versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Subscribing to service notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to <http://www.extremenetworks.com/support/service-notification-form/>.
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: New in this document

The following sections detail what is new in *Network Configuration using Extreme Fabric Orchestrator*, NN48100–501.

Configuration UI enhancements

All Configuration UI components now display the System Name along with the IP Address in the <Device System Name> (IP Address) format. If the System Name is not set on the device, only the IP Address is displayed. Displaying System Name along with the IP address enables the Network Administrator to identify the devices easily in a large network.

Chapter 3: Network Configuration overview

Overview

Configuration views provide detailed device information and management capabilities. These configuration views are designed to provide specialized information in an easy-to-use interface that is consistent in layout across the tools. A network configuration view can request the topology view to update itself with information relevant to the configuration view. For example, VLAN view can instruct the system to highlight all the devices in the view that includes members of a particular VLAN.

You can manage user access to configuration features using Role-based Access Control (RBAC). For more information, see [About access to configuration features](#) on page 27.

The system supports the following network configuration views:

- VLAN
- MultiLink Trunking (MLT)
- Routing
- Virtual Routing and Forwarding (VRF)
- Multicast
- Fabric Connect
- Fabric Extend
- Multimedia
- Trap/Log Registration
- Security
- Device Groups
- File Inventory

The following table lists the supported devices for each network configuration view.

 **Note:**

Not all configuration views are supported for each device or device version.

Configuration view	Device
VLAN	<ul style="list-style-type: none"> • Virtual Services Platform 9xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Virtual Services Platform 4xxx • Ethernet Switch/Ethernet Routing Switch 25xx • Ethernet Routing Switch 16xx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 5xxx/4xxx/35xx • Legacy Ethernet Routing Switch 1424 • Legacy Baystack • Passport 1000 Series switch • Wireless Controller 8xxx • Business Policy Switch 2000 • Alteon • WLAN AP
MLT	<ul style="list-style-type: none"> • Virtual Services Platform 9xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Virtual Services Platform 4xxx • Ethernet Switch/Ethernet Routing Switch 25xx • Ethernet Routing Switch 16xx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 5xxx/4xxx/35xx • Legacy Ethernet Routing Switch 1424 • Ethernet Switch 380, 410/450, 325/425/420, 460/470 • Legacy BayStack • Wireless Controller 8xxx • Passport 1000 Series switch • Business Policy Switch 2000 • Alteon • OM 1000 • WLAN AP
Routing	<ul style="list-style-type: none"> • Virtual Services Platform 9xxx

Table continues...

Configuration view	Device
	<ul style="list-style-type: none"> • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Virtual Services Platform 4xxx • Ethernet Switch/Ethernet Routing Switch 25xx • Ethernet Routing Switch 16xx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 5xxx/4xxx/35xx • Legacy Ethernet Routing Switch 1424 • Legacy Baystack • Wireless Controller 8xxx • Alteon • WLAN AP
VRF	<ul style="list-style-type: none"> • Virtual Services Platform 9xxx • Virtual Services Platform 7xxx • Virtual Services Platform 8xxx • Virtual Services Platform 4xxx • Ethernet Routing Switch 8300/8600 • Ethernet Routing Switch 8800 • Ethernet Routing Switch 5xxx
Multicast	<ul style="list-style-type: none"> • Virtual Services Platform 9xxx • Virtual Services Platform 4xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Ethernet Switch/Ethernet Routing Switch 25xx • Ethernet Routing Switch 16xx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 5xxx/4xxx/35xx • Legacy Ethernet Routing Switch 1424 • Legacy Baystack • Passport 1000 Series switch • Wireless Controller 8xxx • Alteon • WLAN AP

Table continues...

Configuration view	Device
Fabric Connect	<ul style="list-style-type: none"> • Virtual Services Platform 9xxx • Virtual Services Platform 8xxx • Virtual Services Platform 70xx • Virtual Services Platform 72xx • Virtual Services Platform 4xxx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 59xx • Ethernet Routing Switch 48xx
Fabric Extend	<ul style="list-style-type: none"> • Virtual Services Platform 8xxx • Virtual Services Platform 72xx • Virtual Services Platform 4xxx <p>This device does not support Fabric Extend natively and requires Open Networking Adapter (ONA).</p>
Multimedia	<ul style="list-style-type: none"> • Virtual Services Platform 9xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Virtual Services Platform 4xxx • Ethernet Switch/Ethernet Routing Switch 25xx • Ethernet Routing Switch 16xx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 5xxx/4xxx/35xx • Legacy Ethernet Routing Switch 1424 • Ethernet Switch 460/470 • Legacy Baystack • Wireless Controller 8xxx • Alteon • WLAN AP
Trap/Log Registration	<ul style="list-style-type: none"> • Virtual Services Platform 9xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Virtual Services Platform 4xxx • Ethernet Switch/Ethernet Routing Switch 25xx • Ethernet Routing Switch 16xx • Ethernet Routing Switch 8xxx

Table continues...

Configuration view	Device
	<ul style="list-style-type: none"> • Ethernet Routing Switch 5xxx/4xxx/35xx • Legacy Ethernet Routing Switch 1424 • Legacy Baystack • Wireless Controller 8xxx • Alteon • WLAN AP
Security	<ul style="list-style-type: none"> • Virtual Services Platform 9xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Virtual Services Platform 4xxx • Ethernet Switch/Ethernet Routing Switch 25xx • Ethernet Routing Switch 16xx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 5xxx/4xxx/35xx • Ethernet Switch 325/425/420, 460/470 • Passport 1050/1150/1200/1250 • Wireless Controller 8xxx • Business Policy Switch 2000
File Inventory	<ul style="list-style-type: none"> • Virtual Services Platform 9xxx • Virtual Services Platform 8xxx • Virtual Services Platform 7xxx • Virtual Services Platform 4xxx • Ethernet Switch/Ethernet Routing Switch 25xx • Ethernet Routing Switch 16xx • Ethernet Routing Switch 8xxx • Ethernet Routing Switch 5xxx/4xxx/35xx • Legacy Ethernet Routing Switch 1424 • Legacy BayStack • Alteon • WLAN AP • Wireless Controller 8180

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

- For VLAN, see [About VLAN](#) on page 52.
- For MLT, see [About MultiLink Trunking](#) on page 96.
- For Routing, see [About Routing](#) on page 122.
- For VRF, see [About Virtual Routing and Forwarding](#) on page 164.
- For Multicast, see [About Multicast](#) on page 170.
- For Fabric Connect, see [About Fabric Connect](#) on page 222.
- For Fabric Extend, see [About Fabric Extend](#) on page 273.
- For Multimedia, see [About Multimedia](#) on page 315.
- For Trap/Log Registration, see [About Trap and Log Registration](#) on page 339.
- For Security, see [About Security](#) on page 351.
- For File Inventory, see [About File Inventory](#) on page 391.

VLAN

VLAN view enables you to manage VLAN and STG configurations across a single device or multiple devices. You can access the VLAN view only if the administrator has assigned this user role to you. In the VLAN view, you can only access the devices that are assigned to you by a security administrator.

The context setting defines VLAN accessibility for users based on their domain of responsibility. The context setting also determines whether topology maps render for users at login. When a user changes the context, a notification is sent to all opened configuration views with the same logged in user. All opened configuration views are refreshed upon this notification.

With VLAN view you can perform the following tasks:

- add, delete, modify and monitor VLAN and Spanning Tree across one or more devices
- view and edit VLAN nodes across the network
- view and edit port membership information for ports not belonging to an STG
- view and edit port membership information for ports belonging to one, or more than one STG
- view and edit port membership information for individual routing ports and bridge routing ports
- view Spanning Tree configuration information in the topology map, such as the ports that are blocking or forwarding; the user device is the root of the Spanning Tree configuration
- view and edit port membership information for private VLAN ports

For more information about the configuration of VLAN view, see [About VLAN](#) on page 52.

MLT

MLT is a point-to-point connection that aggregates multiple ports so that they logically act like a single port with the aggregated bandwidth. Grouping multiple ports into one logical link means achieving higher aggregate throughput on a switch-to-switch or server-to-server application.

You can configure MLT across multiple devices, and perform the following tasks.

- Create, delete, or modify MLT and Split Multilink Trunks (SMLT).
- View or configure MLT configuration information such as port and VLAN membership.

For more information about the configuration of MLT, see [About MultiLink Trunking](#) on page 96.

Routing

You can use Routing view to configure routing parameters for devices across a network.

Routing view supports the following protocols.

- IP Routing
- RIP
- OSPF
- ARP
- VRRP
- IPv6 Routing
- IPv6 OSPF

With Routing view you can 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 more information about the configuration of Routing view, see [About Routing](#) on page 122.

VRF

You can use VRF view to manage configurations across specific devices. Additionally, you can set the current configuration for each device.

To start VRF view, the administrator must perform the following tasks:

- assign the VRF user role to you.
- assign devices to you.

With VRF view you can perform the following tasks:

- view all VRFs and VRF statistics configured for a specific device.
- edit single or multiple VRF configurations.
- add a new VRF to a device.
- delete a VRF from a device.
- set the current VRF configuration for each device.

For more information about the configuration of VRF, see [About Virtual Routing and Forwarding](#) on page 164.

Multicast

You can use Multicast view to manage Extreme Networks devices that support multicast. The Multicast view displays multicast configurations across a network of devices. You can edit the Multicast view and highlight multicast information on the topology map. However, to fully configure the multicast network, you must use EDM or JDM.

The Multicast view 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

For more information about the configuration of Multicast, see [About Multicast](#) on page 170.

Fabric Connect

The Fabric Connect view is a MultiElement manager with which you can manage L2 Shortest Path Bridging MAC (SPBm) and L3 VSNs throughout the discovered network on ERS 8000 v7.1 and above devices, VSP 4000 v3.0.1 and above, VSP 7000 v10.2 and above, VSP 8000 v4.0, and VSP 9000 v3.4 and above devices.

The Fabric Connect view supports Fabric Connect and Fabric Attach, and provides a Device-centric view of the VSNs, and a Fabric-centric view of the networks for both features.

Fabric Connect

With the Fabric Connect view you can perform the following tasks:

- add, delete, or edit L2 VSNs and L3 VSNs across multiple devices

- configure Multicast-over-SPBm (MoSPBm) on L2-VSN, L3 VSN, and IP Shortcuts on ERS 8000 v7.2,x, VSP 9000 v3.4 and v4.0, and VSP 4000 v3.1 devices
- view SPBm Multicast Routes tables
- display the Multicast Tree by (S, G, V) and perform diagnosis using L2 Trace MRoute option in the SPBm Topology view

For more information about the configuration of Fabric Connect, see [About Fabric Connect](#) on page 222.

Fabric Attach

The Fabric Attach feature extends the flexibility and extensibility of Fabric Connect to non-fabric platforms and provides users with additional automation and service enhancements.

With Fabric Attach, users have a visual display of capable devices through a single GUI. You have the ability to verify that a device can securely connect to the network or authorize a device for a network service.

Fabric Attach supports the following modes:

- Fabric Attach Server: VOSS and ERS 59xx devices
- Fabric Attach Proxy: ERS 48xx, ERS 59xx, VSP 70xx devices
- Fabric Attach Stand Along Proxy: ERS 48xx, ERS 59xx and VSP 70xx devices

For more information the Fabric Attach feature, see [Fabric Attach](#) on page 259.

Fabric Extend

The Fabric Extend view provides a graphical management interface for administrators to configure fabric extensions.

Every Fabric Extend network deployment involves creating numerous bidirectional tunnels. Fabric Extend view automates the provisioning of these tunnels by using Fabric Extend domains. When you add nodes to a Fabric Extend domain, Fabric Extend view automatically creates tunnels between the nodes belonging to the same domain. Fabric Extend view also ensures error-free bidirectional tunnel provisioning.

Fabric Extend functions

Fabric Extend view provides the following functions:

- Identifies Fabric Extend capable switches.
- Provides an easy way to group and manage a set of Fabric Extend capable switches using domains characterized by the type of topology the group forms. For example: Mesh, Hub-and-Spoke.
- Provides an easy way to configure and manage point-to-point fabric extensions.

For more information about the configuration of Fabric Extend, see [About Fabric Extend](#) on page 273.

Multimedia

The Multimedia view manages Auto Detection/Auto Configuration (ADAC) and 802.1ab parameters of the Extreme Networks 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 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

For more information about the configuration of Multimedia, see [About Multimedia](#) on page 315.

Trap Log Registration

You can use the Trap/Log Registration view to configure and view the traps or notifications, and the System Log. The Trap/Log Registration combines the functionality of the Trap Receiver and Log Manager from previous releases, and provides additional capabilities to configure traps, notifications, and syslogs.

For more information about Trap/Log Registration, see [About Trap and Log Registration](#) on page 339.

Security

With Security view you can manage access to device and network management functions on discovered network devices.

You can synchronize, change, and view security features for the following:

- Command Line Interface (CLI) access
- Web access
- Simple Network Management Protocol (SNMP) access
- Access policies
- Remote Access Dial-In User Services (RADIUS) properties
- SNMPv3 properties

- Secure Shell (SSH) bulk password
- Terminal Access Controller Access-Control System (TACACS)

You can configure the network access for each application using one or more security groups that you manage independently. If you want a group of devices to have the same passwords and access features, use security groups to group the devices together.

For more information about the configuration of Security, see [About Security](#) on page 351.

Device Groups

You can use the Device Groups view to create and manage device groups and device group assignments.

With Device Groups you can perform the following:

- use device groups to group a number of discovered devices
- use device 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 what default topology is displayed for the user in Network Map view.

For more information about the Device Groups, see [About Device Groups](#) on page 43.

File Inventory

You can use File Inventory view to manage the hardware and software configurations for different devices.

With File Inventory you can perform the following tasks:

- 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

For more information about the File Inventory, see [About File Inventory](#) on page 391.

Port channelization

Use the channelization feature to configure 40 Gbps QSFP+ ports to operate as four 10 Gbps ports. You can use QSFP+ to four SFP+ breakout cables to connect the 10 Gbps ports to other servers, storage devices, or switches.

*** Note:**

Not all Extreme Networks products provide 40 Gbps ports. Not all 40 Gbps ports support channelization. For more information, see the product-specific documentation.

To enable or disable channelization for a 40 Gbps port, you must use Enterprise Device Manager (EDM) to configure the specific device port. For more information, see [Launching an Element Manager](#) on page 50.

The port numbering syntax is different for channelized ports. If the device supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port. The following list illustrates the syntax differences for the first 40 Gbps port in slot 2:

- Non-channelized: 2/1 (slot/port)
- Channelized: 2/1/1, 2/1/2, 2/1/3, and 2/1/4 (slot/port/sub-port)

To configure a feature on the third sub-port, or channel, of the preceding example port, you need to specify the syntax as 2/1/3 when you provide the port information.

The change to the port numbering syntax is visible. Any feature that requires you to select ports as part of the configuration uses the slot/port/sub-port syntax for channelized ports. For example, in VLAN view, if a channelized port is a member of a VLAN, the system displays the slot/port/sub-port information in the appropriate fields. Most features that you can configure on a non-channelized 40 Gbps port can also be configured on a channelized port. For information about any feature exceptions, see the product specific documentation.

When a 40 Gbps port is channelized, use only breakout cables in it. Otherwise, the link behavior can be unpredictable because it can result in mismatched link status between link partners, which can further lead to network issues.

Also, avoid the use of breakout cables in non-channelized 40 Gbps ports because this can result in mismatched link status between link partners, which can lead to network issues.

Chapter 4: Managing access to configuration features using Role-based Access Control

About access to configuration features

You can use Role-based Access Control (RBAC) to manage and control user access to different configuration features in AFO.

AFO has three built-in roles that have default privileges for accessing configuration features.

The following table describes the built-in roles and the privileges for configuration features.

Built-in roles	Privilege for configuration features
AFO Network Administrator	Read-Write for all features
AFO Network Operator	Read only for all features
AFO System Administrator	Read-Write for all features

If the built-in roles are not suitable for a user, you can control access to specific features.

To control privileges for each feature, you must create custom roles. If you have an AFO System Administrator role, you can create and assign custom roles to control user access to configuration features.

Creating a custom role for configuration features

Use this procedure to create a custom role and assign the role to a user.

If you migrated data from a previous release version or legacy product to AFO, the data for the access control is not migrated because in these new products, the configuration feature access control is performed using the Role-based access control (RBAC). Use this procedure to manually add access control to existing users.

Before you begin

Log on to the system as the administrator. In the User ID field, enter `admin`.

Procedure

1. Select **Administrator > System Management**.
2. In the Users section, select **Administrators**.
3. In the Security section, click **Roles**.
4. Expand the **System Administrator** folder.
5. Click **AFO Network Administrator**, and then click **New**.
6. Enter a role name and enter a role description, and then click **Commit and Continue**.
7. To select element or network service, or both, to map to a created role, click **Add Mapping**.
8. In the Element or Resource Type field, select **AFO Primary Roles**.
9. In the Element or Resource Instance field, select **All**.
10. Click **Next**.
11. Select the check box for **Select/Unselect All**, and then click **Commit**.
 - If you have migrated data from a previous version or legacy product, check the ReadWrite check boxes for the managers you want to assign to the existing user.
12. To select element or network service, or both, to map to a created role, click **Add Mapping**.
 - If the user already exists due to data migration from a previous release version or legacy product, skip this step.
13. In the Element or Resource Type field, select **AFO Configuration Services**.
 - If the user already exists due to data migration from a previous release version or legacy product, skip this step.
14. In the Element or Resource Instance field, select **All**.
 - If the user already exists due to data migration from a previous release version or legacy product, skip this step.
15. Deselect the **Select/Unselect All** check box.
 - If the user already exists due to data migration from a previous release version or legacy product, select the existing user ID.
16. To add a manager to the newly created role, select a manager, and click the ReadWrite check box for that manager. Repeat this step for each manager you want to add to the role.
 - If the user already exists due to data migration from a previous release version or legacy product, select the new role that you created.
17. Click **Commit**.
18. In the Role Details section, click **Commit**.

You can view the role you created in the Roles navigation tree in the AFO Network Administrator folder.

19. In the User Services section, click **Administrative Users**.
20. To create the user, in the Administrative Users section, click **Add**.
21. Enter the user ID, full name of the user, a temporary password, and then click **Commit and Continue**.
22. Click **Commit**.
23. Click on the created user, and in the Roles section, click **Select Roles**.
24. Select the check box of the role you created for the user, and click **Commit**.
25. In the User details section, click **Commit**.
26. Log out of the system, and log back on to the system using the ID of the user created and the temporary password.
27. Change the temporary password.
28. Verify the permissions given to the user.

Chapter 5: Using Network Map

About Network Map

The topology feature displays a topology of the devices discovered using Monitoring through the built-in domain Default. The Network Map view creates a topology map showing the devices discovered by Monitoring and the connections between them. You can use the Network Map 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 using the following:
 - dump topology
 - learned MAC addresses
 - port status
 - ping
 - connections
- 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 the configuration view again.
- reload topology of the discovered devices using Monitoring.

You can perform device discovery using Monitoring, by selecting **Network > Discovery** from the menu bar. The Network Map in the configuration view displays the topology map once the device

discovery is completed by Monitoring. A discovery is a snapshot taken of part, or all, of a network. When you perform a discovery, the information that the system collects to create the topology map is also used to populate the Network Table.

For more information on configuring device credentials for network discovery, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

For more information on performing a device discovery, see *Network Monitoring using Extreme Fabric Orchestrator*, NN48100–500.

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 [Discovery results](#) on page 36. 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 31.

Network Map contents pane

The contents pane provides a view of all the discovered devices and their relationship on the Network Map tab. You can use the tool bar on the Contents pane to manage discovered devices on the topology map.

You also can use the right-click menu options on the Contents pane to perform device query and administrative management. To access the right-click menu options, right-click a device on the topology map. One set of device actions includes query management such as ping devices, connection information, device properties, Launch Element Manager, and port status. The second set of device actions includes administration management, such as Create a Group, Update device topology, and change device IP address. You also can access the right-click menu options by selecting **Device Inventory View**, and then clicking **Perform Device Action**.

Managing the discovered devices

About this task

You can use Perform Device Action to manage the discovered devices on the topology map or inventory grid. The device management takes place on the Network Map and on the Network Table.

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

1. Perform one of the following:
 - Select **Configuration > Network Map**.
Select a device on the topology map or inventory grid and right-click on the device.
 - Select **Configuration > Network Table**.
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.

Device management options

Device management options from the right-click menu on the topology

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






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: <ul style="list-style-type: none"> • 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.
Port Status	Use this option to display the status of the port. <ul style="list-style-type: none"> •  green—the port is in-service •  red—the port is out-of-service

Table continues...

Menu option	Description
	<ul style="list-style-type: none">  blue—the port is being tested  light blue—the port is enabled for Fabric Attach  orange—the port is disabled for Fabric Attach
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	<p>Use this option to change the device attributes. Perform one of the following actions:</p> <ul style="list-style-type: none"> Create a Group—This option appears on the topology map of the Network Map tab only. Update device topology Change device IP Address Close <p>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 system updates the database with the discovered information.</p>
Close	Closes the drop down menu.

Device management options from the Network Map tab Perform Device Action button

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






Menu option	Description
Show Port Status	<p>Use this option to display the status of the port.</p> <ul style="list-style-type: none">  green—the port is in-service  red—the port is out-of-service  blue—the port is being tested

Table continues...

Menu option	Description
	<ul style="list-style-type: none"> •  light blue—the port is enabled for Fabric Attach •  orange—the port is disabled for Fabric Attach
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	<p>Use this option to display the following properties of the device:</p> <ul style="list-style-type: none"> • 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 Addresses	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	<p>Use this option to change the device attributes. Perform one of the following actions:</p> <ul style="list-style-type: none"> • Create a Group —This option appears on the topology map of the Network Map tab only. • Update Device Topology • Change IP Address <p>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 system updates the database with the discovered information.</p>

Device management options from the Network Table Perform Device Action button

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






Menu option	Description
Show Port Status	<p>Use this option to display the status of the port.</p> <ul style="list-style-type: none">  green—the port is in-service  red—the port is out-of-service  blue—the port is being tested  light blue—the port is enabled for Fabric Attach  orange—the port is disabled for Fabric Attach
Ping Device	Use this option to ping the selected device from the server.
Show Properties	<p>Use this option to display the following properties of the device:</p> <ul style="list-style-type: none"> 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.

Table continues...

Menu option	Description
Administrative Actions	<p>Use this option to change the device attributes. Perform one of the following actions:</p> <ul style="list-style-type: none"> • Create a Group —This option appears on the topology map of the Network Map tab only. • Update Device Topology • Change IP Address <p>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 system updates the database with the discovered information.</p>

Discovery results

This section provides information about managing the discovery results and displaying information on the topology map. The Network Map default view contains the devices that belong to the current device group context of the user. If the current context is not assigned to the user, the default view contains all the discovered devices.

When the network discovery is initiated, the system provides the discovery status on the status bar of each configuration view. The status bar provides the following information:

- Discovered information:
 - Icon to represent the discovery status
 - Blue — Not started
 - Green — Completed
 - Blinking green — In progress
 - Red — Failed or stopped
 - Devices — Number of devices discovered .
 - Links — Number of links discovered.
 - Last discovered time stamp — For example, Topology updated on : 09/21/2016 02:44:33 PM
- Topology information:
 - Number of devices loaded and rendered in Network Map/Network Table
 - Number of links discovered and rendered in Network Map/Network Table
 - Last discovered time stamp

*** Note:**

Topology information is not updated after you select **Reload Network Map**. Topology information is updated only after you perform a discovery through **Network Discovery**.

When the network discovery completes, a dialog box displays confirming the completion and prompts the user to refresh the current configuration view.

Managing the discovery results

About this task

You can use the tool bar buttons on the Network Map 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

1. Select **Configuration > Network Map**.
2. Use the buttons on the tool bar to navigate the topology map.



Network Map tool bar options

Option	Description
Context	<p>Use this option to select the available groups assigned to the current logged in user.</p> <p>After you change the context, a notification is sent to all opened configuration views in the system with the same logged in user. All opened views are refreshed after receiving this notification.</p> <p>* Note:</p> <p>After you change the context, the Network Map view changes temporarily. Save the context to make the changes permanent.</p>
Save Context	Use this option to save the context.
Revert to Current Context	Use this option to revert to the current context.
Refresh Groups	Use this option to view the new groups added to the current logged in user.
Show All	<p>Use this option to view all discovered nodes in the system.</p> <p>Displaying devices in topology map is based on the context selected. When the current device group context is not assigned to the user, the default selection is Show All. When this option is selected, context view selection is disabled automatically.</p>

Table continues...

Option	Description
Reload Network Map	Use this option to reload the latest discovered devices and to redraw the network topology based on the discovered devices. The application communicates with the server to get the latest discovered devices
Refresh Topology	Use this option to refresh the topology map based on the current discovered devices.
Zoom Out	Use this option to zoom out the topology map.
Zoom In	Use this option to zoom in the topology map.
Clear Highlights	Use this option to clear the existing highlights on the topology map.
View Device Information	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>Use this option to perform the following actions on a topology map device:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> - create a group - update device topology - change IP address

Table continues...

Option	Description
	<p>You also can access these options through the right-click menu of a device on the Network Map or Network Table tabs.</p> <p> Note:</p> <p>These options are available only when you select a device. Otherwise, the options are disabled.</p>
Search for device IP / SysName	<p>Use this option to search and highlight an IP address or System name you are looking for. You can search based on:</p> <ul style="list-style-type: none"> • a partial or full IP address • a partial or full System name • IPv4 format • IPv6 format <p> Important:</p> <p>If the device is not found, then a topology dialog box appears showing, <code>No additional matches found.</code></p>
Save Topology	<p>Use this option to save the current topology and export it to an XML file which you can load into the system. This provides a way for you to save multiple topologies without having to do a rediscovery.</p>
Clear saved Topology	<p>Use this option to return to the topology that you had previously saved.</p>
Import/Export Topology	<p>Use this option to export in xml and csv, and import in xml formats.</p>
Device navigation window	<p>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.</p> <p>Use Minimize and Maximize to show and hide the area behind the device navigation window.</p>

Displaying information on the topology map

About this task

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

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

Procedure

1. Select **Configuration > Network Map**.
2. From the tool bar, click **View Device Information**.
3. Select the required option from the following:
 - Display port names
 - Toggle Addr / Name
 - Link Data

View Device Information menu

Name	Description
Display port names	Select the check box to display port names on the topology map.
Toggle Addr / Name	Select the check box to toggle between system name and IP address of the device on the topology.
Link data	<p>Select the link details to view:</p> <ul style="list-style-type: none"> • Link Speeds • Link Duplex • Link Types • Link Mismatch • Clear Highlights <p>The system displays the real-time settings for the interface attributes, and highlights the topology map based on the discovered data.</p>

Working with multiple topologies

The Network Map tab displays one active topology at a time, but you can work with multiple topologies if needed. You can export a saved topology from the Network view or from the Inventory, and then discovery a new topology. To work with the saved topology, you can import it using the Import/Export Topology or the Inventory. When you import a saved topology, the existing topology is overwritten by the data in the imported file.

Saving a topology

About this task

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

1. Select **Configuration > Network Map**.

2. Click **Save Topology** on the toolbar, located to the right of the Search for device IP / SysName field.
3. Click **OK** when prompted.

Drawing a topology

You can create a topology map from the Network Table. The system displays an inventory grid on the Network Table tab. After you select Draw Topology, the system renders a logical topology map of your network.

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

Procedure

1. Select **Configuration > Network Table**.
2. From the Network Table tool bar, select **Draw Topology**.

The topology map renders and displays on the Network Map tab.

Exporting and importing a topology from the Network Table

About this task

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 the system.

Procedure

1. Select **Configuration > Network Table**.
2. To save an existing topology, select a device from the device table.
3. From the Network Table tool bar, click **Import/Export Inventory**.
4. Select **Export inventory to an XML file** or **Export Device List to CSV File**, and then click **Export**.
5. Click **Save**.
6. Initiate a new device discovery using Network Discovery.

For information on performing device discovery, see *Network Monitoring using Extreme Fabric Orchestrator*, NN48100–500.

7. To save the currently active topology, repeat steps [2](#) on page 41 through [5](#) on page 41.
8. To reload the original topology, from the Network Table tool bar, click **Import/Export Inventory**.
9. Select **Import inventory from an XML file**, and then click **Browse** to navigate to the location of the file.
10. Select the file, and then click **Open**.
11. Click **Import**.

Result

The table in the Network Table view and the topology map in the Network Map view are updated.

Exporting and importing a topology from the Network Map

About this task

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 the system..

Procedure

1. Select **Configuration > Network Map**.
2. To save an existing topology, Click **Import/Export Topology**, located on the right side of the tool bar.
3. Select **Export inventory to an XML file** or **Export Device List to CSV File**, and then click **Export**.
4. Click **Save file**.
5. Initiate a new device discovery using Network Discovery.
For information on performing device discovery, see *Network Monitoring using Extreme Fabric Orchestrator*, NN48100–500.
6. To save the currently active topology, repeat steps [1](#) on page 42 through [4](#) on page 42.
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**.

Chapter 6: Managing Device Groups

About Device Groups

You can use the Device Groups view to create and manage device groups and device group assignments.

With Device Groups you can perform the following:

- use device groups to group a number of discovered devices
- use device 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 what default topology is displayed for the user in Network Map view.

Groups

Groups are a collection of devices that you can create from the device inventory. You can use the **Groups** tab in **Configuration > Device Groups** to create device groups. Once a device group is created, it can be assigned to users.

Note:

The maximum number of devices can be assigned to a device group is 260.

Device Groups assignments

You can use Group Assignments tab in the Device Groups view to assign device groups to users. You can also assign a current device group context to a user in this tab. The current device group context of a user determines the devices that the user can currently manage using different Configuration views, such as Network Map, VLAN, and MLT.

Launching Device Groups

You can launch Device Groups to gain access to device groups and their assignments.

Complete the following steps to launch the Device Groups view.

Procedure

1. Select **Configuration > Device Groups**.

The Device Groups view has two tabs: Groups and Group Assignments.

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

Device Groups tool bar options

You can use the tool bar options on the Device Groups view to create and manage device groups and device groups assignments. For example, you can create device groups, edit devices in the individual groups, and highlight device groups on the Network Map view.

You can use device groups to group a number of discovered devices, and then assign device groups to users. You can also select one of the assigned group as the current context for the user. Each user can have multiple device groups assigned, but only one current context device group.

The following table lists and describes the Device Groups tool bar buttons available for your use in both the Groups and Group Assignments tabs.

Table 1: Device Groups tab tool bar options












Tools	Tool bar button	Description
Refresh		Refresh the content pane.
Add Device Group		Add a device group to group a number of discovered devices from the inventory. The maximum number of devices can be assigned to a group is 260.
Delete Device Group		Delete a device group.
Apply Changes		Apply changes you have made to a device group
Revert Changes		Revert changes back to what was configured in your previous step.
Unknown Devices		Identifies devices that are part of a device group, but that are excluded from a rediscovery. If you perform a rediscovery and some of the devices which are part of a created device group are not rediscovered, then those devices appear in red. These devices continue to appear in red until you perform another discovery or remove the devices from the device group.

Table 2: Group Assignments tab tool bar

Tools	Tool bar button	Description
Refresh		Refresh the content pane.
Add Device Group Assignment		Assign device group to a user.
Delete Device Group Assignment		Delete a user from the device groups assignment.
Apply Changes		Apply changes you have made to a user device groups assignment.
Revert Changes		Revert changes back to what was configured in your previous step.

Creating a device group

You can create a device group by grouping a number of discovered devices from the single repository. After creating device groups, you have the ability to assign these device groups to users. The device group and the device group assignments determine the devices that users see in Network Map view when they log in to the system.

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. The maximum number of devices can be assigned to a group is 260.

If the user performs a rediscovery, and some of the devices which were part of a created device group are not rediscovered, then those devices appear in red. These devices continue to appear in red until the user performs another discovery or removes the devices from the device group(s).

You can create device groups in the **Configuration > Device Groups** tab.

Perform the following procedure to create a device group.

Procedure

1. Select the **Configuration > Device Groups** to start the Device Groups.
2. On the **Groups** tab, select **Add Device Group**, which is the plus sign on the tool bar on the top left.
The Add Group window displays.
3. In the **Group Name** field, enter a name that uniquely identifies the device group.
4. 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 or system name.

You can use **Filter...** to filter in or filter out a device that appears on the Available list. You can use a complete or partial device IP address, device type, or device name. To use this feature, perform one of the following actions.

- To filter in a device, click **Filter...**, select **In**, enter a device IP address, Type, or Name, and then click **Filter**.

Only the device you filter in appears in the Selected list.

- To filter out a device, click **Filter...**, select **Out**, enter a device IP address, Type, or Name, and then click **Filter**.

Devices other than the device you filter out, appears in the Selected list.

5. Click **Save**.

Editing a device group

You can edit a device group to add or remove devices from the selected device list. The devices that you add or remove from the device list impact the devices that users see in Network Map view and other Configuration views when they log on to the system.

Perform the following procedure to edit a device group.

Procedure

1. Select **Configuration > Device Groups** to start the Device Groups.
2. On the **Group** tab in the **Device Groups** tab, double click the device group listing that you want to modify.
3. Edit the appropriate fields, and click **OK**.
4. Select **Apply Changes**, which is the check mark on the toolbar on the top left.

Result

Further, a similar notification is displayed on all Configuration views (such as VLAN, MLT) that are opened by any user with the modified device group as their current context. On closing the notification, a fresh discovery for the concerned Configuration view is performed automatically.

Assigning device groups to a user

You can assign device groups to a user using the Device Groups view. You can also set the current context device group for a user.

The administrator can use the current context setting to define the accessibility of users to devices based on their domain of responsibility. The context setting determines the devices accessible to a user in any of the Configuration view including Network Map.

Perform the following procedure to assign device groups and current context to a user.

Procedure

1. Select **Configuration > Device Groups** to start the Device Groups.
2. On the **Group Assignments** tab, select **Add Device Group Assignment**, which is the plus sign on the top left tool bar.

The Add Device Group Assignment window displays.

3. In the **User** field, select the name of the user from the drop-down list.
4. In the **Current Context** field, select the name of the device group that you want to set as current context for the user.
5. In the **Groups** field list, select the device groups that you want to associate to the user.
6. Click **Save**.

Editing device group assignments

You can edit a user device group assignment to modify the current context value that is associated to a user. You can also add or remove the device groups associated to the user. A change in the user current context value affects the devices the user can view and manager in various Configuration views.

Editing assigned groups for a user

About this task

Perform the following procedure to edit the assigned device groups and the current context for a user.

Procedure

1. Select **Configuration > Device Groups**.
2. On the Group Assignments tab, double-click the Assigned Groups column cell corresponding to the user.
The Edit Device Group Assignment window is displayed.
3. **(Optional)** Edit the **Current Context** field to change the current context.
4. **(Optional)** Modify the list of selected groups to add or remove assigned groups.
5. Click **OK** to close the Edit Device Group Assignment window.
6. Select **Apply Changes** on the **Group Assignments** tab toolbar.

Result

If there is a change in the current context, a notification is displayed in all Configuration views (such as VLAN, MLT) that are opened by the user. On closing the notification, the context for the concerned Configuration view is updated. If a fresh discovery is required for the new context, it is performed automatically.

Changing the Current Context

About this task

Perform the following procedure to change the Current Context for a user.

Procedure

1. Select **Configuration > Device Groups**.
2. On the Group Assignments tab, double-click the Assigned Groups column cell corresponding to the user.
3. Select the required device group from the drop-down list as the new Current Context.
4. Select **Apply Changes** on the **Group Assignments** tab toolbar.

Result

If there is a change in the current context, a notification is displayed in all Configuration views (such as VLAN, MLT) that are opened by the user. On closing the notification, the context for the concerned Configuration view is updated. If a fresh discovery is required for the new context, it is performed automatically.

Changing the current context from any Configuration view

About this task

Perform the following procedure to change the current context from any of the Configuration view (such as VLAN, MLT) that is currently open and visible.

Procedure

1. Locate the context tool on the top left end of the current Configuration view.
2. From the combo-box select the new context.
3. Select the required device group from the drop-down list as the new Current Context.
4. Click **Save Context** to the right of the combo-box.

Result

A notification indicating the context change is displayed in all Configuration views (such as VLAN, MLT) that are opened by the user. On closing the notification, the context for the concerned view is updated. If a fresh discovery is required for the new context, it is performed automatically.

Chapter 7: Using Network Table

About Network Table

With the Network Table, you can manage the inventory. The system 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.

Launching the Network Table

Procedure

select **Configuration > Network Table**.

Network Table toolbar

You can use the tool bar options on the Network Table 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 Network Table to draw a device topology from the inventory grid.

The following table lists and describes the Network Table tool bar options.

Table 3: Network Table tool bar options

Option	Description
Context	Use this option to select the available groups assigned to the current logged in user. After you change the context, a notification is sent to all opened configuration views in the system with the same logged in user. All opened views are refreshed after receiving this notification.
Save Context	Use this option to save the context.
Revert to Current Context	Use this option to revert to the current context.
Refresh Groups	Use this option to view the new groups added to the current logged in user.
Show All	Use this option to view all discovered nodes in the system.

Table continues...

Option	Description
	Displaying devices in topology map is based on the context selected. The default selection is Show All. When this option is selected, context view selection is disabled automatically.
Perform Device Action	<p>Use this option to perform the following actions on a device in the topology map:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> - Update Device Topology - Change IP Address <p>You also can access these options through the right-click menu of a device on the Network Map or Network Table.</p>
Import/Export Inventory	Imports or exports the inventory from or to a XML file.
Refresh Device Inventory	Refreshes the device inventory information.
Draw Topology	Use this option to create a network topology map from the Network Table.
Reachable	Indicates that the device is reachable.
Help	Displays online help.

Launching an Element Manager

Before you begin

Before you can launch EDM, you must install the required EDM plugins using the Administration > Device Plug-in Management.

For more information on installing EDM plugins, see the EDM section in *Administration using Extreme Fabric Orchestrator*, NN48100–600 .

Procedure

Perform one of the following:

- Select **Configuration > Network Map**.

Right-click on a device in the topology map, and then select **Launch Element Manager**.

- Select **Configuration > Network Table**.

Select a device from the Device table.

From the Network Table tool bar, select **Perform Device Action > Launch Element Manager**.

! **Important:**

If you select a device that does not support EDM, by default the Java Device Manager (JDM) of the corresponding device opens up. If the Java Virtual Machine (JVM) application is not already installed in your system, then the system prompts you to install the application.

Importing devices

Procedure

1. Perform one of the following:
 - Select **Configuration > Network Map**.
From the topology map, click on a device, and then from the Network Map tool bar, select **Import/Export topology**.
 - Select **Configuration > Network Table**.
Select a device from the Device table.
From the Network Table tool bar, click **Import/Export Inventory**.
2. To select the path of the .xml file, click **Browse**.
3. Click **Import**. The system imports the devices and auto refreshes the Network Table.

Exporting devices

About this task

Perform the following procedure to export an inventory to the XML file, or to export a device list to the CSV File.

Procedure

1. Select **Configuration > Network Map**.
2. From the topology map, click on a device, and then click **Import/Export topology**.
OR
 - Select **Configuration > Network Table**.
 - Select a device from the Device table.
 - From the Network Table tool bar, click **Import/Export Inventory**.
3. Select **Export Inventory to XML File**, or **Export Device List to CSV File**.
4. Click **Export**.

Chapter 8: Managing VLAN

About VLAN

VLAN view supports the VLAN and STG MIBs, and lets you manage VLAN and STG configurations across a single device or multiple devices. The following sections describe VLAN view 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).

VLAN features

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

- View Spanning Tree configuration information in the 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 [STG and VLAN information](#) on page 77.

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 to sustain network operations. The collection of ports in one spanning tree is called a Spanning Tree Group (STG) and a network can include multiple STGs.

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

*** Note:**

VSP devices support RSTP and MSTP, but do not support Avaya STG protocol except VSP 7000.

*** Note:**

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

The following table lists the details for different switches.

Table 4: Maximum STGs and VLANs supported by switches

Switch	Maximum number of STGs	Maximum number of VLANs
Passport 1000 Series switch	25	101

Table continues...

Switch	Maximum number of STGs	Maximum number of VLANs
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 configuration

VLAN view allows you to create VLANs and configure routing and domain synchronization for them. You can also use VLAN view 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.

The system 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. 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, VSP 4000, VSP 8000, and VSP 7200 as they are not supported.

*** Note:**

Wireless Controller (WC) devices do not support the MSTP mode.

*** Note:**

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 Vlan 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 the Configuration view 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 configuration for the WC is similar to the ERS5600 version 6.2 and above.

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

Starting VLAN view

Procedure

Select **Configuration > VLAN**.

Result

The VLAN view displays.

VLAN view

This section details the VLAN interface.

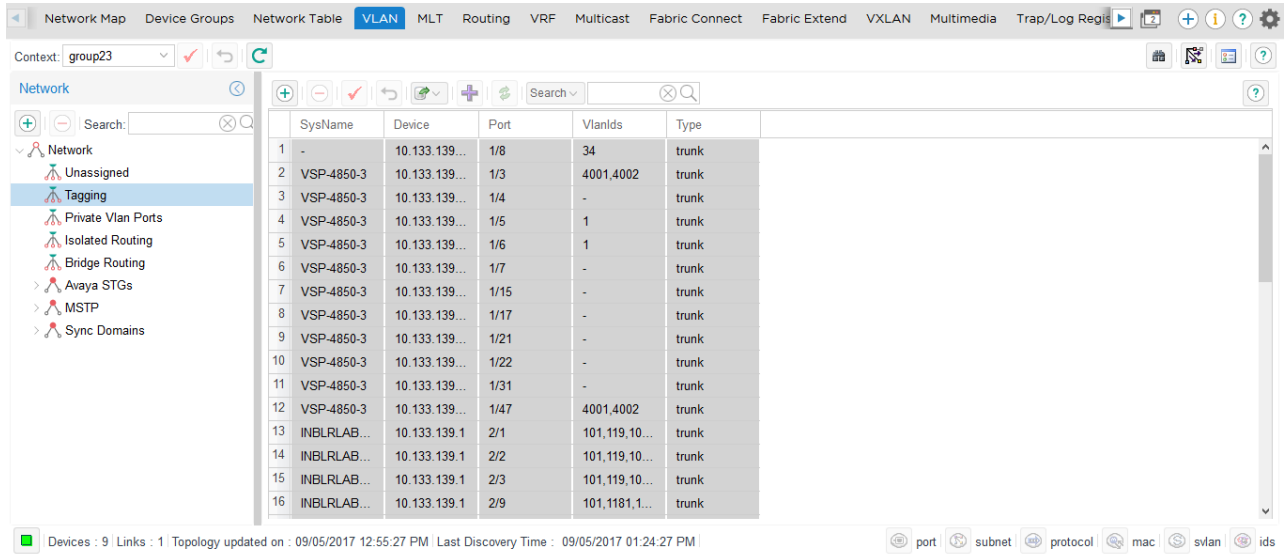


Figure 1: VLAN view

Table 5: VLAN view

Area	Description
Navigation pane	Provides a navigation tree showing VLAN network folder resources and a toolbar for working with items in the pane. For more information, see VLAN manager navigation pane on page 56.
Contents pane	Displays information selected in the contents pane and a toolbar for working with items in the pane. For more information, see VLAN contents pane on page 58.
Status bar	Displays status information, it includes discovery information, type of node highlighted, and command status. For more information, see VLAN status bar on page 58.

VLAN manager navigation pane

The VLAN navigation pane provides access to all VLAN 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 folders and icons in the VLAN navigation pane.

Table 6: VLAN navigation pane

Area	Description
Network	Contains all of the icons and folders in the navigation pane.
Unassigned	Shows the ports of a device that are not currently assigned to an STG.
Tagging	Shows the list of ports for which VLAN tagging is enabled.
Private Vlan Ports	Shows Private VLAN capable devices configured as promiscuous, isolated, or trunk ports.
Isolated Routing	Shows a port that can only route IP packets and does not belong to any STG or VLAN.
Avaya STGs	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 77.
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.

Navigation pane toolbar

The following table lists the navigation pane toolbar options. You can highlight MLT constructs on the Topology Map using the Highlight on Topology button.

Table 7: Navigation pane toolbar fields

Button	Description
Context	Use this option to select the available groups assigned to the current logged in user. After you change the context, a notification is sent to all opened configuration views in the system with the same logged in user. All opened views are refreshed after receiving this notification.
Save Context	Use this option to save the context.
Revert to Current Context	Use this option to revert to the current context.
Refresh Groups	Use this option to view the new groups added to the current logged in user.
Discover Vlans	Manually starts the Vlan discovery process.
Highlight on topology	Highlights devices in the content pane for the selected Vlan or STG.

Table continues...

Button	Description
Preferences	Opens the Preferences dialog box.
Help	Launches help for the current view.

VLAN 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 information 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 8: VLAN 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 to CSV or TXT.
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 .

VLAN status bar

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

Field	Description
Message	Located on the left, the message field displays information about VLAN 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 79.

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 STG

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, select **Network > Avaya STGs**.
3. Click **Add**.
4. In the Add STG window, insert values or select options in the option boxes appropriately.
5. Click **Save**.

Add STG dialog box field descriptions

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.
Tagged BPDU Address	A MAC address, specifically for tagged BPDUs.
Tagged BPDU Vlan ID	The VLAN tag associated with the STG. This ID is used to tag BPDUs through a non-IEEE tagging bridge to another 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).
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 Online Help in a web browser.

Configuring Avaya STG parameters

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, select an Avaya STG folder, and then select **Config** to view and configure Avaya STG parameters.

Avaya STGs Configuration table field descriptions

The following table describes the fields in the Configuration table.

Name	Description
SysName	System name or host name of the device.
Device	IP address of the device.
BridgeRegionalRoot	
BridgePriority	The Spanning Tree Protocol (STP) bridge priority, in decimal. The range is 0 (highest priority) to 65535 (lowest priority). The default is 32768.
BridgeRootCost	
BridgeRootPort	
BridgeEnabled	
BridgeTimeSinceTopologyChange	
BridgeTopChanges	
BridgeNewRootCount	
BridgeInstanceUpCount	
BridgeInstanceDownCount	

Editing an Avaya Spanning Tree Group

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, select an Avaya STG folder.
3. Click **Config**.
4. In the Avaya STG table in the contents pane, click the item you want to edit.
5. Type information in the text boxes, or select from a list.
6. On the VLAN toolbar, click **Apply Changes**.

Deleting an Avaya Spanning Tree Group

Procedure

1. Select **Configuration > VLAN**.
2. From the Navigation pane, select an Avaya STG folder (except STG 1).

3. On the Navigation pane toolbar, click **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

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, select an existing Avaya STG.
3. Select the **Members** tab.
4. Click **Add** to open the Avaya STG dialog to add members.
5. Select the desired additional members from the device list.
6. Insert values or select options in the option boxes, as required.
7. Click **Save**.

Deleting members from STG

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, select an existing Avaya STG.
3. In the contents pane, select **Members** and the device to remove.
4. Click **Delete**.
5. 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

About this task

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

Note:

The VLAN view ng does not support the configuration of port members through the Edit screen for spbm-bvlan-based VLANs.

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, select an Avaya STG folder.
3. Click **Members**.
4. In the Avaya STG table in the contents pane, click the item you want to edit.
5. To change the port membership for a device, click the associated **PortMembers** field, and choose the ports to include.
6. On the contents pane toolbar, click **Apply Changes**.

Create and configure VLANs for an Avaya STG

When you create VLANs for an Avaya STG using the VLAN, 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 the system.

Creating a port based VLAN

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, expand **Network** and then select **Avaya STGs**.
3. Select an **STG**.
4. Click **Add** in the navigation pane toolbar.
5. In the Add Vlan window, type the VLAN ID in the **VLAN ID** field.
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 (required).
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)**.

- From the **Type** field, select the **byPort** type option.

Other fields in the Add Vlan window that apply to a port-based VLAN are activated.

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

! **Important:**

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

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

Creating a subnet based VLAN

Procedure

- Select **Configuration > VLAN**.

- From the navigation pane, select **Network > Avaya STGs**.

- Select an **STG**.

- Click **Add** to insert a subnet based VLAN.

- In the Add Vlan window, type the VLAN ID in the **VLAN ID** field.

The value can be from 1 to 4094, as long as it is not already in use.

- In the **Name** field, type the VLAN name (required).

- For an Ethernet Routing Switch 8600 or VSP 9xxx, select the **QoS Level**.

- For Passport 1000 Series switch, specify whether the VLAN traffic will be tagged as **High Priority (1K)**.

- 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.

- In the **Subnet** field, type the source IP subnet address.

- In the **Mask** field, type the IP subnet mask.

- 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.

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

! **Important:**

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

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

Creating a protocol based VLAN

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, expand **Network > Avaya STGs**.
3. Select an **STG**.
4. Click **Add** to insert a protocol based VLAN.
5. In the Add Vlan window, type the VLAN ID in the **VLAN ID** field.
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 (required).
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 the system 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

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, select **Network > Avaya STGs**.
3. Select an **STG**.
4. Click **Add** to insert a source MAC address based VLAN.
5. In the Add Vlan, type the **VLAN ID** in the **VLAN ID** field.
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 (required).
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 supported devices. 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

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, select **Network > Avaya STGs**.
3. Select an **STG**.
4. Click **Add** to insert a sVLAN based VLAN.
5. In the Add Vlan window, type the **VLAN ID** in the VLAN ID field.
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 (required).
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 the system 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

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, select **Network > Avaya STGs**.
3. Select an **STG**.
4. Click **Add** to insert an ID based VLAN.
5. In the Add Vlan window, type the **VLAN ID** in the VLAN ID field.

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 (required).
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 the system 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. Select **Configuration > VLAN**.
2. From the navigation pane, select **Network > Avaya STGs**.
3. Select an **STG**.
4. To insert an spbm-based VLAN, click **Add**.
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 (required).
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 the system 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. Select **Configuration > VLAN**.
2. From the navigation pane, select **Network > Avaya STGs**.
3. Select one of the following:
 - STG for Avaya STG instances
 - CIST/msti for MSTP instances
4. To insert an spbm-based VLAN, click **Add**.
The Add Vlan window displays.
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 (required).
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.

*** Note:**

Not all VLAN types are available on all devices that the system supports. Devices that do not support spbm-switchedUni VLANs are absent from the device list.

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

Add VLAN field descriptions

Field	Description
VLAN ID	The VLAN ID.

Table continues...

Field	Description
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: <ul style="list-style-type: none"> • by port • by subnet • by protocol • by source MAC Address • by SVLANs • 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

Procedure

1. Select a VLAN.
2. Click **Synchronize VLAN Name** on the contents pane toolbar.
3. In the Synchronize VLAN name dialog box, 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

Procedure

1. Select **Configuration > VLAN**.
2. In the navigation pane, select the **RSTP** folder.
3. Select the **Rapid STG** folder, and select the **Config** item.
4. In the contents pane, click the field of an item that you want to edit.
5. Type information in the field, or select an option from a drop down list.
6. Click the **Apply Changes** icon.

Create and configure VLANs for RSTP

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

*** Note:**

spbm-switchedUni Vlan is not supported under RSTP.

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation tree, select the **RSTP** folder.
3. Select the **Rapid STG** folder, and perform one of the following:
 - From the VLAN menu bar, choose **Edit > Insert**.
 - On the VLAN toolbar, click **Insert**.
4. Insert values or select options in the option boxes.
5. Click **Ok**.

Deleting a VLAN from RSTP

Procedure

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

3. In the Delete dialog box, click **Yes** to confirm the deletion of the VLAN.

Adding members to a VLAN group in Rapid Spanning Tree

Procedure

1. From the Navigation pane, under a Rapid STG group, select a VLAN for adding a member.
2. Perform one of the following:
 - a. From the VLAN menu bar, choose **Edit > Insert**.
 - b. On the VLAN toolbar, click **Insert**.
3. Select the additional members from the device list.
4. Insert the values or select the options as required.
5. Click **OK**.

MSTP configuration

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

Procedure

1. Select **Configuration > VLAN**.
2. From the Navigation pane, select the **MSTP** folder.
3. On the VLAN toolbar, click **Add**
4. In the **Id** field, enter the desired MSTI identifier.
5. Select the **Devices** required for the MSTP.
6. Click **Save**.

Adding port members

Procedure

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

Editing MSTP properties

Procedure

1. From 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.
6. Type information in the fields, or select from the drop down list.
7. On the toolbar, click **Apply Changes**.

Deleting an MSTI

Procedure

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

VLANs configuration 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

Procedure

1. Select the **MSTP** folder.
2. Select the **CIST** folder or an **MSTI** folder.
3. On the VLAN toolbar, click **Add**. On the VLAN toolbar, click **Add**.
4. Insert values or select options in the option boxes.
5. Click **Save**.

Deleting a VLAN from MST

Procedure

1. In the Navigation pane, under the **CIST** or **MSTI** folder, select the VLAN to delete.
2. On the VLAN 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

Procedure

1. From the Navigation pane, under an MSTP group, select the VLAN to add a member.

2. On the content pane toolbar, click **Add**.

Add Vlan

Vlan Properties

VLAN ID: [1 - 4094]

Name:

Qos Level: ▾

High Priority (1K):

Type: ▾

Protocols: ▾

Subnet:

Mask:

ARP Classification ID:

User Defined PID:

[4 digit hex Pid(s) in range or list format, n1, n2-n3 etc.]

Secondary VLAN ID: [2 - 4084]

Devices

SysName	Device
<input type="checkbox"/> VSP-4850-3	10.133.139.101

Save Close Help

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. **(Optional)** In the **Name** field, type the VLAN name. 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 the system supports. Devices that do not support port-based VLANs are absent from the device list.

8. Click **Save**.

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. Select **Configuration > VLAN**.
2. From the navigation pane, select **Private Vlan Ports**.
3. Select the Private VLAN Port.

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

*** Note:**

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

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

Procedure

1. Select **Configuration > VLAN**.

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

For an example of the Add Vlan window, see [Adding members to a VLAN in Multiple Spanning Tree](#) on page 71.

5. Select **private**.
6. 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.

7. Click **Save**.

Adding Private VLAN Ports

Procedure

1. Select **Configuration > VLAN**.
2. Select **Private Vlan Ports**.
3. On the VLAN toolbar, click **Add**.
4. Complete fields in the **Insert/Update Private Vlan Ports** dialog box as appropriate.
5. Click **OK**.

Deleting a Private VLAN in MST

Procedure

1. Select **Configuration > VLAN**.
2. In the Navigation pane, under the **CIST** or **MSTI** folder, select the Private VLAN to delete.
3. On the VLAN toolbar, click **Delete**.
4. Click **Yes** when prompted to confirm the deletion.

Configuring port members

This section provides information about the port membership types, and how to use VLAN to configure them. For information about how to view port membership, including viewing unassigned ports, see [Port membership information](#) on page 82.

Port membership types in VLAN navigation pane

Port type	Description
Unassigned	A port that does not belong to any STG. If no devices in the network contain unassigned ports, a table does not appear in the contents pane. For more information, see Viewing the unassigned ports on page 82.
Tagging	A port that has tagging enabled and can belong to multiple STGs. If a tagged frame is received on a tagged port, with a VLAN ID specified in the tag, the switch directs it to that VLAN, if it is present. For more information, see Viewing tagged ports on page 83.
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 73.
Isolated Routing (IRP ports)	A port that can only route IP packets and does not belong to any STG or VLAN. For more information, see Viewing isolated router ports on page 84.
Bridge Routing (brouter ports)	A port that can route IP packets as well as bridge all non routable traffic. The routing interface is not subjected to the Spanning Tree Protocol. For more information, see Viewing bridge routing ports on page 84.

Adding port members

Procedure

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

Adding tagged ports

Note:

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

Procedure

1. Select **Configuration > VLAN**.
2. In the Navigation pane, select **Tagging**.
3. Click **Add**.

4. Complete the fields as appropriate.
5. Click **OK**. An Operation Result dialog box displays when the addition is complete.
6. Click **OK**. The Operation Result dialog box closes and the added port is visible in the contents pane.

Tagging Ports table field descriptions

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 view allows you to configure certain routing interfaces.

Enabling OSPF on a VLAN interface

About this task

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

Procedure

1. Select **Configuration > VLAN**.
2. In the Navigation pane, select a VLAN.
3. Click the **Routing** tab.
4. In the **OspfEnable** field, choose **true** to enable OSPF on this VLAN.
5. Click **Apply Changes**.

Inserting a VRRP interface on a VLAN

About this task

You can use VLAN view to insert a VRRP routing interface for a VLAN. Before inserting the VRRP interface, ensure the VLAN has an assigned IP address for routing.

Procedure

1. Select **Configuration > VLAN**.
2. In the Navigation pane, select a VLAN.
3. In the VLAN table in the contents pane, select a device that supports VRRP.
4. Click **Add Vrrp**.

5. In the **VrId** and **IpAddr** fields of the Insert VRRP dialog box, enter the Virtual Router ID and IP address for the VRRP interface.
6. Click **Ok**.

Result

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

STG and VLAN information

You can use VLAN view to monitor the status of STGs and VLANs in the network, as well as view information about ports.

STG information

This section provides information about viewing STG information.

Viewing Spanning Tree Groups

About this task

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

Procedure

1. Select **Configuration > VLAN**.
2. From the Navigation pane, select **Network > Avaya STGs**.
3. Select an STG folder to view.

Viewing STG status

About this task

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.

Procedure

1. select **Configuration > VLAN**.
2. From the Navigation pane, select **Network > Avaya STGs**.
3. Open an STG and select the **Status** tab.

Result

The Status table displays in content pane.

Status table field descriptions

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

About this task

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

Procedure

1. Select **Configuration > VLAN**.

2. From the Navigation pane, select **Network > Avaya STGs**.
3. Open an STG folder, and select the **Root** tab in the content pane.

Root table field descriptions

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 shows elements of VLAN icons.



Figure 2: VLAN Icon elements

Elements of VLAN icons

The following table shows the type of VLAN.







Icon	Description
	Port based-a VLAN in which the ports are explicitly assigned to the VLAN.

Table continues...

Icon	Description
	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.

The following table shows information about the VLAN.

Label	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 (<i>italic</i> or normal)	An <i>italic</i> icon label indicates that an IP address has been defined for the VLAN, and that the VLAN is routable.

Viewing the Default VLAN

About this task

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

- Ethernet Routing Switch 8xxx 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, and it is always a port-based VLAN. You cannot delete the default VLAN, although you can remove ports from it.

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation tree, select **Default(1)**.


Result

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

Default VLAN field descriptions

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.
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.
TosValue	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: <ul style="list-style-type: none"> • 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

Table continues...

Field	Description
	 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

About this task

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

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

Procedure

1. Select **Configuration > VLAN**.
2. Click **Discover Vlans** on the Navigation pane toolbar.
3. In the Operation Result dialog box, click **OK**.

Port membership information

You can use VLAN view to monitor the status of ports in a VLAN. VLAN 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

Procedure

1. Select **Configuration > VLAN**.
2. In the Navigation pane, click **Unassigned**.

Result

The Unassigned Ports table displays in the contents pane.

Unassigned Ports table field descriptions

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

Viewing tagged ports

Procedure

1. Select **Configuration > VLAN**.
2. In the Navigation pane, select **Tagging**.

Result

The Tagging Ports table displays in the contents pane.

Tagging Ports table field descriptions

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

Viewing Private VLAN ports

About this task

Perform the following procedure to view Private VLAN ports

Procedure

1. Select **Configuration > VLAN**.
2. 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 of the device.
SysName	System name or host name of the device.
Port	Ports that route only IP packets.
Private VLAN Type	Private VLAN capable devices configured as Promiscuous, Isolated, and Trunk ports.

Viewing isolated router ports

Procedure

1. Select **Configuration > VLAN**.
2. In the Navigation pane, select **Isolated Routing**.

Result

The Isolated Routing Ports table displays in the contents pane.

Isolated routing ports table field descriptions

Field	Description
Device	IP address of the device.
SysName	System name or host name of the device.
Ports	Ports that route only IP packets.

Viewing bridge routing ports

About this task

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

Procedure

1. Select **Configuration > VLAN**.
2. In the Navigation pane, click **Bridge Routing**.

Result

The Bridge Routing Ports table displays in the contents pane.

Bridge Routing Ports table field descriptions

Field	Description
Device	IP address of the device.
SysName	System name or host name of the device.
Ports	Port numbers of the port on which frames are received.

Viewing port members of an STG

About this task

Use the Port Members table to view the ports that are members of the specified STG.

Procedure

1. Select **Configuration > VLAN**.
2. From the Navigation pane, select **Network > Avaya STGs**.
3. Open an STG, and then select the **Members** tab in the content pane.

Port members table field descriptions

Field	Description
Device	IP address of the device.
SysName	System name or host name of the device.
Port Members	Ports on the device that are members of the STG.

Viewing VLAN Port Members in MSTP**About this task**

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

Procedure

1. Select **Configuration > VLAN**.
2. From the Navigation pane, select **Network > MSTP** folder.
3. Select the **CIST** folder or an **MSTI** folder.
4. Select a VLAN.

Result

The VLAN Port Members table displays in the contents pane.

VLAN Port Members table field descriptions

Field	Description
Device	IP address of the device.
SysName	System name or host name of the device.
PortMembers	Ports on the device that are members of the STG.

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**About this task**

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

Procedure

1. Select **Configuration > VLAN**.
2. In the Navigation pane, choose a VLAN.

The Ports table displays in the contents pane.
3. On the VLAN menu bar, click **Highlight on topology**.

Result

The highlighted topology view displays in the contents pane.

Viewing STG port members on the topology map

About this task

When you select an STG in the VLAN navigation pane, you can view the devices and ports associated with that STG in the 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

1. Select **Configuration > VLAN**.
2. In the VLAN navigation pane, choose an **STG Members** icon.
The STG Members table displays in the VLAN contents pane.
3. On the VLAN menu bar, click **Highlight on topology**.

Result

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

Viewing STG root configuration on the topology map

About this task

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

1. Select **Configuration > VLAN**.
2. In the Navigation pane, select an **STG Root**.
The Root table displays in the contents pane.
3. On the VLAN menu bar, click **Highlight on topology**.

Result

The highlighted topology view displays in the Monitoring 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 87
 - [Sync Domain interface](#) on page 88
 - [Server node VLAN interface](#) on page 89
 - [IP Address and Net Mask interfaces](#) on page 91
- [Domain synchronization procedures](#) on page 92
 - [Creating a sync domain](#) on page 92
 - [Adding a VLAN to a sync domain server node](#) on page 93
 - [Modifying a sync domain](#) on page 93
 - [Modifying a sync domain server node VLAN](#) on page 94
 - [Deleting a sync domain](#) on page 95
 - [Deleting a server node VLAN](#) on page 95

Domain synchronization interfaces

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

- [Sync Domain interface](#) on page 88
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 89
Use the VLAN interface to add a new VLAN or private VLAN to the server node.
- [IP Address and Net Mask interfaces](#) on page 91
Use the IP Address and Net Mask interfaces to review and change the IP addresses and network masks of domain members.

Sync Domain interface

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	<p>Synchronization is a global parameter. There are two synchronization options:</p> <ul style="list-style-type: none"> • 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.
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.
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 discovered by VLAN 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	<p>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.</p> <p>Sync is False for all VLANs when the sync domain is created.</p>
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 91.

Table continues...

Field	Description
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 91.
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 that you use to add a new VLAN to the server node.

The following table describes the elements of the interface.

Table 9: VLAN interface elements

Element	Description
VLAN ID	This is the primary identity of the VLAN. VLAN 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.

Table continues...

Element	Description
Type	Choose private to configure a private VLAN.
Subnet, Mask, ARP Classification Id, User Defined 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 [Sync Domain interface](#) on page 88 for details).

VLAN 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.

	SysN...	Device	Id	Name	Type	Port...	MSTPInsta...	Vrflid	HighPri...	Qos...	TosV...	Ifindex	IpAddress	NetMask
1	VSP...	10.133.139...	50	VLAN-50	byPort	1/8	msti-1	0	-	-	0	2098	3.3.3.1	255.255.25...
2	-	10.133.139...	50	VLAN ...	byPort	1/4	msti-1	0	false	-	-	10050	10.10.10.2	255.255.25...
3	ERS...	10.133.139...	50	IST-VL...	byPort		msti-1	0	-	level1	1	2098	200.200.20...	255.255.25...
4	ERS...	10.133.139...	50	IST-VL...	byPort	4/2...	msti-1	0	-	level1	1	2098	200.200.20...	255.255.25...

Figure 3: Current VLAN configuration

IP Address interface

VLAN 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 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 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

Before you begin

Familiarity with the Sync Domain interface is required for this procedure. See [Adding a VLAN to a sync domain server node](#) on page 93 for more details.

About this task

This procedure does not provide instructions for adding a new VLAN to the server node; those instructions are provided by [Sync Domain interface](#) on page 88.

Procedure

1. Select **Configuration > VLAN**.
2. From the navigation pane, select **Network > Sync Domains**.
3. From the navigation pane toolbar, click **Add**.
4. In the New Sync Domain dialog box, enter a domain name for the new sync domain.
5. Click **Save**.
6. Select the newly added sync domain from the navigation pane.
7. In the **Global Parameters** region, select the required synchronization option.
8. In the **Domain Parameters** region, select **Enable**.
9. From the **Server** list, select a node as the server node.

10. To add devices to the domain, perform 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.
11. In the **Current VLAN Configuration** table, click the **Sync** entry and select the check box to change it to **True** for each VLAN as required.
12. Click **Save Changes**.

Adding a VLAN to a sync domain server node

Before you begin

Familiarity with the New VLAN interface is required for this procedure. See [New server node VLAN interface](#) on page 89 for more details.

Procedure

1. Select **Configuration > VLAN**.
2. From the Navigation pane, select **Network > Sync Domains**.
3. Select the sync domain for adding a VLAN.
4. From the toolbar, click **Add VLAN**.
5. Edit the STG Id in the **Id**, if required.
6. Edit the **VLAN Id**, if required.
7. In the **Name** field, type a name for the VLAN.
8. Select the **QOS Level**.
9. For **Type**, if you require byProtocolId, then perform the following:
 - 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**.
13. From the Sync Domain interface, click **Save Changes**.

Modifying a sync domain

Before you begin

Familiarity with [Creating a sync domain](#) on page 92 is required for this procedure.

About this task

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 94.

Procedure

1. Select **Configuration > VLAN**.
2. From the Navigation pane, select **Network > 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

Before you begin

Familiarity with the IP Address and Net Mask interfaces is required for this procedure. See [IP Address and Net Mask interfaces](#) on page 91 for details.

About this task

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

Procedure

1. Select **Configuration > VLAN**.
2. From the Navigation pane, select **Network > Sync Domains**.
3. Select the required sync domain.
4. In the Current VLAN Configuration table, 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**.

Result

The SyncDomain Operation Description interface appears.

Deleting a sync domain

Procedure

1. Select **Configuration > VLAN**.
2. From the Navigation pane, select **Network > Sync Domains**.
3. Select the required sync domain.
4. From the toolbar, click **Delete VLAN**.
5. Click **Save changes** when prompted to confirm the action.

Deleting a server node VLAN

Procedure

1. Select **Configuration > VLAN**.
2. From the Navigation pane, select **Network > Sync Domains**.
3. Select the required sync domain.
4. In the **Current VLAN Configuration** table, select any cell of the VLAN for deletion.
5. From the toolbar, click **Delete VLAN**.
6. Click **Save changes** when prompted.

Result

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 9: Managing MultiLink Trunking

About MultiLink Trunking

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

The following sections describe MLT types and features.

Create and manage MultiLink Trunks

MultiLink 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 multi-vendor 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 the MultiLink Trunking view to configure MLTs, SMLTs, and ISTs.

*** Note:**

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 ERS5600 devices. The workflow of the MLT for these devices are similar to the ERS5600 devices, except that there are no SMLT IDs for WC devices.

MultiLink Trunks in different switch types

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

Table 10: 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
Ethernet Routing Switch 48xx	32
Ethernet Routing Switch 49xx	32
Ethernet Routing Switch 56xx	32
Ethernet Routing Switch 59xx	32
OM 1000	1
Ethernet Routing Switch 45xx, 25xx, 3510	6
Ethernet Routing Switch 5600	32
Wireless Controller	32
Ethernet Routing Switch 8300	32
Virtual Services Platform 4xxx	512
Virtual Services Platform 7xxx	64

Table continues...

Switch	Maximum number of MLTs
Virtual Services Platform 72xx	512
Virtual Services Platform 8xxx	512

MultiLink Trunking view features

MultiLink Trunking view supports devices that implement the VLAN and STG MIB groups.

MultiLink Trunking view 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 MLT view

Procedure

Select **Configuration > MLT**.

Result

The MLT view is launched and displayed in the content pane.

MLT view

The MLT view contains the parts identified in the following figure.

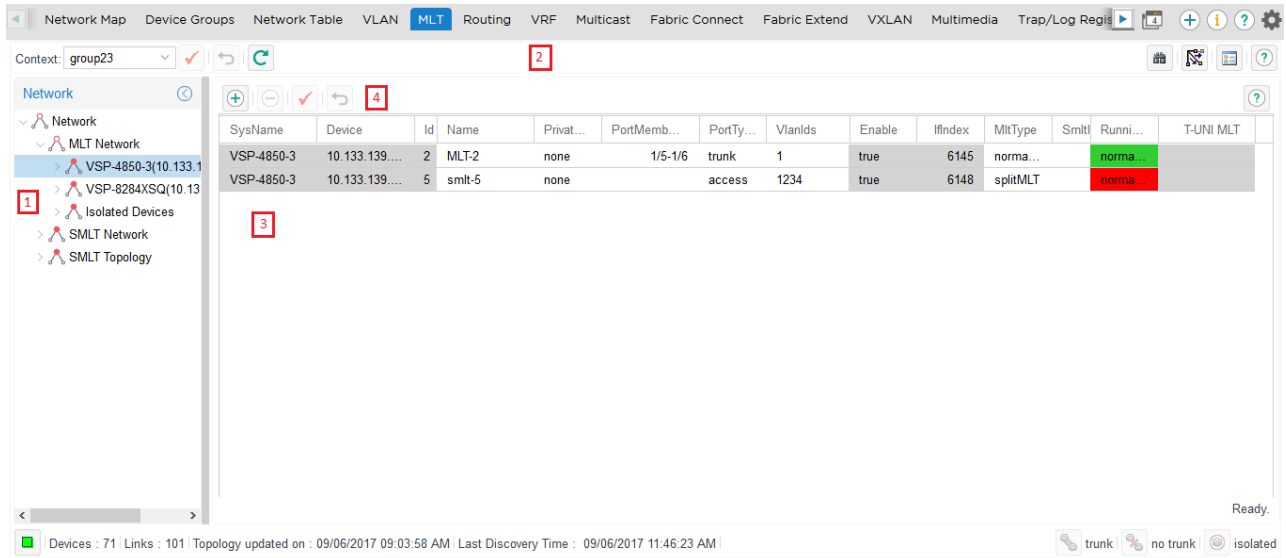


Figure 4: MLT view

The following table describes the parts of the MLT view.

Table 11: MLT view

Part	Description
Navigation pane (1)	Provides a navigation tree showing MLT Network folder resources.
Navigation pane tool bar (2)	Provides tools for MultiLink Trunking.
Contents pane (3)	Displays MultiLink Trunking tables.
Contents pane toolbar (4)	Provides quick access to commonly used MultiLink Trunking commands. These commands apply only to the content pane table.

MLT navigation pane

The MLT 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 System Name and IP address, as discovered by the system. Adjacent devices are listed in the device folder.

The following figure shows the navigation pane.

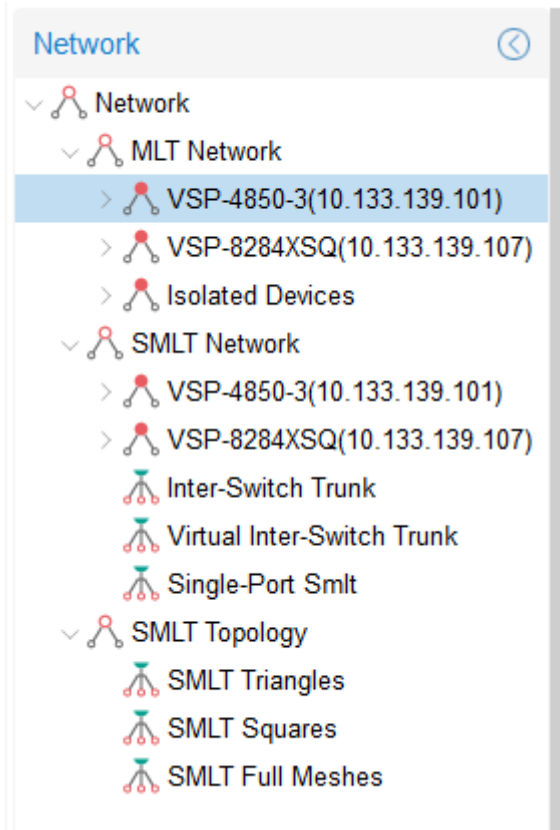


Figure 5: MLT navigation pane

The Network folder has the following resources available in it.

- [MLT Network folder](#) on page 100
- [SMLT Network folder](#) on page 101
- [SMLT Topology folder](#) on page 102

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 shows the MLT Network folder and its contents.

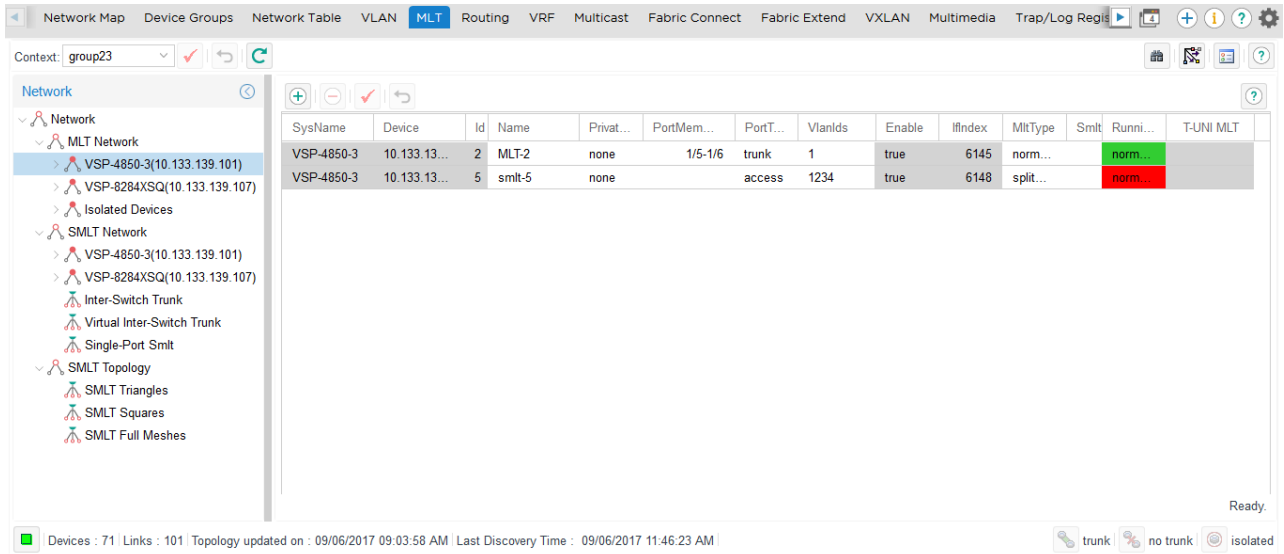


Figure 6: MLT Network

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.

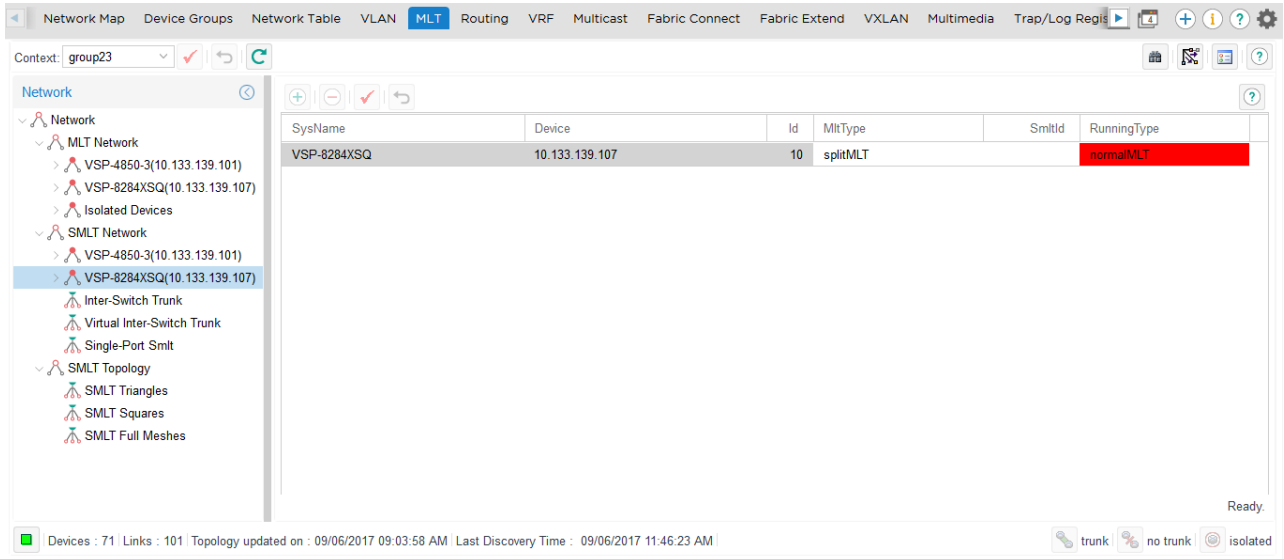


Figure 7: SMLT Network

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

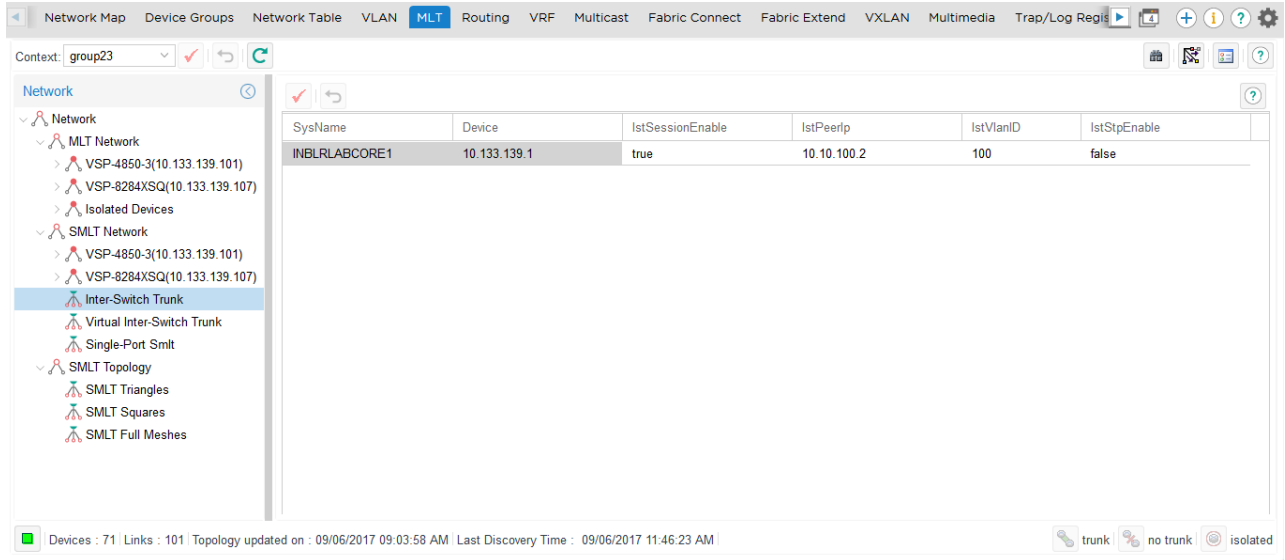


Figure 8: SMLT Network IST

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.

MLT view navigation pane toolbar

The MLT view navigation pane toolbar provide tools and commands to address discovery of trunks, Preferences and topology highlights.

Icon	Name	Description
Context: subnet139	Context	Use this option to select the available groups assigned to the current logged in user. After you change the context, a notification is sent to all opened configuration views in the system with the same logged in user. All opened views are refreshed after receiving this notification.
✓	Save Context	Use this option to save the context.

Table continues...

Icon	Name	Description
	Revert to Current Context	Use this option to revert to the current context.
	Refresh Groups	Use this option to view the new groups added to the current logged in user.
	Discover MultiLink Trunks	Discovers the network and reloads MLT view with the latest information.
	Highlight on topology	Highlights MLT items in the contents pane.
	Preferences	Identifies specific devices for MLT to configure and manage.
	Help	Opens the online Help.

Viewing MLT Network folder

About this task

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

Procedure

1. Select **Configuration > MLT**.
2. In the MLT navigation pane, select the **Network** folder.
3. Click a device from the list in the **Network** folder.

Result

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

MLT contents pane toolbar

The contents pane toolbar provides tools to add an MLT, delete an MLT, commit the changes, and undo the changes.






Icon	Name	Description
	Add	Opens the Insert dialog box, where you insert an MLT on a selected device. For more information, see Create MLTs on ERS and VSP devices on page 104.
	Delete	Removes a selection and displays a message box to confirm deletion of the selected MLT. For more information, see

Table continues...

Icon	Name	Description
		Deleting an MLT from ERS and VSP on page 110.
	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.

MLT management

The following sections describe common operations you can perform using MultiLink Trunks (MLT).

Create MLTs on ERS and VSP devices

To create an MLT on Ethernet Routing Switch 1424/16xx, Ethernet Routing Switch 8000, VSP 9xxx and VSP 4000 3.0, and VSP 8000 4.0.x devices, the device must have more than one connection to another device. With MultiLink Trunking, 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 105.

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 the system.

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 105
- [Creating an MLT with one device for ERS 1424 16xx](#) on page 106
- [Creating an MLT with one device for VSP4000 8000 7200](#) on page 107

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

About this task

When you create an MLT with one device, MLT 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

1. Select **Configuration > MLT**.
2. Select a device from the first (folder) level of the MLT navigation pane.
3. On the content pane toolbar, click **Add**.
4. In the Insert MLT window, select the Id number for the MLT in the **Id** field.
5. In the **Name** field, type the name of the MLT.
6. 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.
7. Select the **Port type** option.
The default is **access**.
8. In the **Vlan IDs** field, select the VLAN IDs that belong to the MLT port.
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 configuration](#) on page 116.
10. Click **Save**.

Insert MLT field descriptions

Field	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.
Private Vlan Type	Private VLAN type
Port Type	One of the following types of MLT: <ul style="list-style-type: none"> • access • trunk The default is Access.
Vlan IDs	VLAN IDs found on the device.

Table continues...

Field	Description
MLT Type	<p>One of the following types of MLT links:</p> <ul style="list-style-type: none"> • normalMLT- Use for normal MLT that do not use SMLT features. • splitMLT- Use for SMLT links between peer devices and non-peer devices in SMLT configurations. • istMLT- Use for IST (inter-switch trunk) links between peer devices in SMLT configurations.
SmltId ID	<p>Sets the SMLT ID number for IST links.</p> <p> Note: In the VSP device there is no SMLT ID. The MLT ID is used for both MLT and SMLT trunks.</p>

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

About this task

When you create an MLT with one device, MultiLink Trunking 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

1. Select **Configuration > MLT**.
2. In the MLT navigation pane, select a device from the first folder level to display the device table.
3. From the content pane toolbar, click **Add** for the Ethernet Routing Switch 1424/16xx devices.
4. In the Insert MLT window, select the Id number for the MLT in the Id field.
5. In the **Name** text box, type the name of the MLT.
6. 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.
7. Select the **Port type** option.
The default is **access**.
8. In the **Vlan IDs** field, select the VLAN IDs that belong to the MLT port.
9. For **MLT Type**, choose **normalMLT**.
10. The istMLT and splitMLT types, and also the SMLT Id value, are used only for split multilink trunks. For more information, see [Managing SMLT configuration](#) on page 116.

11. Click **Save**.

Insert MLT dialog box for ERS 1424/16xx

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

Table 12: 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 Members	Ports in the MLT. The maximum number of ports for one trunk is four.
Private Vlan Type	Private VLAN capable devices configured as none, isolated, promiscuous, and trunk.
Port Type	One of the following types of MLT: <ul style="list-style-type: none"> • access • trunk The default is access.
Vlan IDs	VLAN IDs found on the device.
MLT Type	One of the following types of MLT links: <ul style="list-style-type: none"> • 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.

Creating an MLT with one device for VSP 4000 v 3.0.1, VSP 8000 4.1 and above, and VSP 7200 (all versions)

About this task

When you create an MLT with one device, MultiLink Trunking 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 device for VSP 4000 v 3.0.1, VSP 8000 4.1 and above, and VSP 7200 (all versions).

Procedure

1. Select **Configuration > MLT**.
2. In the MLT navigation pane, select a device from the first folder level.
3. On the content pane toolbar, click **Add**.
4. In the Insert MLT window, select the Id number for the MLT in the Id field.
5. In the Name text box, type the name of the MLT.

6. 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.

7. Select the **Private Vlan Type**.

8. Select the **Port Type** option.

The default is access.

9. In the Vlan IDs field, select the VLAN IDs that belong to the MLT port.

10. 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 configuration](#) on page 116.

11. 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 13: 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.
Private Vlan Type	Selection is available for a Private VLAN-capable device only. <ul style="list-style-type: none"> • Trunk • Isolated • Promiscuous • None
Port Type	One of the following types of MLT: <ul style="list-style-type: none"> • Access • Trunk The default is Access.
Vlan IDs	VLAN IDs found on the device.

Table continues...

Item	Description
MLT type	<p>One of the following types of MLT links:</p> <ul style="list-style-type: none"> • 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

About this task

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

Procedure

1. Select **Configuration > MLT**.
2. In the navigation pane, select an MLT.
3. In the MLT table, double-click the **PortMembers** field.

The PortMembers dialog box displays.

4. 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 105.

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

Procedure

1. Select **Configuration > MLT**.
2. In the navigation pane, select an MLT.
3. In the MLT table in the content pane, double-click the **PortMembers** field.

The screenshot shows a dialog box titled "Port Members" with a close button in the top right corner. Below the title bar, there is a text input field containing "card 3". Below this, there are two rows of port number buttons. The first row contains buttons for ports 01 through 24, and the second row contains buttons for ports 25 through 48. Below the port buttons, there are three status indicator buttons: "Up" with a green square, "Down" with a red square, and "Testing" with a blue square. At the bottom right of the dialog box, there are two buttons: "Save" and "Cancel".

4. In the Port Members dialog box, click the port numbers you want to add or delete from the MLT.

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

5. Click **Save**.

Editing an MLT

Procedure

1. Select **Configuration > MLT**.
2. From the navigation pane, select a device.
3. Select a field to edit in the table.
4. Type information into the field, or select from a drop down list.
5. On the toolbar, click **Apply Changes**.

Deleting an MLT from ERS 1424/16xx, ERS 8000, VSP 9xxx, or VSP 4000

Procedure

1. Select **Configuration > MLT**.
2. In the navigation pane, select a device.
3. In the MLT table, select an MLT for deletion.
4. Click **Delete** from the content pane toolbar.
5. Click **Ok** when prompted to confirm deletion.

MLT configurations

In the MLT 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 MLT.

Viewing trunk connections

About this task

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

Procedure

1. Select **Configuration > MLT**.
2. In the navigation pane, select a device that is represented by a trunk icon.



Result

The Trunk table appears in the contents pane.

Trunk table field descriptions

Field	Description
Device	IP address of the device.
SysName	System name or host name of the device.
Id	Number of the MLT (assigned by MLT).
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • normalMLT • istMLT • splitMLT
T-UNI MLT	Indicates whether the MLT belongs to a T-UNI.

Viewing no trunk configurations

About this task

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.

Procedure

1. Select **Configuration > MLT**.
2. In the MultiLink Trunking Manager navigation pane, select a device IP address above the IP address represented by a no trunk icon.



No trunk table field descriptions

Field	Description
Device	IP address of the device.
SysName	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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

Table continues...

Field	Description
SmltId	Shows the SMLT ID number for split multilink trunk links.
RunningType	Read only field displaying the MLT operational type: <ul style="list-style-type: none"> • normalMLT • istMLT • splitMLT


Viewing isolated devices

About this task

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

1. Select **Configuration > MLT**.
2. In the MultiLink Trunking Manager navigation tree, expand the Isolated Devices folder, and then select an isolated device. 

The Isolated Device table appears in the contents pane.

Isolated Device table field descriptions

Field	Description
Device	IP address of the device.
SysName	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: <ul style="list-style-type: none"> • 512–519 for Passport (legacy) 1050, 1150, 1200, and 1250 devices • 4096–4127 for Ethernet Routing Switch 8000 family devices

Table continues...

Field	Description
MltType	For SMLT configurations, shows one of the following types of MLT links: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • normalMLT • istMLT • splitMLT
T-UNI MLT	Indicates whether the MLT belongs to a T-UNI.

Viewing inter-switch trunks

About this task

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

Procedure

1. Select **Configuration > MLT**.
2. In the MultiLink Trunking Manager navigation tree, select the **Inter-Switch Trunk** under the SMLT Network folder. The inter-switch trunk table appears in the contents pane.

Inter-switch trunk table field descriptions

Field	Description
Device	IP address of the device on which the IST is configured.
SysName	System name or host name of the device.
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.
IstStpEnable	Specifies whether Spanning Tree Protocol (STP) on the IST is enabled.

Viewing single port SMLTs

Procedure

1. Select **Configuration > MLT**.
2. In the navigation pane, select **Network > SMLT Network > Single-Port Smlt**. The single-port SMLT table appears in the contents pane.

SMLT table field descriptions

Field	Description
Device	IP address of the device.
SysName	System name or host name of the device.
SmltId	Shows the SMLT ID number for split MLTs.
Port	The port for the SMLT.
OperType	The current operate type of the port normal or SMLT.
VlanIds	Vlan ID for the SMLT.

Viewing devices and MLT links on the topology map

About this task

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

Perform the following procedure to highlight devices and their MLTs.

Procedure

1. Select **Configuration > MLT**.
2. In the navigation pane, select a device with a trunk connection.
The Trunk table displays in the MultiLink Trunking Manager contents pane.
3. From the MultiLink Trunking Manager menu bar, choose **Highlight On topology**.
The topology view appears in the contents pane with devices connected to the MLT highlighted in blue, and the ports in the MLT or SMLT highlighted in green. Pink highlights the MLT on the device.

Updating information in MLT manager

About this task

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.

Procedure

1. Select **Configuration > MLT**.

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

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

3. Click **OK** to view the MLT Manager window.

SMLT configuration

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 a single device](#) on page 117.
- 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 117.
- On the non peer device, you configure normal MLT links to the two peer devices. For more information, see [Configuring SMLT links on non peer devices](#) on page 118.
- On the two peer devices, you configure the IST peers. For more information, see [Configuring IST peers](#) on page 118.

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.

Procedure

1. Select **Configuration > MLT**.
2. In the MultiLink Trunking Manager navigation pane, select a folder for one of the devices on which you want to configure the IST.
3. On the Content Pane Toolbar, click **Add**.
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 **Port Members** area, select the ports that will be part of the IST.
7. For **Port Type**, select **trunk**.
8. In the **VLAN Ids** 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 117.
- You configure a normalMLT link on the non-peer device. For more information, see [Configuring SMLT links on non peer devices](#) on page 118.

Configuring SMLT links on peer devices

Procedure

1. Select **Configuration > MLT**.
2. In the MLT navigation pane, select a folder for the peer device to configure the link.
3. On the Content Pane Toolbar, click **Add**.
4. In the **Id** box, enter a MLT ID. For SMLT links on peer devices, the MLT ID is ignored.
5. 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.
6. In the **Name** box, enter a name for the MLT.
7. In the **Port Members** area, select the ports on the peer device that are part of the SMLT link.

8. In the **VlanIds** box, select the VLAN. All ports on the SMLT configuration must belong to the same VLAN.
9. For the **MLT Type**, choose **splitMLT**.
10. In the **SMLT Id** field, enter the SMLT Id.
11. Click **Save**.

Configuring SMLT links on non peer devices

About this task

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.

Procedure

1. Select **Configuration > MLT**.
2. In the MLT navigation pane, select a folder for the non-peer device on which you are configuring the link.
3. On the Content Pane Toolbar, click **Add**.
4. In the **Id** box, enter an MLT ID.
5. In the **Name** box, enter a name for the MLT.
6. In the **Port Members** area, select all of the ports on the non-peer device that will be part of the SMLT configuration.
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 **normalMLT**.
9. Click **Save**.

Configuring IST peers

After configuring the IST links using the procedure in [Configuring IST links](#) on page 116, you must configure the IST peers.

Procedure

1. Select **Configuration > MLT**.
2. In the MLT navigation pane, open the **Smlt Network** folder.
3. In the **Smlt Network** folder, click the **Inter-Switch Trunk** folder.
The contents pane shows all of the devices with inter switch trunks configured.
4. For the **IstPeerIp** of each peer device, enter the IP address associated with the VLAN on the other peer in the SMLT configuration.
5. For the **IstVlanId** of both peer devices, enter the VLAN ID of the SMLT configuration.
6. All ports in an SMLT configuration must be in the same VLAN.

7. Click **Apply**.
8. For the **IstSessionEnable** of both peer devices, click the entry to select **true**.
9. Click **Apply**.

Configuring a single port SMLT

About this task

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.

Procedure

1. Select **Configuration > MLT**.
2. In the MultiLink Trunking Manager navigation pane, under the **SMLT Network** folder, select the **Single-Port Smlt** folder.
3. On the Content Pane Toolbar, click **Add**.
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**.

Deleting a single port SMLT

Procedure

1. Select **Configuration > MLT**.
2. In the navigation pane, select the **single-port SMLT** folder.
3. On the Content Pane Toolbar, click **Delete**.
4. In the Delete dialog box, click **Yes** to confirm deletion.

Virtual Inter-Switch Trunk (vIST)

SMLT provides subsecond failover when a switch fails. Virtual Inter-Switch Trunk (vIST) improves upon that Layer 2 and Layer 3 resiliency by using a virtualized IST channel through the Shortest Path Bridging MAC (SPBM) cloud. The vIST channel carries the vIST control traffic and data traffic during an SMLT failover. This feature dramatically improves resiliency over other methods.

Because vIST uses a virtual channel and because Intermediate System to Intermediate System (IS-IS) runs over it, vIST eliminates the potential single point of failure with a dedicated MultiLink Trunk (MLT). The vIST channel is always up as long as there is SPBM connectivity between the vIST peers.

*** Note:**

vIST interoperates between any two devices that support vIST, and the devices do not have to be of the same type. Not all Extreme Networks products support vIST. For more information, see the product documentation.

vIST creates a virtualized channel through the SPBM cloud, and this channel connects two SMLT devices to form a virtualized Switch Cluster. The SPBM cloud can consist of as few as two nodes.

Users may observe a momentary increase in activity when a MAC delete message is received from a peer. This is due to vIST engaging in MAC learning activities. This is a normal operational procedure.

To configure vIST, you must complete the following actions:

1. Enable SPBM and IS-IS globally.
2. Configure SPBM and IS-IS.
3. Configure a Layer 2 VSN by assigning an I-SID to the C-VLAN, which is used by the vIST.
4. Create the vIST by configuring the peer IP address and VLAN ID.

*** Note:**

You must disable IS-IS globally before you delete a vIST, and then re-enable IS-IS after you create a new vIST.

Configuring vIST links

Perform the following procedure to add a vIST between aggregation switches.

Before you begin

- Enable SPBM and IS-IS globally.
- Configure SPBM and IS-IS.
- Configure a Layer 2 VSN by assigning an I-SID to the C-VLAN, which is used by the vIST.

Procedure

1. Select **Configuration > MLT**.
2. In the MLT navigation pane, expand the **SMLT Network** folder.
3. In the **SMLT Network** folder, click the **Virtual Inter-Switch Trunk** folder.
4. On the contents pane toolbar, click **Add**.
5. Select the IS-IS manual area.
6. In the **Device** fields, enter the IP address associated with each switch.
7. In the **Vlan IP** fields, enter the IP address associated with the vIST VLAN on both peers in the SMLT configuration.
8. In the **Subnet Mask** fields, enter the mask for each VLAN.
9. In the **Vlan Id** fields, enter the vIST VLAN IDs of the SMLT configuration.

10. Enter the I-SID.

11. Click **Save**.

Add Virtual Inter-Switch Trunk field descriptions

The following table describes the fields in the **Add Virtual Inter-Switch Trunk** dialog box.

Name	Description
Manual Area	Specifies the IS-IS manual-area (1–13 bytes in the format: <xx.xxx.xxx...xxx>.
Device	Specifies the IP addresses of the peer switches.
Vlan IP	Specifies the IP addresses of the vIST VLAN on the peer switches.
Subnet Mask	Specifies the subnet mask for the vIST VLANs.
Vlan Id	Configures a vIST VLAN ID number.
ISID	Specifies the I-SID associated with the C-VLAN.

Editing vIST peers

Perform the following procedure to edit vIST peers.

Procedure

1. Select **Configuration > MLT**.
2. In the MLT navigation pane, expand the **SMLT Network** folder.
3. In the **SMLT Network** folder, click the **Virtual Inter-Switch Trunk** folder.
4. In the **VistPeerIp** field of each peer device, enter the IP address associated with the vIST VLAN on the other peer in the SMLT configuration.
5. In the **VistVlanId** field of both peer devices, enter the vIST VLAN ID of the SMLT configuration.
6. Click **Apply**.

Virtual Inter-Switch Trunk field descriptions

The following table describes the fields in the Virtual Inter-Switch Trunk table.

Name	Description
Device	Shows the IP address of the vIST-capable switch.
SysName	Shows the system name of the vIST-capable switch.
VistSessionEnable	Shows the current administrative status of the vIST.
VistPeerIp	Specifies the peer IP address, which is the IP address of the vIST VLAN on the other aggregation switch.
VistVlanID	Configures a vIST VLAN ID number.

Chapter 10: Managing Routing

About Routing

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

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

Starting Routing view

Procedure

Select **Configuration > Routing**.

Result

The Routing view is launched and displayed in the content pane.

Routing view toolbar

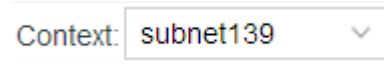







Icon	Name	Description
	Context	Use this option to select the available groups assigned to the current logged in user. After you change the context, a notification is sent to all opened configuration views in the system with the same logged in user. All

Table continues...

Icon	Name	Description
		opened views are refreshed after receiving this notification.
	Save Context	Use this option to save the context.
	Revert to Current Context	Use this option to revert to the current context.
	Refresh Groups	Use this option to view the new groups added to the current logged in user.
	Discover Routing	It discovers Routing view 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. The device appears in the add devices dialog box after this operation.
	Preferences	The user can select the required configuration by clicking on this button.

Routing view navigation pane

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

The following figure shows Routing view navigation pane.

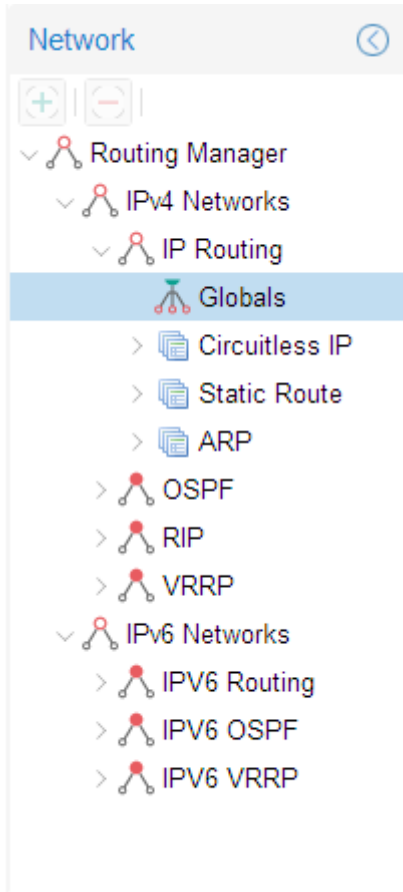


Figure 9: Routing view navigation pane

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

Rediscovering Routing

About this task

You can refresh the information in the Routing view with routing information polled from the network devices. You can use this feature to load any updated information that takes effect after you open the Routing view.

Procedure

1. Select **Configuration > Routing**.
2. On the Routing tool bar, click **Discover Routing**.
3. Click **OK** when the discovery operation is complete.

Viewing Routing folder contents

About this task

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






Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, expand Routing Manager and select a Routing folder.

Result

The contents of the folder appear as a table in the contents pane.

Routing view contents pane

Icon	Name	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.

Discover Routing

When you open the Routing Manager, an automatic discovery is performed for the available devices. After this step, you can obtain 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 you can see the possible warnings or errors that might appear during the discovery process. For more information about warnings and errors, see the log file.

Adding devices

Procedure

1. Click **Add Devices** in the toolbar.

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.

	<input type="checkbox"/>	Device ↑
1	<input type="checkbox"/>	10.133.139.1
2	<input type="checkbox"/>	10.133.139.100
3	<input type="checkbox"/>	10.133.139.102
4	<input type="checkbox"/>	10.133.139.254

2. Select the desired devices to add them to the Routing Manager tree.
3. Click **Save**.

Setting Routing Manager preferences

Procedure

1. Select **Configuration > Routing**.
2. Click **Preferences** icon from the tool bar.
3. In the Routing Manager Preferences window, 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.
 - 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 routing manager uses only the selected devices in the next discovery process.
4. Click **Ok** to add the changes.

Routing view features

You can use Routing view 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.

Supported devices for Routing view

The following table provides a feature/device matrix for the Routing view for ERS 8800, ERS 8600, and ERS 8300 devices.

Features		Supported devices		
		ERS 8800	ERS 8600	ERS 8300
IPv4 Routing	Circuitless IP	v3.3 and later	v3.3 and later	v2.2 and later
	Static Route	All versions	All versions	All versions
	ARP	All versions	All versions	All versions
OSPF	Interfaces	All versions	All versions	v3.0 and later
	Area	All versions	All versions	v3.0 and later
	Neighbors	All versions	All versions	v3.0 and later
RIP	Interfaces	All versions	All versions	All versions
	Status	All versions	All versions	All versions
VRRP	Interfaces	v7 and later	All versions	v3.0 and later
IPv6 Routing	Interfaces	v7 and later	v4.1 and later	not supported
IPv6 OSPF	Interfaces	v7 and later	v4.1 and later	not supported
	Area	v7 and later	v4.1 and later	not supported
	Neighbors	v7 and later	v4.1 and later	not supported
IPv6 VRRP	Interface	3.3 and later	3.3 and later	not supported

The following table provides a feature/device matrix for the Routing view 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 later	v2.0 and later
	Static Route	v5.1.1 and later	v5.5 and later	v4.0 and later	v2.1 and later
	ARP	v5.1.1 and later	v5.5 and later	v3.0 and later	v2.1 and later
OSPF	Interfaces	not supported	v5.5	v5.0 and later	v2.1 and later
	Area	not supported	v5.5	v5.0 and later	v2.1 and later
	Neighbors	not supported	v5.5	v5.0 and later	v2.1 and later
RIP	Interfaces	v5.2	v5.5	v5.0 and later	v2.1 and later
	Status	v5.2	v5.5	v5.0 and later	v2.1 and later
VRRP	Interfaces	not supported	v5.5	v5.0 and later	v2.1 and later
IPv6 Routing	Interfaces	v5.1.1 and later	v5.6.3 and later	v6.2.7 and later	not supported
IPv6 OSPF	Interfaces	not supported	v5.6.3 and later	not supported	not supported
	Area	not supported	v5.6.3 and later	not supported	not supported
	Neighbors	not supported	v5.6.3 and later	not supported	not supported
IPv6 VRRP	Interface	not supported	v5.6.3 and later	not supported	not supported

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

Features		Supported devices			
		VSP 7xxx	VSP 9xxx	VSP 8xxx	WC 8xxx
IPv4 Routing	Circuitless IP	v10.2 and later	v3.0.0, v4.0	v4.0	not supported
	Static Route	v10.2 and later	v3.0.0, v4.0	v4.0	v1.0.0
	ARP	v10.2 and later	v3.0.0, v4.0	v4.0	v1.0.0
OSPF	Interfaces	v10.2 and later	v3.0.0, v4.0	v4.1 and later	not supported
	Area	v10.2 and later	v3.0.0, v4.0	v4.1 and later	not supported
	Neighbors	v10.2 and later	v3.0.0, v4.0	v4.1 and later	not supported
RIP	Interfaces	v10.2 and later	v3.0.0, v4.0	v4.0	not supported
	Status	v10.2 and later	v3.0.0, v4.0	v4.0	not supported
VRRP	Interfaces	v10.1 and later	v3.0.0, v4.0	v4.1 and later	not supported
IPv6 Routing	Interfaces	v10.3 and later	v3.0.0, v4.0	v4.1 and later	not supported
IPv6 OSPF	Interfaces	v10.3 and later	v4.0	not supported	not supported
	Area	v10.3 and later	v4.0	not supported	not supported
	Neighbors	v10.3 and later	v4.0	not supported	not supported
IPv6 VRRP	Interface	v10.3 and later	v4.0	not supported	not supported

The following table provides a feature/device matrix for the Routing view for APLS, VSP 4xxx, and VSP 72xx devices.

Features		Supported devices		
		APLS	VSP 4xxx	VSP 72xx
IPv4 Routing	Circuitless IP	not supported	not supported	not supported
	Static Route	not supported	not supported	not supported
	ARP	not supported	not supported	not supported
OSPF	Interfaces	v4.3.1 and later	v4.1 and later	all versions
	Area	v4.3.1 and later	v4.1 and later	all versions
	Neighbors	v4.3.1 and later	v4.1 and later	all versions
RIP	Interfaces	not supported	not supported	not supported
	Status	not supported	not supported	not supported
VRRP	Interfaces	v4.3.1 and later	v4.1 and later	all versions
IPv6 Routing	Interfaces	v4.3.1 and later	v4.1 and later	all versions
IPv6 OSPF	Interfaces	not supported	not supported	not supported
	Area	not supported	not supported	not supported
	Neighbors	not supported	not supported	not supported
IPv6 VRRP	Interface	not supported	not supported	not supported

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 Globals

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > IP Routing > Globals**.

The Globals table appears in the contents pane.

3. To modify any of the configurable global routing properties, modify the fields directly in the contents pane, and click **Apply Changes**.

IP Routing Globals table field descriptions

Field	Description
Devices	Identifies the device.
SysName	System name
Forwarding	Sets the switch for forwarding (routing) or not-forwarding.
DefaultTTL	Sets the default time-to-live (TTL) value for a routed packet. TTL indicates the maximum number of seconds elapsed before a packet is discarded. Enter an integer between 1 and 255. The default value of 255 is inserted in the TTL field whenever one is not supplied in the datagram header.
ReasmTimeout	The maximum number of seconds that received fragments are held while they wait for reassembly at this entity. The default value is 30 seconds.
ArpExtLifeTime	The lifetime in minutes of an ARP entry within the system.
ICMPUnreachableMsgEnable	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).
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.
AllowMoreSpecificNonLocal RouteEnable	Enables or disables a more specific nonlocal route.
UdpCheckSumEnable	Enables or disables UDP checksum calculation.
ICMPRedirectMsgEnable	Enables or disables the switch from sending ICMP destination redirect messages.
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.

Table continues...

Field	Description
EcmpMaxPath	Used to globally configure the maximum number of ECMP paths. <ul style="list-style-type: none"> • 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

About this task

You can configure circuitless IP (Clip) interfaces on the following devices:

- ERS 1600 v2.0 and later
- ERS 45xx v5.7.2 and later
- ERS 48xx v5.7.2 and later
- ERS 5xxx v6.3.1 and later
- ERS 8300 v2.2 and later
- ERS 8600 v3.3 and later
- ERS 8800 v3.3 and later
- VSP 4xxx all versions
- VSP 72xx all versions
- VSP 8xxx all versions
- VSP 70xx v10.2 and later
- VSP 9xxx v3.0.0

Perform the following procedure to configure circuitless IP and to add or delete circuitless IP interfaces.

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > IP Routing > Circuitless IP**.
3. Select the device to configure CLIP.

4. From the Routing Manager toolbar, select **Add Entry with Form**.
5. In the Circuitless IP Insert dialog box, enter the required information.
6. Click **Save**.
The new CLIP interface appears in the contents pane.
7. 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.

*** Note:**

You cannot modify CLIP interface fields in the contents pane.

IPv4 Routing Circuitless IP table field descriptions

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

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > IP Routing > Static Route**, then select a device.
3. To add a route, from the tool bar, click **Add Entry with Form**.
4. Complete the fields as required, and select the devices for which the static route applies.
5. Click **Save**.
The new entry appears in the contents pane.
6. To modify any of the configurable static route properties of an entry, modify the fields directly in the contents pane and click **Apply Changes**.

Job aid

Field	Description
OwnerVrflid	Specifies the VRF to which the route belongs to.
Destination	Specifies the destination IP address of this route.
Mask	Specifies the destination address IP mask.
NextHop	Specifies the next hop IP address for the route.
NextHopVrflid	Specifies the next-hop VRF ID in interVRF static route configurations. Identifies the VRF in which the ARP entry resides.

Table continues...

Field	Description
Enable	Adds a static or default route to the router or VRF.
Status	Specifies the status of the route.
Metric	Specifies the primary routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route RouteProto value.
Interface	Specifies the route index of the Next Hop. The interface index identifies the local interface through which the next hop of this route is reached.
Preference	Configures the preference for the static route in the range 1–255.
LocalNextHop	Enables and disables LocalNextHop. If enabled, the static route becomes active only if the system has a local route to the network. If disabled, the static route becomes active if the system has a local route or a dynamic route.

Configuring IPv4 routing ARP

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > IP Routing > ARP**, and then select a device.
3. To add a route, from the tool bar, click **Add Entry with Form**.
4. In the Insert ARP dialog box, complete the fields as required, and select the devices for which the ARP route applies.
5. Click **Save**.

The new entry appears in the contents pane.

IPv4 routing ARP field descriptions

Field	Description
Interface	The router interface for this ARP entry: <ul style="list-style-type: none"> • 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.

Table continues...

Field	Description
Type	The type of ARP entry: <ul style="list-style-type: none"> • 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 view](#) on page 128.

Configuring OSPF General Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > OSPF > General**.
3. In the OSPF – General table, modify the fields of configurable OSPF general properties as needed.
4. Click **Apply Changes**.

OSPF general field descriptions

Field	Description
Devices	Identifies the device.
SysName	System name.
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). <p>! Important:</p> <p>The AreaBdrRtrStatus value must be true to create a virtual router interface.</p>
ASBdrRtrStatus	When the ASBdrRtrStatus option is selected, the router is configured as an autonomous system boundary router (ASBR).

Table continues...

Field	Description
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 change occurred in a router link state database and to compare the link state databases of two routers.
OriginateNewLsas	The number of new link state advertisements that have been originated. This number is incremented each time the router originates a new link state area (LSA).
RxNewLsas	The number of link state advertisements received that are determined to be new instances. This number does not include newer instances of self-originated link state advertisements.
DefaultMetric 10MegPort	Indicates the default cost to be applied to the 10 Mb/s interface (port).
DefaultMetric 100MegPort	Indicates the default cost to be applied to the 100 Mb/s interface (port).
DefaultMetric 1000MegPort	Indicates the default cost to be applied to the 1000 Mb/s interface (port).
DefaultMetric10000MegPort	Indicates the default cost to be applied to the 10000 Mb/s interface (port).
TrapEnable	Indicates whether to enable traps relating to the OSPF.
AutoVirtLink Enable	Enables or disables automatic creation of virtual links.
SpfHoldDown Time	Allows you to change the OSPF hold-down timer value (3 to 60 seconds).
Action	Allows you to initiate a new SPF run to update the routing table.
Rfc1583 Compatibility	Allows you to control the preference rules used when choosing among multiple AS-External LSAs advertising the same destination. When you enable this setting, the preference rule is the same as specified by RFC 1583. When you disable the setting, the new preference rule as described in RFC 2328 is applicable, which potentially prevents the routing loops when AS-External LSAs for the same destination originate from different areas.
LastSpfRun	Used to indicate the time (SysUpTime) since the last SPF calculated by OSPF.

Configuring OSPF Interfaces

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > OSPF > Interfaces**, and then select a device.
3. Select the **OspfInterfaces** tab.
4. To add an interface, from the menu bar, click **Add Entry with Form**.
5. In the Insert IPV4 OSPF window, complete the fields as required.
6. Click **Save**.
7. In the OSPF Interfaces table, modify any of the configurable OSPF interface properties as needed, then click **Apply**.

OSPF interfaces table field descriptions


Field	Description
IpAddress	IP address of the current OSPF interface.
AddressLessIf	Designates whether an interface has an IP address. Interfaces with an IP address = 0 Interfaces without IP address = ifIndex
AreaId	Dotted decimal value to designate the OSPF area name. VLANs that maintain the default area setting on the interface cause the link-state database (LSDB) to be inconsistent.  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.

Table continues...

Field	Description
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.
Type	Type of OSPF interface (broadcast or passive)
AuthType	Type of authentication required for the interface. <ul style="list-style-type: none"> • 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.
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. <p>! Important:</p> <p>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.</p>
TransitDelay	Length of time, in seconds between 1 and 3600, required to transmit an LSA update packet over the interface.
RetransInterval	Length of time, in seconds between 1 and 3600, required between LSA retransmissions.
RtrDead 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.
PollInterval	Length of time, in seconds, between Hello packets sent to an inactive OSPF router.
Events	Number of state changes or error events that occurred through all interfaces.

Configuring OSPF advanced interfaces

About this task

Perform the following procedure to configure OSPF interfaces on ERS 8300 devices.

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPv4 Networks > OSPF > Interfaces**.
3. Click the **OspfAdvancedInterfaces** tab and select the device you want to configure.
4. To modify any of the configurable OSPF interface properties for an entry, modify the fields directly in the contents pane and click **Apply Changes**.

OSPF Advanced Interfaces table field descriptions




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: <ul style="list-style-type: none"> • 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	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. <p> Important: The link state database (LSDB) is inconsistent if the settings is default area for VLAN.</p>
Advertise WhenDown	Indicates when the interface advertises. <p> Important: Indicates even when it is non-operational.</p>

Table continues...

Field	Description
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	<p>It is used only during the election and backup of the designated router.</p> <p>The OSPF priority for the interface during the election process for the designated route:</p> <ul style="list-style-type: none"> • designated router—interface with the highest priority number • backup designated router—interface with the second highest priority <p> Important:</p> <p>The priority range is from 0 to 255 and the default is 1. The interface is not designated if the priority is 0.</p>
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

About this task

Before you can enable OSPF on a circuitless IP (CLIP) interface, you must configure the CLIP interface on the device.

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > OSPF > Interfaces**, then select a device.
3. In the contents pane, select the **OspfClipInterfaces** tab.
4. To modify any of the configurable OSPF CLIP interface properties for an entry, modify the fields directly in the contents pane and click **Apply Changes**.

OSPF CLIP Interfaces table field descriptions

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.
IfAreald	Dotted-decimal value to designate the OSPF area name.

Configuring OSPF Area**Procedure**

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > OSPF > Area**, then select a device.
3. To add an area to the OSPF Area table, from the menu bar, click **Add Entry with Form**.
4. Complete the fields as required, and select the devices for which the area applies.
5. Click **Save**.

Result

The new entry appears in the OSPF Area table.

OSPF area field descriptions

Field	Description
Areald	A 32-bit integer uniquely identifying an area. Area ID 0.0.0.0 is used for the OSPF backbone. VLANs that maintain the default area setting on the interface cause the LSDB to be inconsistent.
ImportAsExtern	The area support for importing AS-external link-state advertisements (LSA). Options include importExternal (default), importNotExternal, or importNssa (not so stubby area).
SpfRuns	Used to indicate the number of SPF calculations performed by OSPF.
AreaBdrRtrCount	The total number of area border routers reachable within this area. The value, initially zero, is calculated in each SPF Pass.
AsBdrRtrCount	The total number of autonomous system border routers reachable within this area. The value, initially zero, is calculated in each SPF pass.

Table continues...

Field	Description
AreaLsaCount	The total number of link state advertisements in the link state database for this area, excluding AS-external LSAs.
AreaLsaCksumSum	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.
Activelfcount	The number of active interfaces in the area.

Configuring OSPF Neighbors

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPv4 Networks > OSPF > Neighbors**, and then select a device.
3. To add a neighbor entry, from the menu bar, click **Add Entry with Form**.
4. In the Add Entry window, complete the fields as required.
5. Click **Save**.

OSPF neighbor table field descriptions

Field	Description
IpAddr	The neighbor IP address.
AddressLessIndex	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.

Table continues...

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.
ospfNbmaNbrPermanence	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 view](#) on page 128.

Configuring RIP Globals

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > RIP > Globals**.
3. In the RIP–Globals table, modify the fields of configurable RIP global properties as needed, then click **Apply Changes**.

RIP Globals table field descriptions

Field	Description
Devices	Identifies the device.
SysName	System name.
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.

Table continues...

Field	Description
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

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > RIP > Interfaces**, and then select a device.
3. In the RIP interfaces table, modify the fields of configurable interface parameters as needed, then click **Apply Changes**.

RIP Interfaces table field descriptions

Field	Description
Address	The IP address of the router interface.
Domain	The domain of the router interface.
AuthType	The type of authentication required for the interface.
AuthKey	Specify key if the simple password is selected in the interface AuthType field. The key can be up to 8 characters.
Send	What the router sends on this interface (selected from a menu): <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • rip1 • rip2 • rip1OrRip2 The rip2 and rip1OrRip2 imply reception of multicast packets.

Configuring RIP Advanced Interface parameters

About this task

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > RIP > Interfaces**, and then select a device.
3. Click the **RipAdvancedInterfaces** tab.
4. In the Interfaces Advance table, modify the fields of configurable interfaces as needed, then click **Apply Changes**.

RIP Advanced Interfaces table field descriptions

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

Table continues...

Field	Description
	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

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > RIP > Status**, and then select a device.

Result

The RIP Status table appears in the contents pane.

RIP Status table field descriptions

Field	Description
Address	The IP address of the router interface.
RcvBadPackets	The number of RIP response packets received by the RIP process that were subsequently discarded for any reason (for example, a version 0 packet or an unknown command type).
RcvBadRoutes	The number of routes, in valid RIP packets, that were ignored for any reason (for example, unknown address family or invalid metric).
SentUpdates	The number of triggered RIP updates actually sent on this interface. This field explicitly does not include full updates sent containing new information.

Configuring VRRP

For a list of devices that support VRRP, see [Supported devices for Routing view](#) on page 128.

Configuring VRRP Globals

Procedure

1. Select **Configuration > Routing**.

2. In the navigation pane, select **Routing Manager > IPV4 Networks > VRRP > Globals**, and then select a device.
3. In the VRRP Globals table, modify any of the configurable properties as required, then click **Apply Changes**.

VRRP Globals table field descriptions

Field	Description
Devices	Identifies the device.
SysName	System name.
NotificationCntl	Indicates whether the VRRP-enabled router generates Simple Network Management Protocol (SNMP) traps for events defined in this management information base (MIB): <ul style="list-style-type: none"> • Enabled—SNMP traps are sent • Disabled—no traps are sent
VirtualAddrEnable	Used to configure whether this device must respond to pings directed to a virtual router IP address.

Configuring VRRP Interfaces

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV4 Networks > VRRP > Interfaces**.
3. In the VRRP – Interfaces table, modify any of the configurable properties, then click **Apply Changes**.

VRRP Interfaces table field descriptions

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: <ul style="list-style-type: none"> • initialize—waiting for a startup event • backup—monitoring availability and state of the master router

Table continues...

Field	Description
	<ul style="list-style-type: none"> • 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.
FasterAdvIntervalEnable	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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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).

Table continues...

Field	Description
	<ul style="list-style-type: none"> The VRRP holddown timer applies to the VRRP BackupMaster feature.
HoldDownState	When Hold Down Timer is counting down status is active and preemption occurs. The text box displays dormant when preemption is not pending.
HoldDownTimeRemaining	The remaining time (in seconds) before preemption.
CriticalIpAddrEnable	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.
BackUpMasterState	<p>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.</p> <ul style="list-style-type: none"> up: during BackupMaster state down: during the original state

View and configure 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 view](#) on page 128.

Configuring IPv6 routing

Configuring IPv6 routing Globals Procedure

1. Select **Configuration > Routing**.

2. In the navigation pane, select **Routing Manager > IPV6 Networks > IPV6 Routing > Globals**.

The Globals table appears in the contents pane.

3. To modify any of the configurable global routing properties, modify the fields directly in the contents pane and click **Apply Changes**.

IPv6 Routing Globals table field descriptions

Field	Description
Devices	Identifies the device.
SysName	System name.
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 unreachable 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.

Configuring IPv6 routing Interfaces

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPV6 Networks > IPV6 Routing > Interfaces**, and then select a device.
3. To add an interface entry, from the menu bar, click **Add Entry with Form**.
4. In the Insert IPv6 Routing Interface window, complete the fields as required.
5. Click **Save**.

Result

The new entry appears in the Interfaces table.

IPv6 Routing Interfaces table field descriptions

Field	Description
Interface	A unique value to identify a physical interface or a logical interface (VLAN). For the brouter port, this is the ifindex of the port. For the VLAN, this is the ifindex of the VLAN.
Identifier	IPv6 address interface identifiers. This is a binary string of up to 8 octets in network byte-order.
IdentifierLength	The length of the interface identifier in bits.
Descr	A textual string containing information about the interface. This string can be set by a network management system.
VlanId	A value that uniquely identifies the VLAN associated with this entry. This value corresponds to the lower 12 bits in the IEEE 802.1Q VLAN tag.
Type	The interface type.
ResmMaxSize	MTU for this IPv6 interface. This value should be the same for all the IP addresses defined on this interface.
PhysAddress	The media-dependent physical address. For Ethernet media, this is the MAC address.
AdminStatus	The indication of whether IPv6 is enabled (up) or disabled (down) on this interface. This object does not affect the state of the interface itself, only its connection to an IPv6 stack.
OperStatus	Operating status of the interface.
ReachableTime	The time (in milliseconds) a neighbor is considered reachable after receiving a reachability confirmation. Reference RFC2461, Section 6.3.2
RetransmitTime	The time (in milliseconds) between retransmissions of Neighbor Solicitation messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Reference RFC2461, Section 6.3.
MulticastAdminStatus	The admin status for multicast for this interface.

Configuring IPv6 OSPF

For a list of devices that support IPv6 OSPF, see [Supported devices for Routing view](#) on page 128.

Configuring IPv6 OSPF General Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select **Routing Manager > IPv6 Networks > IPv6 OSPF > General**.
3. In the IPv6 OSPF – General table, modify the fields of configurable IPv6 OSPF general properties as needed.
4. Click **Apply Changes**.

IPv6 OSPF General table field descriptions


Name	Description
Devices	Identifies the device.
SysName	System name.
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.
AreaBdrRtrStatus	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).
AsScopeLsaCount	A read-only field displaying the number of external (LS type 5) LSAs in the link-state database.
AsScopeLsaChecksumSum	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.
OriginateNewLsas	A read-only field displaying the number of new LSAs. The number is incremented each time the router originates a new LSA.

Table continues...

Name	Description
RxNewLsas	A read-only field displaying the number of new LSAs received. This number does not include new instantiations of self-originated LSAs.
ExtLsaCount	A read-only field displaying the number of external (LS type 0x4005) LSAs in the link-state database.
ExtAreaLsdbLimit	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).
MulticastExtensions	<p>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:</p> <ul style="list-style-type: none"> • <code>intraAreaMulticast</code>—forwards to directly attached areas (called intra-area multicast routing) • <code>interAreaMulticast</code>—forwards between OSPFv3 areas (called inter-area multicast routing) • <code>interAsMulticast</code>—forwards between Autonomous Systems (called inter-AS multicast routing)
ExitOverflowInterval	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.
DemandExtensions	The router support for demand routing.
TrafficEngineeringSupport	The router support for traffic engineering extensions.
ReferenceBandwidth	The reference bandwidth in kilobits per second for calculating default interface metrics. The default value is 100 000 Kb/s (100 Mb/s).
RestartSupport	<p>The router support for OSPF hitless restart. Options include no restart support, only planned restarts, or both planned and unplanned restarts. Options include:</p> <ul style="list-style-type: none"> • <code>none</code> (default) • <code>plannedOnly</code> • <code>plannedAndUnplanned</code>

Table continues...

Name	Description
RestartStatus	A read-only field indicating the current status of OSPF hitless restart. Options include: <ul style="list-style-type: none"> • 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.
RestartExitReason	A read-only field indicating the outcome of the last attempt at a hitless restart. Options include: <ul style="list-style-type: none"> • 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

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select a node under **Routing Manager > IPv6 Networks > IPv6 OSPF > Interfaces**.
3. In the OSPF Interfaces table, modify the fields of any configurable IPv6 OSPF interfaces as needed.
4. Click **Apply Changes**.

IPv6 OSPF Interfaces table field descriptions

Name	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.

Table continues...

Name	Description
	<p>! Important:</p> <p>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).</p>
Type	Type of OSPF interface (broadcast, nbma, point-to-point, or point-to-multipoint).
AdminStat	Current administrative state of the OSPF interface (enabled or disabled).
RtrPriority	OSPF priority for the interface during the election process for the designated router. The interface with the highest priority number is the designated router. The interface with the second-highest priority becomes the backup designated router. If the priority is 0, the interface cannot become the designated router or the backup. The priority is used only during election of the designated router and backup designated router. The range is 0 to 255. The default is 1.
TransitDelay	Length of time, in seconds (1 through 1800), required to transmit an LSA update packet over the interface.
RetransInterval	Length of time, in seconds (1 through 1800), required between LSA retransmissions.
HelloInterval	<p>Length of time, in seconds, between Hello packets. This value must be the same for all routers attached to a common network.</p> <p>! Important:</p> <p>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.</p>
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.

Table continues...

Name	Description
State	<p>A read-only field indicating the OSPFv3 interface state. Options include:</p> <ul style="list-style-type: none"> • down • loopback • waiting • pointToPoint • designatedRouter • backupDesignatedRouter • otherDesignatedRouter
DesignatedRouter	<p>A read-only field indicating the router ID of the designated router.</p>
BackupDesignatedRouter	<p>A read-only field indicating the router ID of the backup designated router.</p>
Events	<p>A read-only field indicating the number of times this OSPF interface changed state or an error occurred.</p>
MetricValue	<p>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.</p>
LinkScopeLsaCount	<p>A read-only field indicating the number of Link-Scope LSAs in the link-state database.</p>
LinkLsaCksum Sum	<p>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.</p>
InstId	<p>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.</p>
DemandNbrProbe	<p>Indicates whether neighbor probing is enabled. Neighbor probing determines whether the neighbor is inactive.</p>
DemandNbrProbeRetxLimit	<p>The number of consecutive LSA retransmissions before the neighbor is deemed inactive and the neighbor adjacency is deactivated.</p>
DemandNbrProbeInterval	<p>Defines how often, in seconds, the neighbor is probed.</p>

Configuring IPv6 OSPF Area

Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select a node under **Routing Manager > IPv6 Networks > IPv6 OSPF > Area**.

The IPv6 OSPF – Area table appears in the contents pane.

3. To add an area, from the menu bar, click **Add Entry with Form**.
4. Complete the fields as required.
5. Click **Save**.
6. Click **OK** or **Details** if there are errors or warnings.

The new entry appears in the contents pane.

IPv6 OSPF area table field descriptions

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.

Table continues...

Field	Description
StubMetric	The number of active interfaces in this area.
NssaTranslatorRole	Indicates an NSSA border router ability to translate NSSA type-7 LSAs into type-5 LSAs. Options include: <ul style="list-style-type: none"> • always • candidate (default)
NssaTranslatorState	Indicates if and how an NSSA border router translates NSSA type-7 LSAs into type-5 LSAs. Options include: <ul style="list-style-type: none"> • 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.
NssaTranslatorStabilityInterval	The number of seconds after an elected translator determines translation is not required that it resumes translation duties.
NssaTranslatorEvents	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: <ul style="list-style-type: none"> • rcOspfV3Metric indicates the OSPF metric • comparableCost indicates an external type 1 • nonComparable indicates an external type 2

Configuring IPv6 OSPF Neighbors Procedure

1. Select **Configuration > Routing**.
2. In the navigation pane, select a node under **Routing Manager > IPv6 Networks > IPv6 OSPF > Neighbors**.
3. Select and modify any of the fields in the IPv6 OSPF – Neighbors table in the contents pane.
4. Click **Apply Changes**.

IPv6 OSPF Neighbors table field descriptions

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: <ul style="list-style-type: none"> • unknown • ipv6 • 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: <ul style="list-style-type: none"> • 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.

Table continues...

Field	Description
LsRetransQLen	A read-only field indicating the number of elapsed seconds between advertising retransmissions of the same packet to a neighbor.
HelloSuppressed	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.
RestartHelperStatus	A read-only field indicating that the router acts as a hitless restart helper for the neighbor. Options include: <ul style="list-style-type: none"> • notHelping • helping
RestartHelperAge	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.
RestartHelperExtReason	A read-only field indicating the outcome of the last attempt to act as a hitless restart helper for the neighbor. Options include: <ul style="list-style-type: none"> • 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 • 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. Select **Configuration > Routing**.
2. In the navigation pane, select a node under **Routing Manager > IPv6 Networks > IPv6 VRRP > Globals**.

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): <ul style="list-style-type: none"> • 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. Select **Configuration > Routing**.
2. In the navigation pane, select a node under **Routing Manager > IPv6 Networks > IPv6 VRRP > Interfaces**.
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: <ul style="list-style-type: none"> • initialize—waiting for a startup event • backup—monitoring availability and state of the master router

Table continues...

Field	Description
	<ul style="list-style-type: none"> • 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.
BackUpMasterState	<p>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.</p> <ul style="list-style-type: none"> • 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.

Table continues...

Field	Description
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 11: Managing Virtual Routing and Forwarding

About Virtual Routing and Forwarding

Virtual Routing and Forwarding (VRF) 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 to v4.1.1
- VSP 4xxx all versions
- VSP 72xx up to v5.1.1
- VSP 8xxx all versions

You can use VRF view to configure Virtual Routing and Forwarding 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. The system discovers the VRF information using the GlobalRouter (VRF0) context, which allows the administrator to access and manage the entire switch. When the administrator assigns users the ability to use VLAN view, the 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 configuration views, such as Routing and EDM plug-ins.

When an administrator configures a context, the context applies to the system access, 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 correctly operate the VRF view.
- 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.

VRF view

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 user role assigned by the administrator.
- You must have devices assigned by the administrator.

Starting VRF view

Procedure

1. Select **Configuration > VRF**.
The VRF discovery is triggered.
2. In the VRF discovery result dialog box, click **Ok**.
3. In the navigation pane, select a node under **VRF Device > Device List**.

Result

The VRF tabs appear in the content pane.

VRF view 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.

VRF navigation pane toolbar options

Parts	Description
Context	Use this option to select the available groups assigned to the current logged in user. After you change the context, a notification is sent to all opened configuration views in the system with the same logged in user. All opened views are refreshed after receiving this notification.
Save Context	Use this option to save the context.
Revert to Current Context	Use this option to revert to the current context.
Refresh Groups	Use this option to view the new groups added to the current logged in user.
Discover VRF	Discovers the network and reloads VRF view with the latest information.
Help	Opens the online help.

Adding VRF on a device or multiple devices

Procedure

1. Select **Configuration > VRF**.
2. In the navigation pane, select a node under **VRF Device > Device List**.
3. In the Content pane toolbar, click **Create Entry**.

Add

Add Entry

Id [1 - 127 | 255 | 512][VSP4k/72xx/8k support [1-511]]

Name

TrapEnable

MaxRoutes [0 - 8000 | 25000 | 250000 | 500000]

RpTrigger

rip ospf bgp

pim

[VSP 4850 (v3.0) & VSP 8284XSQ (v4.0) doesn't support RpTrigger]

MaxRoutesTrapEnable

Devices

<input type="checkbox"/>	Device
<input checked="" type="checkbox"/>	10.133.139.1
<input type="checkbox"/>	10.133.139.81
<input type="checkbox"/>	10.133.139.95
<input type="checkbox"/>	10.133.139.98
<input type="checkbox"/>	10.133.139.100
<input type="checkbox"/>	10.133.139.103

Ok Close Help

*** Note:**

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

- Configure the parameters as appropriate.
- In the **Devices** table, select the target device or devices.

If you select multiple devices, then the VRF view 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 Devices table.

- Click **Ok**.

Setting VRF content for devices

Procedure

1. Select **Configuration > VRF**.
2. In the navigation pane, select **VRF Device > Set Current VRF**.
3. In the Current VRF table in the contents pane, change the VRF Id in the **Id** field for the target devices.
4. 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 VRF details

Procedure

1. Select **Configuration > VRF**.
2. In the navigation pane, select a node under **VRF Device > Device List**.
The VRF information displays in the contents pane.
3. To see the VRF statistics in the contents pane, click the **VRF Stats** tab.

Result

The VRF statistics information displays in the contents pane.

Editing a single or multiple VRF configurations

Procedure

1. Select **Configuration > VRF**.
2. In the navigation pane, select a node under **VRF Device > Device List**.
3. Select the **VRF** tab.
4. Edit the fields directly in the VRF configuration table in the contents pane.
5. Click **Apply Changes** to confirm the changes you made.
6. **(Optional)** Click **Revert Changes** to revert all the changes made in the VRF table.

Deleting a VRF configuration from a device

Procedure

1. Select **Configuration > VRF**.
2. In the navigation pane, select a node under **VRF Device > Device List**.
3. In the content pane, select the VRF configuration for deletion.
4. Click **Delete Entry**.
5. Click **Yes** to confirm deletion.

VRF enhancement—VLAN and routing

Multicast and routing use the selected VRF ID from the VRF view to discover the protocol information. Protocols are virtualized based on the supported devices and enabled protocols for the particular VRF.

VRF - based discovery

The system 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 view uses the VRF ID to communicate with the device. The VLAN view 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 12: Managing Multicast

About Multicast

With the Multicast view you can manage approved vendor devices that support multicast. The Multicast view displays multicast configurations across a network of devices. You can edit the Multicast view and highlight multicast information on the topology map; however, to fully configure the multicast network, you must use EDM or JDM.

The Multicast view 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 view requires EFO and one or more of the following devices:

- APLS v4.3 and v4.3.1
- VSP 7000/9000
- VSP 4000 v3.1 and later
- VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1 and later
- ERS 8600/8800
- ERS 48xx/55xx/35xx/45xx/25xx
- ERS 1424/16xx
- ERS 59xx v7.0 and later
- Ethernet Switch
- Legacy BayStack devices

Multicast view

After you start the Multicast view for the first time, the Multicast performs a discovery of devices, and shows the progress of the discovery. As with all Configuration views of the system, you can filter the devices through the Preferences button at the top left of the Multicast tab near the Discovery button. You can use the Discovery button to perform subsequent discoveries.

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

- The Multicast 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 content pane—displays to the right of the Multicast navigation tree. After you select a node in the Multicast navigation tree, information about the node displays in the Multicast content pane.

Starting Multicast view

About this task

Perform the following procedure to start the Multicast view.

Procedure

1. Select **Configuration > Multicast**.
2. In the navigation pane, expand **Multicast Manager**.

Actions

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

Manager actions

You can perform the following actions in the Multicast view context:

- Context—Select the available groups assigned to the current logged in user.
- Save Context—Saves the Context.
- Revert to Current Context—Use this option to revert to the current context.
- Refresh Groups—Use this option to view the new groups added to the current logged in user.
- 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 view single table context:

 **Note:**

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.

Performing a Multicast Discovery

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

Procedure

1. Select **Configuration > Multicast** to start Multicast.
2. From the Multicast menu bar, click **Discover Multicast**.
The Multicast discovery progress bar appears.
3. To view details of the discovery, click **Details**.
4. After the discovery is complete, click **OK**.

Adding a device in the Multicast view

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

 **Note:**

The Add button is available only if you select a major functionality from the 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 system.
- There are devices that are discovered after performing a discovery in the Multicast view.
- 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. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select a location for the device.
3. From the Multicast menu bar, click **Add Devices**.

4. Select the required devices.
5. Click **Save**.

Deleting a device from the Multicast view

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

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select a device.
3. From the Multicast menu bar, click **Remove Device**.

Editing Protocol tables in the Multicast view

Perform the following procedure to edit Protocol tables in the Multicast view.

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select the appropriate folders and select a device.
3. In the Multicast content pane, select a tab.
4. In the table, select a cell with a white background and change the value.
5. Click **Apply Changes**.

Selecting preferences for the Multicast view

Perform the following procedure to manage user preferences.

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast menu bar, click **Preferences**.

The Multicast Preferences window appears.

3. 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 preferences are:
 - **Manage by device family**—allows you to choose the supported device families: APLS, VSP 4XXX, VSP 8XXX, VSP 9XXX, ERS 8000, ERS 16XX, Ethernet Switch/ERS 25XX, Alteon, Legacy BayStack, Legacy ERS 1424/16XX, VSP 70XX, ERS 5XXX/4XXX/3XXX, WC 8XXX, WLAN AP, VSP 72XX.
 - **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.
4. Click **OK**.

Navigation tree structure

The Multicast view 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, Multicast view 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
- DVMRP
- PIM_SM
- MSDP
- Multicast Route
- Policy

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

Using tables to change device configuration

The Multicast 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.

IGMP and IGMP Snoop

You configure IGMP and IGMP Snooping using the Device Manager. You can configure all devices supported by the system 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 14: 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.

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 15: Parts of the IGMP and IGMP Snoop Globals folder

Parts	Description
Devices	IP address of the device.
SysName	Identifies the system name 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: <ul style="list-style-type: none"> 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

Table continues...

Parts	Description
	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.

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 16: Parts of the IGMP and IGMP Snoop Devices folder

Parts	Description
Interfaces tab for APLS v4.3 and v4.3.1, ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and later, ERS 1424/16xx devices, and VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1 and later.	Displays information about ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and later, ERS 1424/16xx, and VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1 and later IGMP interfaces.
Groups tab for APLS v4.3 and v4.3.1, ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and later, ERS 8300 devices, and VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1 and later.	Displays information about ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and later, ERS 8300, and VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1 and later multicast groups.
Cache tab for APLS v4.3 and v4.3.1, ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and later, ERS 1424/16xx devices, and VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1 and later.	Displays information about ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and later, ERS 1424/16xx, VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1 and later multicast groups.
Senders tab for APLS v4.3 and v4.3.1, ERS 8600/8800, VSP 9000, VSP 4000 v3.1 and later, ERS 8300 devices, and VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1 and later.	Displays information about ERS 8600/8800, VSP 9000, VSP 4000 v3.1 and later, ERS 8300, VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1, and later multicast senders.

Interface tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000, ERS 1424/16xx, and VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1 and above 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, and VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1 and above devices only. Otherwise, the field applies to ERS 8600 and ERS 1424/16xx devices.

Table 17: 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, ERS 1424/16xx, and VOSS (VSP82xx, VSP84xx, VSP72xx) v4.1 and above devices

Part	Description
Interface	Interface on which IGMP is enabled.
QueryInterval	Frequency with which IGMP Host-Query packets are transmitted on this interface.
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.
Querier	Address of the IGMP querier on the IP subnet to which the interface is attached.
QueryMaxResponseTime	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.

Table continues...

Part	Description
	Set the parameter according to the version of IGMP currently in use to maximize the network performance. The parameters are: <ul style="list-style-type: none"> • IGMPv1—Disable • IGMPv2—Enable • IGMPv3—Enable
SsmEnable Not applicable for VSP 7000 devices.	Enables SSM.

Groups tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000, ERS 8300, and VOSS (VSP82XX, VSP84XX, VSP 72XX) v4.1 and above 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 above, ERS 8300, and VOSS (VSP82XX, VSP84XX, VSP 72XX) v4.1 and above devices.

Table 18: Parts of the IGMP and IGMP Snoop Devices folder Groups tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000 v3.1 and above, ERS 8300, and VOSS (VSP82XX, VSP84XX, VSP 72XX) v4.1 and above devices

Part	Description
IpAddress	Multicast group Address (Class D) that members can join. A group address can be the same for many incoming ports.
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.
IfIndex	A unique value that identifies a physical interface or a logical interface (VLAN) that receives Group reports from various sources.
Expiration	Time left before the group report expires on this port. The system updates this variable after receiving a group report.

Cache tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000, ERS 1424/16xx, and VOSS (VSP82XX, VSP84XX, VSP 72XX) v4.1 and later 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 above, ERS 1424/16xx devices, and VOSS (VSP82XX, VSP84XX, VSP 72XX) v4.1 and later .

Table 19: IGMP and IGMP Snoop Devices folder Cache tab for ERS 8600/8800, VSP 7000, VSP 9000, VSP 4000, ERS 1424/16xx devices, and VOSS (VSP82XX, VSP84XX, VSP 72XX) v4.1 and later

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.
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.
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.
ExtnType	

Senders tab for ERS 8600/8800, VSP 9000, VSP 4000, ERS 8300, and VOSS (VSP82XX, VSP84XX, VSP 72XX) v4.1 and above

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, ERS 8300, and VOSS (VSP82XX, VSP84XX, VSP 72XX) v4.1 and above

Table 20: Parts of the IGMP and IGMP Snoop Devices folder Senders tab for ERS 8600/8800, VSP 9000, VSP 4000 v3.1 and up, ERS 8300, and VOSS (VSP82XX, VSP84XX, VSP 72XX) v4.1 and above

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

Table continues...

Part	Description
	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.

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 21: 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 rclgmpNewGroupExpiration.
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

Table continues...

Part	Description
	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.

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 22: 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 source expires.

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.

IGAP tab

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

Table 23: 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.

IGAP Groups

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

Table 24: 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: <ul style="list-style-type: none"> • 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

IGAP Counters

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

Table 25: Parts of the IGAP Counters tab

Part	Details
IfIndex	The VLAN name that uniquely identifies the interface.
AuthSuccess	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.
RespTimeout	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.

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.

Snoop tab

The following table describes the parts of the Snoop tab from the **IGMP and IGMP Snoop > Snoop** folder.

Table 26: Parts of the Snoop folder, Snoop tab

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.
ProxySnoopEnable For BayStack devices, the attribute name is SnoopReportProxyEnable.	Indicates if the IGMP report proxy feature is enabled. If this feature is enabled, reports are forwarded from hosts to the multicast router once

Table continues...

Part	Description
	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.
SsmEnable	Enables SSM feature.
SnoopMRouterPorts For BayStack devices, the attribute name is SnoopQuerierPort.	The port on which the multicast querier router is heard.
SnoopActiveMRouterPorts For BayStack devices, the attribute name is SnoopActiveQuerier.	The IP address of a multicast querier router.
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.

IGMP Snoop Trace tab

The following table describes the parts of the IGMP Snoop Trace tab from the IGMP and IGMP Snoop > Snoop folder.

Parts of the IGMP Snoop Trace tab

Part	Description
GrpAddr	The IP multicast address of the group.
SrcAddr	The Source Subnet IP address of the multicast group address.
OutVlan	The egress vlan id of the multicast group.
InPort	The Ingress port of the multicast group.
InVlan	The Ingress vlan id of the multicast source.
OutPort	The egress vlan id for the multicast source.

IGMP Snoop Router Ports folder

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

Table 27: 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

Part	Description
	<p>router so the multicast data and group reports are forwarded to the router.</p> <p>! Important:</p> <p>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.</p>

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.

Stream Limit tab

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

Table 28: Parts of the Stream Limit tab

Part	Details
IfIndex	The slot and port number or the VLAN ID for the interface.
StreamLimitEnable	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.

Stream Limit Members tab

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

Table 29: 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.

Table continues...

Part	Details
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.
NumStreams	The current number of streams received on this interface. This is a read-only value.

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. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select **IGMP and IGMP Snoop > Stream Limit**.
3. Click **Add Devices**.
4. From the Add Devices list, choose one or more devices.
5. Click **Save**.

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. The system 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.

SSM Global tab

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

Table 30: 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: <ul style="list-style-type: none"> • 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.

Table continues...

Part	Details
	<ul style="list-style-type: none"> • 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.

SSM Channel tab

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

Table 31: Parts of the IGMP and IGMP Snoop SSM Channel tab

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

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. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select **IGMP and IGMP Snoop > SSM** .
3. From the Multicast toolbar, click **Add Devices**.
4. From the Add Devices list, choose one or more devices.
5. Click **Save**.

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 32: 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.

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 33: 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.
DiscoveredRouterPorts	Lists ports discovered by IGMP Multicast Router Discovery (MRDISC) Protocol.
MaxAdvertiseInterval	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.
MinAdvertiseInterval	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.
MaxInitialAdvertiseInterval	Sets the maximum number, in seconds, of multicast advertisement intervals that you can configure on the switch.
MaxInitialAdvertments	Used to set the maximum number of initial multicast advertisements that you can configure on the switch.
NeighborDeadInterval	The time interval, in seconds, before the router interface drops traffic after you leave the multicast group.

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.

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 34: 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.

Adding a device to IGMP static members folder

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

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select **IGMP and IGMP Snoop > Access list > Static Members**.
3. From the Multicast toolbar, click **Add Devices**.
4. From the Add Devices list, choose one or more devices.
5. Click **Save**.

Inserting a device in the IGMP Static list

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

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select a device under **IGMP and IGMP Snoop > Access List > Static Members**.
3. From the Multicast content pane, click **Add Entry with Form**.
4. 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
5. Click **Save**.
 6. Click **Apply Changes**.

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.

Adding a device to IGMP Group access folder

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

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select **IGMP and IGMP Snoop > Access List > Group Access**.
3. From the Multicast toolbar, click **Add Devices**.
4. From the Add Devices list, choose one or more devices.
5. Click **Save**.

Inserting a device in the Group access list

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

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select a device under **IGMP and IGMP Snoop > Access List > Group Access**.
3. From the Multicast toolbar, click **Add Entry with Form**.
4. 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.
5. Click **Save**.
 6. Click **Apply Changes**.

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 35: 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: <ul style="list-style-type: none"> • Denied IP multicast transmitted traffic. The value is denyTX. • 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.

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.

Table continues...

Part	Description
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: <ul style="list-style-type: none"> denyTx—deny transmit mode denyRx—deny receive mode denyBoth—deny transmit and receive mode

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 36: 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.

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 37: Parts of the DVMRP Globals folder

Part	Description
Devices	The IP address of the device.

Table continues...

Part	Description
SysName	Identifies the 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	Triggerred 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.
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.

DVMRP Interfaces folder

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

Interfaces tab

The following table describes the parts of the Interfaces tab.

Table 38: Parts of the DVMRP Interfaces tab

Part	Description
Interface	DVMRP interface, slot and port number or VLAN identification.
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.
OperState	Current operational state of the DVMRP interface (up or down).

Interfaces Advance tab

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

Table 39: Parts of the DVMRP Interfaces Advance tab

Part	Description
Interface	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.
InPolicyName	Selects the name of the DVMRP accept policy applied to the interface.
OutPolicyName	Selects the name of the DVMRP announce policy applied to the interface.
AdvSelf	Sets the interface to advertise (true) or not advertise (false) its local route to neighbors. The default value is True.
DefRtLis	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.
DefRtSup	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.

Table continues...

Part	Description
DefRtMet	Sets the metric, which is the number of hops for DVMRP, of the default route. The range is from 1 to 31 hops.
InterfaceType	Sets the interface type as passive or active.

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 40: 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.

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 41: 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.
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.

Table continues...

Part	Description
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.

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 42: 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: <ul style="list-style-type: none"> • 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. • The mtrace bit (3) indicates that the neighbor can handle mtrace requests.
State	State of neighbor adjacency. The states are: <ul style="list-style-type: none"> • oneway—The switch recognizes a packet from the neighbor but no adjacency is established.

Table continues...

Part	Description
	<ul style="list-style-type: none"> • active—Adjacency exists in both directions. • ignoring—The switch ignores neighbor packets. • down—The interface is not enabled.

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 43: 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: <ul style="list-style-type: none"> • 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.

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 44: 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.

Table continues...

Part	Description
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.

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 45: 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.
Bootstrap Switches folder	Displays all configured BootStrap switches.

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 46: Parts of the PIM SM Globals folder

Part	Description
Devices	The IP address of the device.
SysName	Identifies the system name or host name of the device.
Enable	Indicates whether PIM-SM is enabled or disabled.

Table continues...

Part	Description
Mode	The configured mode of this interface. Sparse is the only valid entry.
JoinPruneInterval	Enables or disables the time interval setting.
pimJoinPruneInterval	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.
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.
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.
FastJoinPrune	Pim Fast Join Prune.
StaticRP	Indicates whether the static RP feature is enabled or disabled.

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.

Interfaces tab

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

Table 47: Parameters available under the Interfaces tab

Part	Description
Interface	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.
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.
InterfaceType	Indicates if the selected interface is active or passive: <ul style="list-style-type: none"> • 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.
Enable	Enables or disables PIM on the Interface.
InterfaceOperState	Indicates the status of PIM on the interface. The values are enabled or disabled.

Clip Interfaces tab

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

Table 48: 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.
PimMode	The configured mode of the interface. The valid modes are dense, sparse, sparseDense, and SSM.

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 49: 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.
Address	The IP address of the Candidate RP. The interface address must be one of the local PIM-SM enabled interfaces.

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. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select **Multicast Manager > PIM_SM > Candidate RPs**.
3. From the Multicast toolbar, click **Add Devices**.
4. From the Add Devices list, choose one or more devices.
5. Click **Save**.

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. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select a device under **Multicast Manager > PIM_SM > Candidate RPs**.
3. From the Multicast toolbar, click **Add Entry with Form**.
4. Enter the following properties:
 - Group Address
 - Group Mask
 - Address
5. Click **Save**.
6. Click **Apply Changes**.

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 50: 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.
Address	The IP address of the Static RP. This address has to be one of the local PIM-SM enabled interfaces.
Status	The static RP nodes configuration status.

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. Select **Configuration > Multicast**.
2. From the Multicast tree, select **Multicast Manager > PIM_SM > Static RPs**.

3. From the Multicast toolbar, click **Add Devices**.
4. From the Add Devices list, choose one or more devices.
5. Click **Save**.

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

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 51: 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.

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 52: 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.

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 53: 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

Table continues...

Part	Description
	transmitted by this device. The default value is 100 (1 second).
ExpiryTime	Amount of time, in seconds, remaining before the entry is aged out.

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 54: Parts of the MSDP Protocol folder

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

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 55: Parts of the MSDP Globals folder

Part	Description
Devices	The IP address of the device.
SysName	Identifies the 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.

MSDP Peers folder

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

Table 56: 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

Table continues...

Part	Description
	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, 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, it is recommended to configure PeerHoldTimeConfigured on the other side of the peer relationship as 0.

Adding a device to the MSDP Peers folder

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

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select **Multicast Manager > MSDP > Peers**.
3. From the Multicast toolbar, click **Add Devices**.
4. From the Add Devices list, choose one or more devices.

5. Click **Save**.

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 57: Parts of the MSDP Mesh Group table

Part	Description
Name	Name of the Mesh Group.
PeerAddress	IP address of the MSDP peer.
Status	Mesh Group configuration status.

Adding a device to the MSDP Mesh Group

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

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select **Multicast Manager > MSDP > Mesh Group**.
3. From the Multicast toolbar, click **Add Devices**.
4. From the Add Devices list, choose one or more devices.
5. Click **Save**.

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 58: Parts of the MSDP Cache table

Part	Description
GroupAddr	The group address of the SA Cache entry.
SourceAddr	The source address of the SA Cache entry.
OriginRP	The address of the RP which originated the last SA message accepted for the entry.
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 continues...

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

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 59: 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.

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 60: 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.

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 61: Parts of the Multicast Route Timed Prune folder

Part	Description
GroupAddress	Indicates the IP Multicast Group Address associated with the IP multicast stream.
SourceAddress	The Source Subnet IP address of the sender of the IP multicast stream.
SrcSubnetMask	The Source Subnet Mask IP address of the sender of the IP multicast stream.
AgingTimer	Indicates the amount of time (in minutes) the timed prune entry is displayed in the forwarding table when there are no more receivers. Once the timer expires, the timed prune entry is treated as a normal DVMRP/PIM forwarding entry. AgingTimer value of 0 (infinite time) indicates that the timed prune entry is not deleted even if there are no more receivers.

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. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select **Multicast Manager > Multicast Route > Timed Prune**.
3. From the Multicast toolbar, click **Add Devices**.
4. From the Add Devices list, choose one or more devices.

5. Click **Save**.

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. Select **Configuration > Multicast**.
2. From the Multicast navigation tree, select **Multicast Manager > Multicast Route > Timed Prune**, and then select a device.
3. From the Multicast Content Panel toolbar, click **Add Entry with Form**.
4. Enter the following properties:
 - GroupAddress
 - SourceAddress
 - SrcSubnetMask
5. Click **Save**.

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 62: Part of the Multicast Route Routes folder

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

MRoute Routes tab

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

The following table describes the parts of the MRoute Routes tab.

Table 63: Parts of the Multicast Route Routes folder MRoute Routes tab

Parts	Description
InIfIndex	A unique identifying number associated with an interface.
UpstreamNeighbor	The address of the upstream neighbor, for example RPF neighbor, from which IP datagrams from these

Table continues...

Parts	Description
	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.
Interface	The slot and port number or VLAN ID on which IP datagrams sent by these sources to this multicast address are received.
Source	The network address which, if combined with the corresponding route SourceMask value, identifies the sources for which the entry contains multicast routing information.
SourceMask	The network mask which, if combined with the corresponding route Source value, identifies the sources for which this entry contains multicast routing information.
ExpiryTime	

MRoute Next Hops tab

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

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

Table 64: Parts of the Multicast Route Routes folder MRoute Next Hops tab

Part	Description
State	Indicates if the outgoing interface and next hop represented by this entry is currently being used to forward IP datagrams. The values are: <ul style="list-style-type: none"> forwarding—indicates it is currently being used. pruned—indicates it is not being used.
ExpiryTime	The minimum amount of time remaining before the entry ages out. The value 0 indicates that the entry is not subject to aging.
ClosestMemberHops	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.
Interface	The slot and port number or VLAN ID for the outgoing interface for this next hop.
Group	The IP multicast group for which the entry specifies a next hop on an outgoing interface.

Table continues...

Part	Description
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.
SourceMask	The network mask which, if combined with the corresponding next hop Source value, identifies the source for which the entry specifies a next hop on an outgoing interface.
IfIndex	A unique identifying number associated with an interface.
Address	The IP address of the VLAN for the next hop.

MRoute Interfaces tab

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

Table 65: Parts of the Multicast Route Routes folder MRoute 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.

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 66: 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.

Table continues...

Parts	Description
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.

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 214, and [Policy Route table](#) on page 215.

Prefix List

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

Table 67: 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

Table continues...

Part	Details
	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.

Route Policy table

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

Table 68: Parts of the Route Policy 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.

Table continues...

Part	Details
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 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 1 to 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.

Table continues...

Part	Details
Set CommunityMode	<p>The values are:</p> <ul style="list-style-type: none"> • 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. <p>The default value is Unchanged. Applies to the BGP protocol only.</p>
SetMetricTypeInternal	<p>Sets the MED value for routes advertised to BGP numbers to the Interior Gateway Protocol (IGP) metric value. The default is 0.</p>
SetMetric	<p>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 RIP, the original cost of the route or the default value is used.</p>
SetMetricType	<p>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.</p>
SetNextHop	<p>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.</p>
SetOrigin	<p>The values are:</p> <ul style="list-style-type: none"> • IGP • EGP • incomplete • unchanged <p>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.</p>
SetLocalPref	<p>Use during the route decision process in the BGP protocol. The default is 0. Applies to the BGP protocol only.</p>
SetOriginEgpAs	<p>Indicates the remote autonomous systems number. The default is 0. Applies to the BGP protocol only.</p>

Table continues...

Part	Details
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 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.

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. Select **Configuration > Multicast**.
2. From the Multicast navigation pane, select **Multicast Manager > Policy > Device List**.
3. From the Multicast tool bar, click **Add Devices**.

The Add Devices dialog box appears that lists the devices discovered by Multicast Manager.

4. Select one or more devices from the list of devices, and then click **Save**.

Deleting a device from the Policy folder

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

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation pane, select **Multicast Manager > Policy > Device List**.

3. Select the device.
4. From the Multicast tool bar, select **Remove Device**.

Adding a Prefix

Perform the following procedure to add a prefix.

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation pane, select **Multicast Manager > Policy > 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**.
6. Complete the fields as appropriate, and click **Save**.

Deleting a prefix

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

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation pane, select **Multicast Manager > Policy > 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**.

Adding a Route Policy

Perform the following procedure to add a Route Policy.

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation pane, select **Multicast Manager > Policy > 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**.
6. Complete the fields as appropriate, and click **Save**.

Deleting a Route Policy

Perform the following procedure to delete a Route Policy from the policy folder.

Procedure

1. Select **Configuration > Multicast**.
2. From the Multicast navigation pane, select **Multicast Manager > Policy > 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**.

Highlight multicast data in the topology map

You can highlight the following information in the topology:

- Multicast device
- Multicast forwarding tree

Highlighting a multicast device in the topology map

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

Procedure

1. Select **Configuration > Multicast**.
2. In the Multicast 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.

3. From Multicast menu bar, select **Highlight on Topology**.
4. The system displays the topology on the Network Map.
 - 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.

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. Select **Configuration > Multicast**.
2. In the Multicast navigation pane, select **Multicast Manager > DVMRP > Dvmrp RPB Trees** or **Multicast Manager > Multicast Route > MRoute RPM Trees**.
3. From the Multicast menu bar, select **Highlight on Topology**.
4. The system displays the topology on the Network Map.

The devices and forwarding paths are highlighted.

Highlighting a multicast forwarding tree using multicast protocol features

You can select a multicast protocol feature in the Multicast view, and on the Network Map, the devices that are actively using the multicast protocol feature are highlighted.

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

Procedure

1. Select **Configuration > Multicast**.
2. In the Multicast navigation pane, select a multicast protocol feature icon from the folders and subfolders of the navigation tree.
3. From the Multicast menu bar, select **Highlight on Topology**.
4. The system displays the topology on the Network Map.

The devices you selected that use the multicast protocol feature are highlighted.

Chapter 13: Managing Fabric Connect

About Fabric Connect

The Fabric Connect view enables 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 Fabric Connect view, you can view and configure these features on multiple devices that have SPBm enabled. L2 VSNs can be based on C-Vlans, Switched UNI Vlans, Transparent UNI (T-UNI), or Flex UNI. You can configure Multicast-over-SPBm for L2, L3, and IP-shortcuts based VSNs.

*** Note:**

Switched UNI Vlans can be configured for VSP 7000 v10.2 and later, and ERS 4800 v5.7 and later devices only.

The following table outlines the supported devices for Fabric Connect:

Supported device for Fabric Connect	Features supported
APLS 4.3.1 APLS 6.0 and later Includes the following hardware: DSG6248, DSG6248P, DSG6248CFP, DSG7648, DSG7648C, DSG7480, and DSG8032.	L2 VSN L2 MoSPBm L3 VSN L3 MoSPBm GRT-IP Shortcuts SPBm Multicast Tree Fabric Attach (supported only on versions 6.0 and later)
Ethernet Routing Switch 35xx 5.3.1, and later Includes the following hardware: ERS3550T, and ERS3550T-PWR+.	Fabric Attach
Ethernet Routing Switch 45xx 5.7.3	Fabric Attach
Ethernet Routing Switch 48xx 5.2, 5.3, 5.4, 5.5, 5.6, 5.6.1, 5.6.2, 5.7, and 5.7.2 Ethernet Routing Switch 48xx 5.7.3 and later	L2 VSN L2 MoSPBm GRT-IP Shortcuts SPBm Multicast Tree

Table continues...

Supported device for Fabric Connect	Features supported
	Fabric Attach (supported only on versions 5.7.3 and later)
Ethernet Routing Switch 49xx 7.1, and 7.2 Includes the following hardware: ERS4950GTS, ERS4950GTS-PWR+, ERS4926GTS, ERS4926GTS-PWR.	L2 VSN L2 MoSPBm L3 VSN L3 MoSPBm GRT-IP Shortcuts SPBm Multicast Tree Fabric Attach
Ethernet Routing Switch 55xx 6.6.1 and later	Fabric Attach
Ethernet Routing Switch 56xx 6.6.1, and later	Fabric Attach
Ethernet Routing Switch 59xx 7.0, 7.0.1, 7.1, and 7.2 Includes the following hardware: ERS5928GTS-uPWR, ERS59100GTS, and ERS59100GTS-PWR +.	L2 VSN L2 MoSPBm L3 VSN 3 MoSPBm GRT-IP Shortcuts SPBm Multicast Tree Fabric Attach
ERS 8600/8800 7.1 and 7.1.3 ERS 8600/8800 7.2 and later Includes the following hardware: 8681XLW module, 8681XLR module, 8616GTE module, 8672ATME MDA, 8608GBM module, 8608GTM module, 8632TXM module, 8648TXM module, 8672ATMM module, and 8683POSM module.	L2 VSN L2 MoSPBm (supported only on versions 7.2 and later) L3 VSN L3 MoSPBm (supported only on versions 7.2 and later) GRT-IP Shortcuts (supported only on versions 7.2 and later) BGP-VPN SPBm Multicast Tree (supported only on versions 7.2 and later)
VSP 4000 3.0, and 3.0.1 VSP 4000 3.1 and later	L2 VSN L2 MoSPBm (supported only on versions 3.1 and later) L3 VSN (supported only on versions 3.1 and later) L3 MoSPBm (supported only on versions 3.1 and later)

Table continues...

Supported device for Fabric Connect	Features supported
	GRT-IP Shortcuts (supported only on versions 3.1 and later) SPBm Multicast Tree (supported only on versions 3.1 and later) Fabric Attach (supported only on versions 5.0 and later)
VSP 7000 10.1, 10.2, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.4, and ¹	L2 VSN Fabric Attach (supported only on versions 10.4 and later)
VSP 7200 4.2.1, 4.2.2, 4.2.3, 5.0, 5.1, 5.1.1 Includes the following hardware: Port-Licensed 7200 models.	L2 VSN L2 MoSPBm L3 VSN L3 MoSPBm GRT-IP Shortcuts SPBm Multicast Tree Fabric Attach (supported only on versions 5.0 and later)
VSP 8000 4.0, and 4.0.1.1 VSP 8000 4.1, and later	L2 VSN L2 MoSPBm (supported only on versions 4.1 and later) L3 VSN (supported only on versions 4.1 and later) L3 MoSPBm (supported only on versions 4.1 and later) GRT-IP Shortcuts (supported only on versions 4.1 and later) SPBm Multicast Tree (supported only on versions 4.1 and later)
VSP 9000 3.2 and 3.3 VSP 9000 3.4, and later	L2 VSN (supported only on versions 3.4 and later) L2 MoSPBm L3 VSN (supported only on versions 3.4 and later) L3 MoSPBm BGP-VPN (supported only on versions 3.4 and later) GRT-IP Shortcuts SPBm Multicast Tree

¹ — SPB Infrastructure and L2 SPB Service support only.

Launching the Fabric Connect view

Perform the following procedure to launch the Fabric Connect view.

Procedure steps

1. From the menu bar, select **Configuration > Fabric Connect**.

Fabric Connect view performs a discovery. After the discovery is complete, the Operation Completed dialog box displays.

2. In the **Operation Completed** dialog box, click **Ok**.

Fabric Connect navigation pane toolbar options

The following table lists and describes the Fabric Connect toolbar options.

Table 69: Fabric Connect toolbar options

Option	Description
Context	Use this option to select the available groups assigned to the current logged in user. After you change the context, a notification is sent to all opened configuration views in the system with the same logged in user. All opened views are refreshed after receiving this notification.
Save Context	Use this option to save the context.
Revert to Current Context	Use this option to revert to the current context.
Refresh Groups	Use this option to view the new groups added to the current logged in user.
Discover Fabric Network Configurations	Use this option to discover the configuration of the Fabric Network.
Toggle Device/Fabric centric view	Use this option to toggle between Device-centric and Fabric-centric views.
Preferences	Use this option to configure Fabric Connect preferences.
Show/Re-draw Fabric Topology	Use this option to view or re-draw Fabric topology.
Help	Use this option to view online help.

Fabric Connect view

After you launch the Fabric Connect view, the system discovers the following tables:

- SPBm Globals
- Virtualized Networks
- SPBm Multicast Routes
- CFM Globals

- Fabric Attach Globals

All related tables are saved in the Fabric Connect view. After the system populates the User Interface (UI) with the discovered information, you can view or modify the configuration of the Fabric Connect.

There are two Fabric Connect views: Fabric-centric, and device-centric. The following sections describe each view.

Fabric-centric view

The default view of the Fabric Connect is the Fabric-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 Fabric-centric view contains the following :

- SPBm Globals (Global SPBm configuration data)
- Virtualized Networks
- SPBm Multicast Route tables
- CFM Global configuration
- Fabric Attach (Fabric Attach global configuration)

Various Fabric-centric features are described in detail in subsequent sections of the document.

The following figure shows the Fabric-centric view.

SysName	IPAddress	ServiceName	I-SID	UNIType
V4K-VOSS-VISTB-2	10.139.123.10		1	C-VLAN UNI
VSP-8k-R1-BEB-7	10.139.123.167		1	C-VLAN UNI
VSP-8k-R1-BEB-8	10.139.123.168		1	C-VLAN UNI
V4K-APLS-VISTB-1	10.139.123.9		1	C-VLAN UNI
VSP-4K-R1-BEB-5-HighTemp	10.139.123.186		2	C-VLAN UNI
VSP-8k-R1-BEB-7	10.139.123.167		3	C-VLAN UNI
VSP-8k-R1-BEB-8	10.139.123.168		3	C-VLAN UNI
VSK4k-Bandaru	10.177.220.164		3	C-VLAN UNI, Flex UNI

4818 Rows

Figure 10: Fabric-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 Fabric Centric View.

The following graphic shows the SPBm Globals table.

Device SysName	Device IP	Node Nickname	Primary B-Vlan	B-Vlans
BLR-VSP44xx	10.133.139.85	00:00:85	64	64,128
BLR-VSP70xx	10.133.139.102	00:11:02	64	64,128
VSP-4850GTS	10.133.139.81	00:01:81	64	64,128
VSP-7254XTQ	10.133.139.127	00:01:27	64	64,128
VSP-4850GTS	10.133.139.80	00:01:80	64	64,128
VSP-8284XSQ_B...	10.177.216.21	09:10:07	64	64,128
VSP-8404_BEB	10.177.216.20	09:10:06	64	64,128
	10.177.216.30	00:00:00	0	
VSP-7254XTQ_B...	10.177.216.24	09:10:08	64	64,128

Figure 11: SPBm Globals table

Device centric view

The default view on the Fabric Connect is the Fabric-centric view. To change the view to a device centric view, click **Toggle Device/Fabric centric view** on the Fabric Connect toolbar.

After you change the view to the device centric view, the system restores the node that you selected during the view change. The hierarchy that appears in the Fabric-centric view exists in the device centric view; however in the device centric view, the hierarchy appears under each single device. Additional components exist under each device that you can view and configure, if required.

The following sections describe components of the device centric view.

Device node

After you select the required device node from the device centric view of the Fabric Connect, the system displays the following device information in the contents pane depending on which type of device you select

For C_VLAN UNI VSN devices:

- IP Address
- SysName
- ServiceName
- ISID
- VRFName
- VLAN ID
- IP Interface
- MoSPBm
- IGMP Version

Managing Fabric Connect

- Snoop Querier

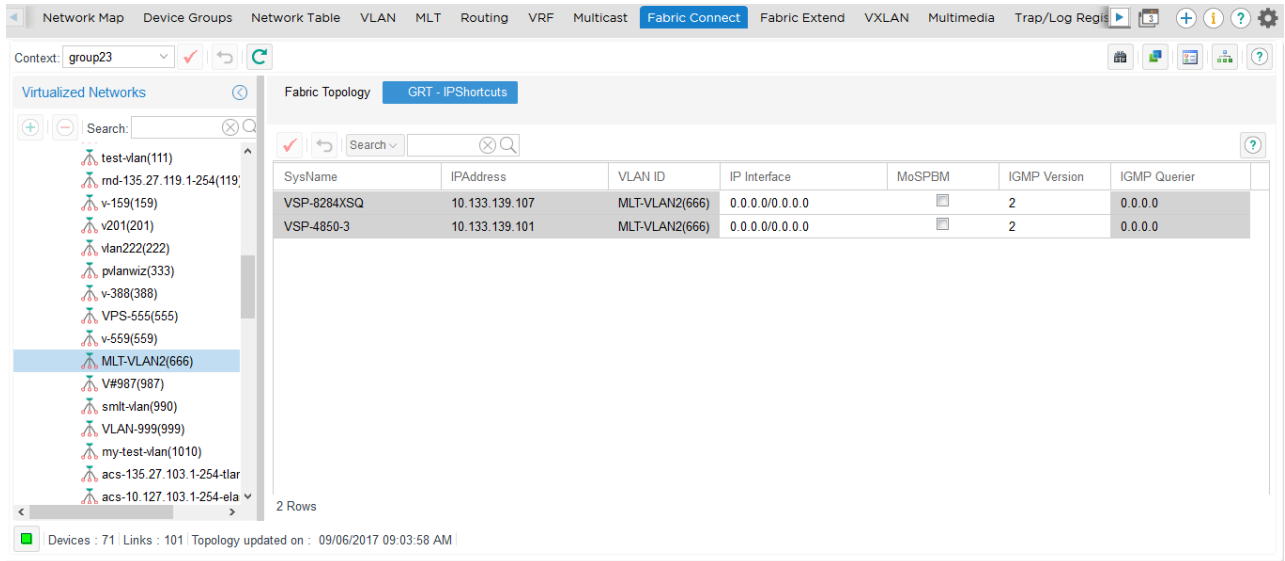
For Transparent UNI VSN devices:

- IP Address
- SysName
- ServiceName
- ISID
- PortMembers
- MLT IDs

For Flex UNI VSN devices:

- IP Address
- Sys Name
- ServiceName
- ISID
- MAC LIMIT Enable
- MAX MAC LIMIT
- Origin

The following figure is an example of the Device-centric view in Fabric Connect.



The screenshot shows the Fabric Connect interface with the following data in the table:

SysName	IP Address	VLAN ID	IP Interface	MoSPBM	IGMP Version	IGMP Querier
VSP-8284XSQ	10.133.139.107	MLT-VLAN2(666)	0.0.0.0/0.0.0.0	<input type="checkbox"/>	2	0.0.0.0
VSP-4850-3	10.133.139.101	MLT-VLAN2(666)	0.0.0.0/0.0.0.0	<input type="checkbox"/>	2	0.0.0.0

Figure 12: 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:

- IP Address
- System Name
- Service Name
- I-SID
- VRF Name
- VLAN
- IP Interface
- Port Members

The following sections describe the options under the is-is node.

Interfaces

The Interfaces node exists under the is-is node and displays the ISIS interfaces configured on the device

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.

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 the 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 CFM Globals 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 the CFM Globals table.

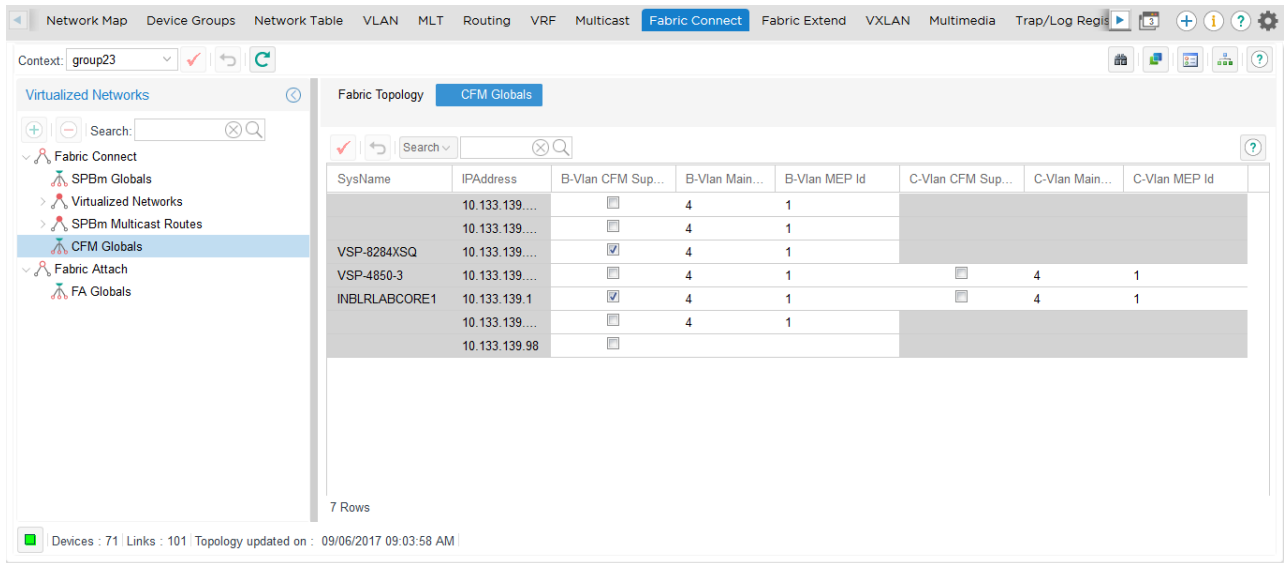


Figure 13: CFM Globals table

The following table describes the CFM Globals table.

Field	Description
IPAddress	The corresponding IP address of the device.
SysName	The corresponding system name of the device.
B-Vlan CFM Support	Use to enable or disable global CFM support for SPBM VLANs.
B-Vlan Maint Level	Use to configure the global CFM Maintenance level for SPBM VLANs.
B-Vlan MEP Id	Use to configure the global CFM Maintenance End Point ID value for SPBM VLANs.
C-Vlan CFM Support	Use to enable or disable global CFM support for C-VLANs.
C-Vlan Maint Level	Use to configure the global CFM Maintenance level for C-VLANs.
C-Vlan MEP Id	Use to configure the global CFM Maintenance End Point ID value for C-VLANs.

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.

VLAN Name	MEP Nodal	MIP Nodal
SPBM-Primary	spbm.64.4	4
SPBM-Secondary	spbm.128.4	4

Figure 14: 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.

VRF table

In the 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 Fabric Connect 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.

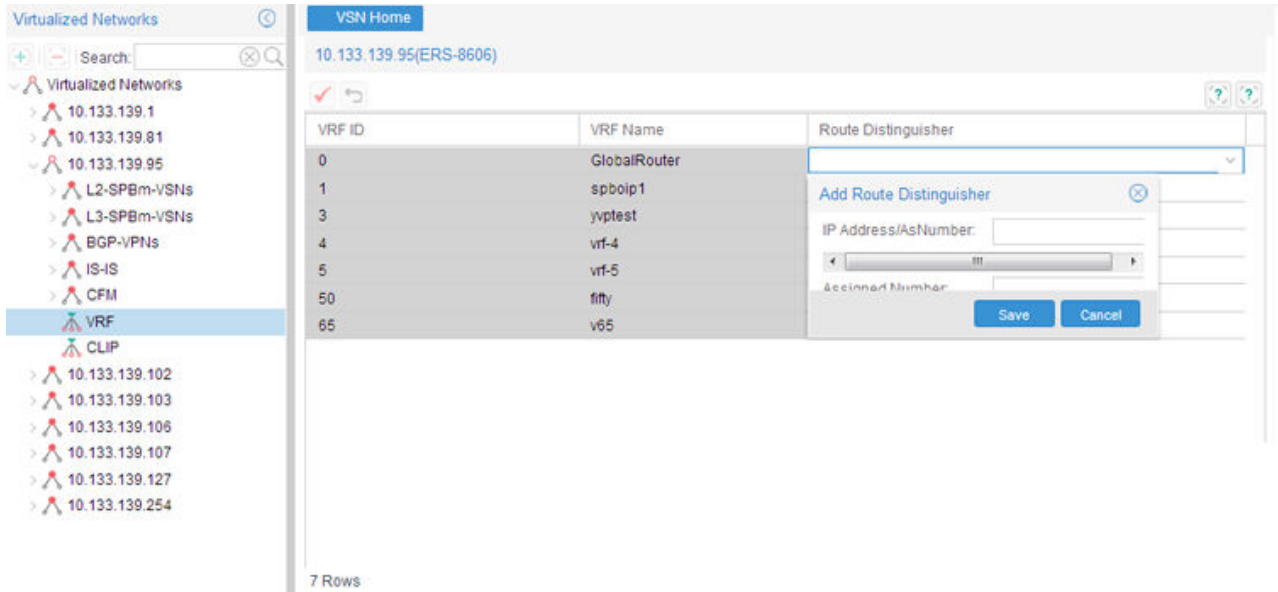


Figure 15: Add Route Distinguisher

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 Fabric Connect 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 toolbar.

The following figure is an example of the CLIP contents pane.

*** Note:**

The CLIP features is not supported for VSP 7000 v10.2.

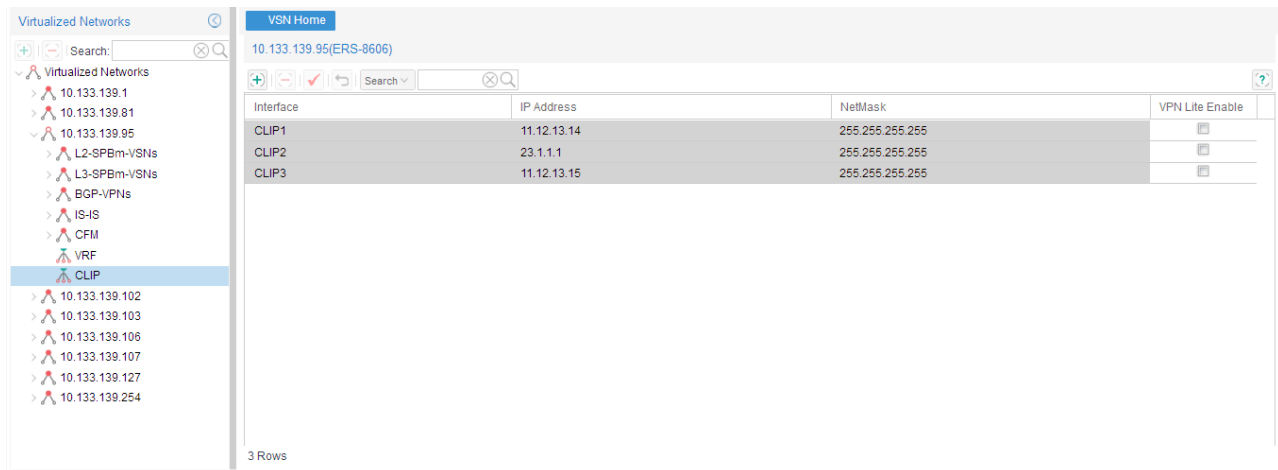
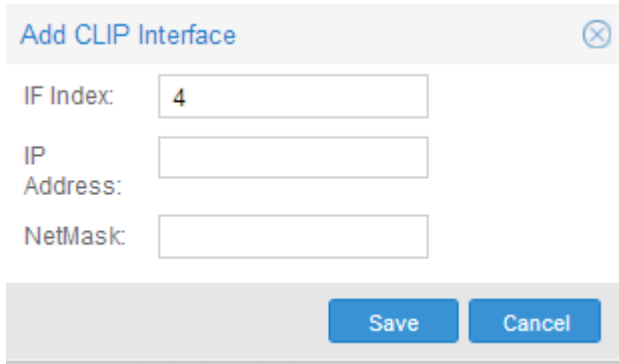


Figure 16: CLIP contents pane

The following figure is an example of the CLIP contents pane with the Add CLIP Interface dialog box.



The image shows a dialog box titled "Add CLIP Interface" with a close button (X) in the top right corner. It contains three input fields: "IF Index" with the value "4", "IP Address", and "NetMask". At the bottom, there are two buttons: "Save" and "Cancel".

Figure 17: Add CLIP Interface dialog box

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 no tag on the packets. Untagged ports cannot be used as trunk ports.
4. On trunk ports – traffic that originated from isolated ports is tagged with the secondary VLAN_ID.

- 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.

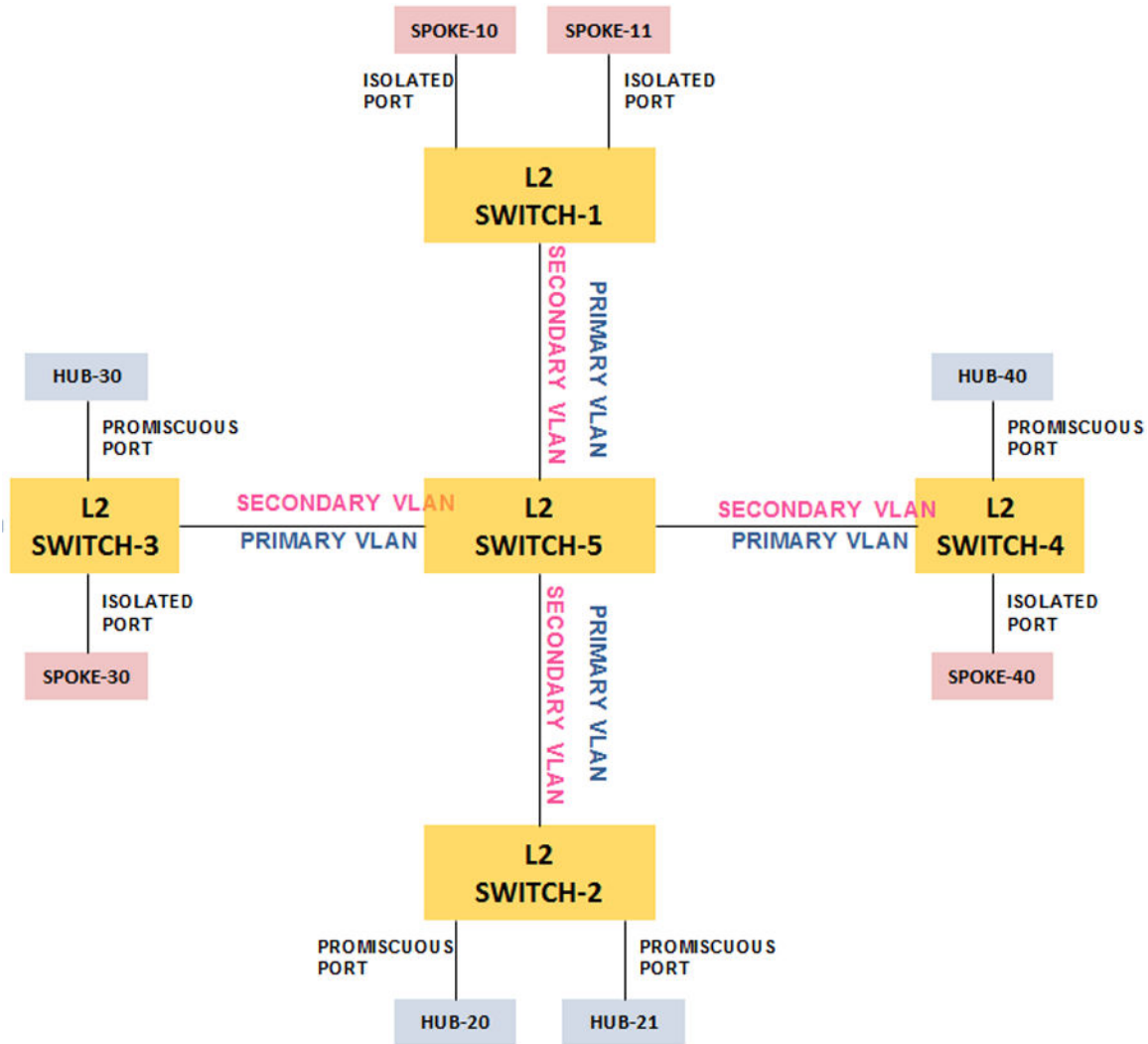


Figure 18: Private VLAN on five switches

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.

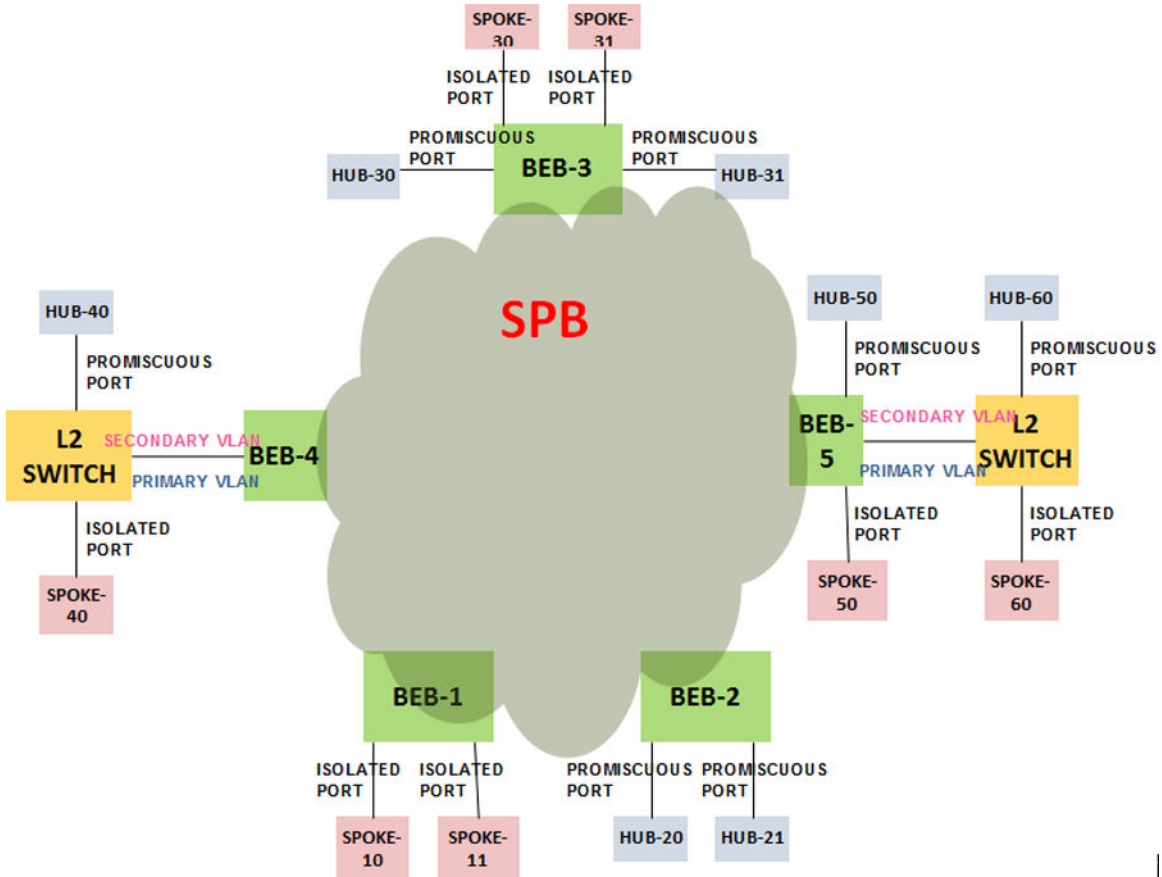


Figure 19: Etree reference model

An Etree instance is 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** table provides additional information about the associated private vlan.

IPAddress	SysName	Primary VLAN ID	Secondary VLAN ID	Primary/Secondary ISID	Promiscuous Ports	Isolated Ports	Trunk Ports
10.133.139.127	VSP-7254XTQ	VLAN-489(489)	498	10003	1/14	1/15	1/16

Figure 20: Etree Info table

Editing Global Routing Table — IP Shortcuts

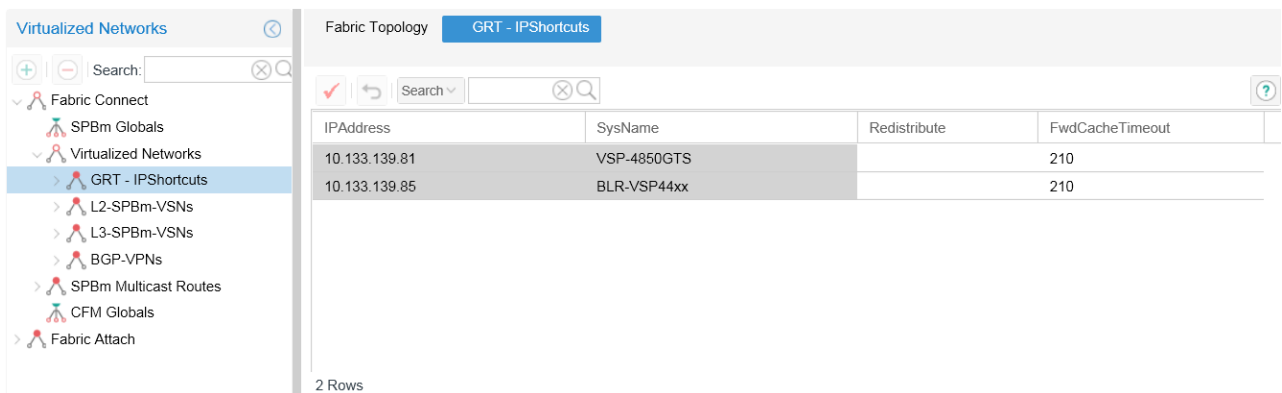
You can configure Global Routing Table (GRT) level attributes for IP Shortcuts and for IP Multicast over SPBm (MoSBBm).

After you select an GRT—IP Shortcuts from the Fabric-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 Fabric-centric view, information on that device displays in a table in the contents pane. In the table, you can modify the following information:

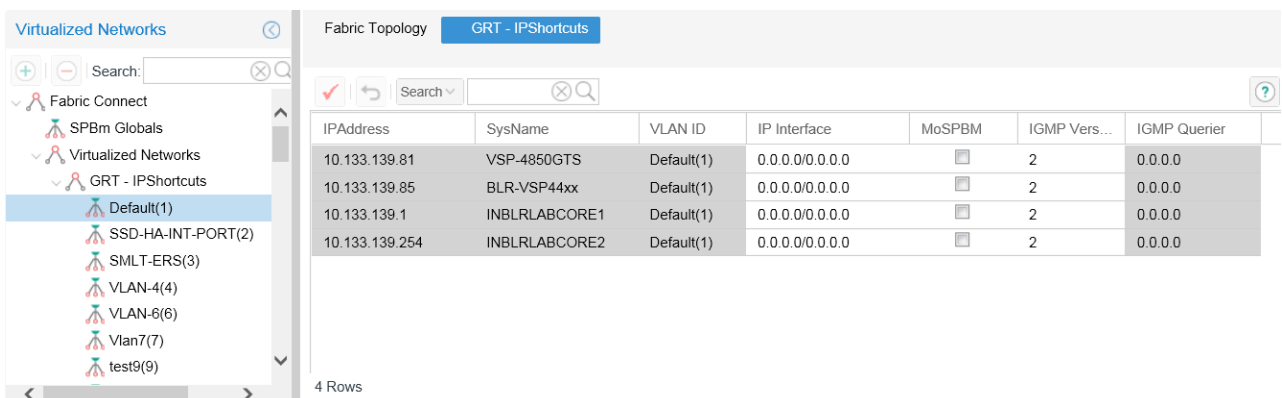
- IP Interface
- MoSPBm
- IGMP version



IPAddress	SysName	Redistribute	FwdCacheTimeout
10.133.139.81	VSP-4850GTS		210
10.133.139.85	BLR-VSP44xx		210

2 Rows

Figure 21: IPShortcuts — global



IPAddress	SysName	VLAN ID	IP Interface	MoSPBM	IGMP Vers...	IGMP Querier
10.133.139.81	VSP-4850GTS	Default(1)	0.0.0.0/0.0.0.0	<input type="checkbox"/>	2	0.0.0.0
10.133.139.85	BLR-VSP44xx	Default(1)	0.0.0.0/0.0.0.0	<input type="checkbox"/>	2	0.0.0.0
10.133.139.1	INBLRLABCORE1	Default(1)	0.0.0.0/0.0.0.0	<input type="checkbox"/>	2	0.0.0.0
10.133.139.254	INBLRLABCORE2	Default(1)	0.0.0.0/0.0.0.0	<input type="checkbox"/>	2	0.0.0.0

4 Rows

Figure 22: IPShortcuts — device

L2 SPBm functionality

Before you create Layer 2 Shortest Path Bridging MAC (SPBm) Fabric Connect on a device, you must configure Intermediate System to Intermediate System (IS-IS), SPBm, and other infrastructure features. The Fabric Connect view only permits you to configure the service configuration of the Layer 2 SPBm feature, which is the mapping of a customer VLAN to an ISID, an identifier for the Layer 2 SPBm.

SPBm and ISIS infrastructure configurations can be done using the Fabric Connect wizard. For information, refer to [Fabric wizard](#) on page 464.

The following figure shows the top level Layer 2 SPBm view.

SysName	IPAddress	ServiceName	I-SID	UNIType
V4K-VOSS-VISTB-2	10.139.123.10		1	C-VLAN UNI
VSP-8k-R1-BEB-7	10.139.123.167		1	C-VLAN UNI
VSP-8k-R1-BEB-8	10.139.123.168		1	C-VLAN UNI
V4K-APLS-VISTB-1	10.139.123.9		1	C-VLAN UNI
VSP-4K-R1-BEB-5-HighTemp	10.139.123.186		2	C-VLAN UNI
VSP-8k-R1-BEB-7	10.139.123.167		3	C-VLAN UNI
VSP-8k-R1-BEB-8	10.139.123.168		3	C-VLAN UNI
VSK4k-Bandaru	10.177.220.164		3	C-VLAN UNI, Flex UNI

Figure 23: Layer 2 SPBm VSNs

In the Layer 2 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 Fabric Connect view showing all the devices that belong to ISID-99.

IPAddress	SysName	ServiceName	I-SID	VRFN...	VLAN ID	IP Interface	MoSP...	IGMP...	Snoop Qu...
10.139.12...	V4K-VOS...		1	Global...	Defaul...	0.0.0.0/0.0.0.0	<input type="checkbox"/>	2	
10.139.12...	VSP-8k-R...		1	Global...	VLAN-...	1.1.1.1/255.255...	<input type="checkbox"/>	2	0.0.0.0
10.139.12...	VSP-8k-R...		1	Global...	VLAN-...	1.1.1.2/255.255...	<input type="checkbox"/>	2	0.0.0.0
10.139.12...	V4K-APL...		1	Global...	Defaul...	0.0.0.0/0.0.0.0	<input type="checkbox"/>	2	

Figure 24: Layer 2 SPBm VSN device view

In the preceding image, a customer VLAN is mapped to the ISID-11. 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 Fabric-centric view.

* Note:

The **Add** and **Delete** buttons are context-sensitive.

Procedure steps

1. From the menu bar, select **Configuration > Fabric Connect**.
2. In the navigation pane of the Fabric-centric view, select **Fabric Connect > Virtualized Networks > L2-SPBm-VSNs**.
3. From the toolbar, click **Add**.

The Add L2 ISID window displays.

4. Select UNI Type

5. 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.

6. 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.

7. Select the check box to use the ISID Service Name, then you can perform the following actions:
 - a. Select the Service Group.
 - b. Select the Service Name.
8. If you do not select to use the ISID Service Name, then enter the ISID number.

*** Note:**

If you selected C-VLAN UNI as the UNI Type, you can select the VLAN.

If you selected Switched UNI as the UNI Type, you can select VLAN and port members.

If you selected Transparent UNI as the UNI Type, you can select the option to allow ports/MLTs belonging to Vlans to be selected.

If you selected Flex UNI as the UNI Type, you can enter the C-VID, and allow ports/MLTs 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.

9. For the devices that remain unmodified, you can either select a different VLAN, or leave the devices unmodified.
10. Click **Save**.

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 Fabric-centric view.

*** Note:**

The **Add** and **Delete** buttons are context-sensitive.

Procedure steps

1. From the menu bar, select **Configuration > Fabric Connect**.
2. In the navigation pane of the Fabric-centric view, select **L2-SPBm-VSNs**, and then click on the required ISID.

- From the toolbar, click **Add**.

The Add L2 ISID page displays.

- Select UNI Type.

- 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.

- 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.

- For the devices that remain unmodified, you can either select a different VLAN, or leave the devices unmodified.

- Click **Save**.

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 Fabric-centric view.

*** Note:**

The **Add** and **Delete** buttons are context-sensitive.

Procedure steps

- From the menu bar, select **Configuration > Fabric Connect**.
- To delete the ISID for all the devices, in the Navigation pane of the Fabric-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 Fabric-centric view, select a VSN type, select an ISID, and then select a device.

- From the Fabric Connect 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 Fabric-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
- IP Interface
- MoSPBm
- 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 Fabric-centric view, information on that device displays in a table in the contents pane.

Flex UNI

The Flex UNI VSN table provides information about I-SID devices. You can configure MAC limit information, however, the shaded cells in the table are read-only.

- IP address
- System name
- Service name
- I-SID
- MAC LIMIT Enable
- MAX MAC LIMIT
- Origin

The following figure shows a Flex UNI VSN table for an ISID node.

The screenshot shows the Fabric Connect interface with the 'Flex UNI VSN' table selected. The table contains the following data:

SysName	IPAddress	ServiceName	I-SID	MAC LIMIT Enable	MAX MAC LI...	Origin
VSP-4850-3	10.133.139.101		990	<input type="checkbox"/>	32000	config
VSP-8284XSQ	10.133.139.107		990			config

At the bottom of the interface, it indicates '2 Rows' and 'Devices : 71 | Links : 101 | Topology updated on : 09/06/2017 09:03:58 AM'.

Figure 25: Flex UNI VSN table for an ISID node

You can also view the following Flex UNI VSN information about a device. This information is read-only.

- IP address
- System name
- Service name
- I-SID
- C-VID
- Port member
- MLT ID
- Origin

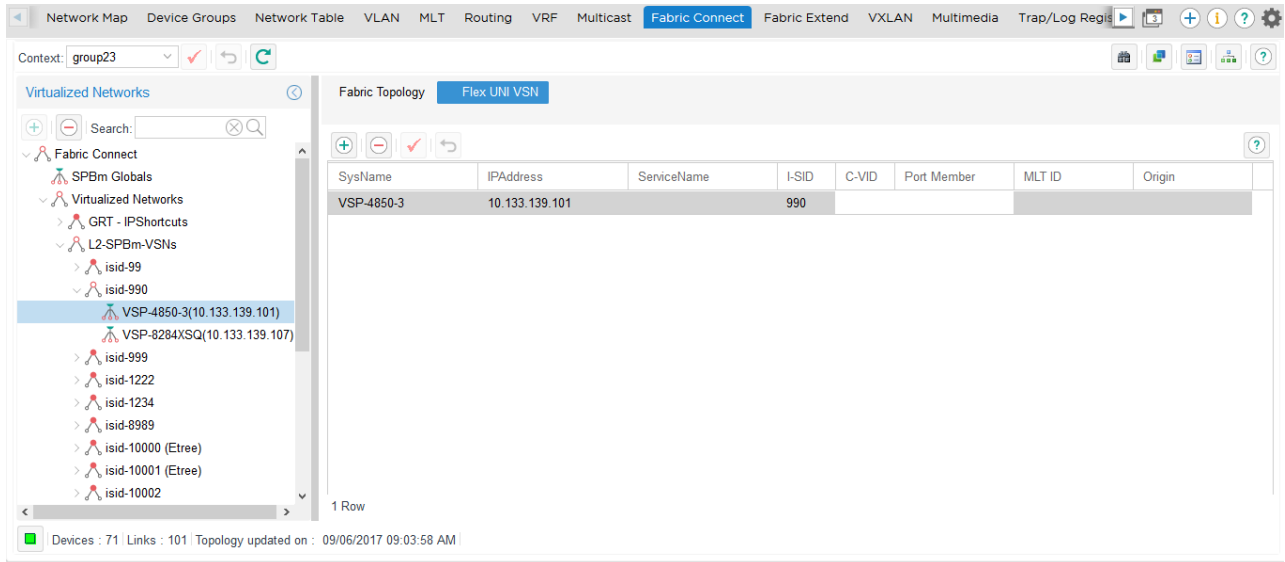


Figure 26: Flex UNI VSN table for a device

Adding a Flex UNI VSN

For information about adding a Flex UNI VSN, see [Adding an L2 ISID](#) on page 239.

Modifying the Flex UNI VSN table

Use this procedure to edit information in the Flex UNI VSN table.

About this task

You can configure the MAC LIMIT Enable and the MAX MAC LIMIT fields only. The shaded fields are read-only.

Before you begin

The L2–SPBm-VSN I-SID must have at least one Flex UNI VSN.

You must be in the Fabric-centric view.

Procedure

1. Select **Configuration > Fabric Connect**.
2. In the navigation pane, select **Fabric Connect > Virtualized Networks > L2–SPBm-VSNs**.
3. Expand **L2–SPBm-VSNs**, and select an isid node.
4. Select the **Flex UNI VSN** tab.
5. Configure the table values as required.
 - MAC LIMIT Enable — click on the check box to enable MAC limit.
 - MAX MAC LIMIT — double-click on a cell, and enter a value.
6. Click **Apply**.

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.

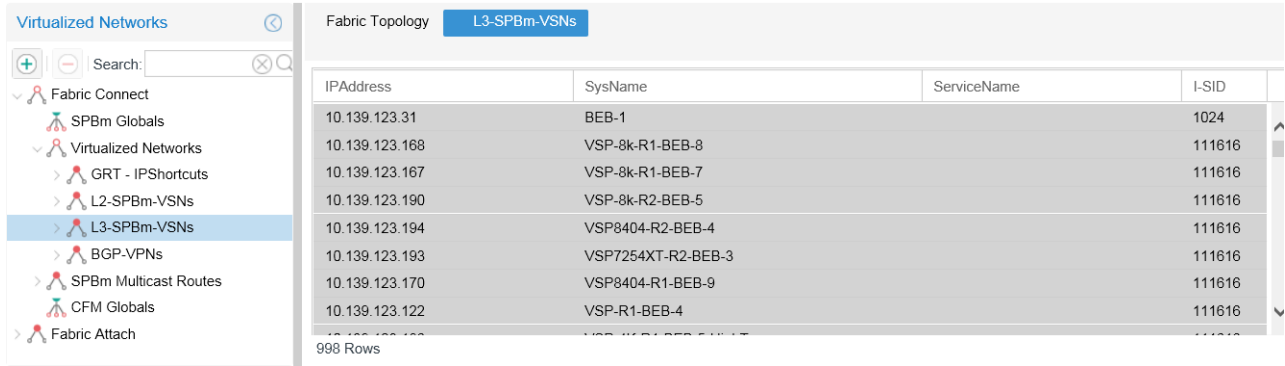


Figure 27: Layer 3 VSNs

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. From the menu bar, select **Configuration > Fabric Connect**.
2. In the navigation pane of the Fabric Connect, select **L3-SPBm-VSNs**.
3. From the Fabric Connect toolbar, click **Add**.

The Device Selection page appears.

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, Select a device, and click the left-pointing arrow.

5. Click **Select**.

After you have selected the required devices, the Configuration page appears.

6. Select the Service Group.
7. Select the Service Name.
8. Enter the ISID Number.
9. 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.

10. For the devices that remain unmodified, you can either select a VRF from the pull-down menu, or leave the devices unmodified.
11. Click **Save**.

Adding a device to an L3 ISID

Perform the following procedure to add devices to an existing L3 ISID.

Procedure steps

1. From the menu bar, select **Configuration > Fabric Connect**.
2. In the navigation pane, select **L3-SPBm-VSNs**, and then click on an ISID.
3. From the Fabric Connect toolbar, click **Add**.
The Device Selection page appears.
4. To move a device from the Available Devices panel to the Selected Devices panel, double-click the device name or, select the device and click the right-pointing arrow.

*** Note:**

To remove a device from the Selected Devices list, select the device, and click the left-pointing arrow.

5. Click **Select**.
After you have selected the required devices, the Configuration page appears.
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.
You cannot modify the ISID number, and there is no add option on the device and VRF node context.
7. Click **Save**.

Deleting an L3 ISID

Perform the following procedure to delete an L3 ISID from all the devices.

Procedure steps

1. From the menu bar, select **Configuration > Fabric Connect**.
2. From the Fabric Connect navigation tree, select an ISID.
3. From the Fabric Connect 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 menu bar, select **Configuration > Fabric Connect**.
2. From the Fabric Connect navigation pane, select **L3-SPBm-VSNs**, and select a device from an ISID.
3. From the Fabric Connect toolbar, 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

The screenshot shows the 'Fabric Topology' view for 'L3-ISID'. The left sidebar shows a tree view with 'L3-SPBm-VSNs' expanded to 'isid-311'. The main table displays the following data:

IPAddress	SysName	ServiceName	I-...	VRF ID	Redistrib...	MVPN	FwdCacheTi...
10.139.123.168	VSP-8k-R1-BEB-8		311	green(1)	direct,sta...	<input checked="" type="checkbox"/>	210
10.139.123.167	VSP-8k-R1-BEB-7		311	green(1)	direct,sta...	<input checked="" type="checkbox"/>	210
10.139.123.122	VSP-R1-BEB-4		311	green(1)		<input checked="" type="checkbox"/>	210
10.139.123.186	VSP-4K-R1-BEB-5-High...		311	green(1)	direct,sta...	<input checked="" type="checkbox"/>	210

Figure 28: Layer 3 VSNs by ISID

After you select a device from a specific ISID, from the Fabric-centric view in Fabric Connect, 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

The screenshot shows the 'Fabric Topology' view for 'L3-ISID'. The left sidebar shows 'isid-311' expanded to the device '10.139.123.122'. The main table displays the following data:

IPAddress	SysName	ServiceName	I-SID	VRF ID	VLAN	IP Interface	MoSPBm
10.139.123.122	VSP-R1-BEB-4		311	green(1)	Green-V...	10.1.1.2/255.255...	<input type="checkbox"/>
10.139.123.122	VSP-R1-BEB-4		311	green(1)	green-31...	10.3.78.14/255.2...	<input type="checkbox"/>

Figure 29: Layer 3 VSNs by device

BGP-VPN

In the Fabric Connect view, the BGP-VPN node exists in both the Fabric-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 Fabric-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 Fabric-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 Fabric Connect view supports the following:

- Add a Circuitless/Loopback IP address for iBGP peering
- Add a Circuitless/Loopback IP address for IPVPN Lite
- Add Route Target and add RD

Adding a Route Target

To add a Route Target in the Fabric Connect view, you must perform the following procedures.

1. [Adding a Route Target](#) on page 249
2. [Adding a Route Distinguisher to the VRF](#) on page 250
3. [Enabling the VPN status](#) on page 251

Adding a Route Target

Perform the following procedure to add a Route Target to the BGP-VPN node.

Prerequisites

You must be in the Fabric-centric view.

Procedure steps

1. From the menu bar, select **Configuration > Fabric Connect**.
2. In the navigation pane of the Fabric Connect, select **BGP-VPNs**.
3. In the Fabric Connect toolbar, click **Add**.
The Device Selection page appears.
4. To move a device from the Available Devices panel to the Selected Devices panel, double-click the device name or, select the device and click the right-pointing arrow.

Note:

To remove a device from the Selected Devices list, select the device and click the left-pointing arrow.

5. Click **Select**.
The BGP-VPN Configuration page appears.
6. Complete the fields as appropriate and click **Create Route Target**.
The system performs a discovery, and the Operation Result dialog box appears.
7. Click **Ok**.
8. At the bottom of the **BGP-VPN Configuration** page, expand on the **Add Route Target to VPN(s)**.
9. In the **Direction** column, select the direction for the devices that you added.
10. 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 device-centric view. To change the view from the Fabric-centric view to the BGP-VPN device-centric view, in the **Virtualized Networks** tool bar, click **Toggle Device/Fabric centric view**.
- You must see the Route Distinguisher column in the VRF table. To view the Route Distinguisher column, select a column header, click the down arrow, and select the check box for Route Distinguisher.

Procedure steps

1. From the menu bar, select **Configuration > Fabric Connect**.
2. From the navigation pane, select a device and then click **VRF**.
3. From the Fabric Connect tool bar, click **Add**.
4. In the content pane, click on a **Route Distinguisher** field, and enter the appropriate information.

5. Click **Save and apply**.

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 Fabric-centric view. To change the view from the device-centric view to the VSN-centric view, in the Fabric Connect tool bar, click **Toggle Device/Fabric centric view**.

Procedure steps

1. From the menu bar, select **Configuration > Fabric Connect**.
2. From the navigation pane, select **Virtualized Networks > BGP-VPNs**.
3. Select the first child node.
4. In the table, select an IP address, and 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.

Procedure steps

1. From the menu bar, select **Configuration > Fabric Connect**.
2. In the navigation pane of the Fabric Connect, select **Virtualized Networks > BGP-VPNs**, and select the required Route Target node.
3. From the Fabric Connect toolbar, click **Add**.
The Device and UNI Selection page appears.
4. To move a device from the Available Devices panel to the Selected Devices panel, double-click the device name or, select the device and click the right-pointing arrow.

Note:

To remove a device from the Selected Devices list, select the device, and click the left-pointing arrow.

5. Click **Select**.
The Create Route Target page appears.
6. Enter the Route Target Index 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 Fabric-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 Fabric-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 menu bar, select **Configuration > Fabric Connect**.
2. From the Fabric Connect navigation tree, select **BGP-VPNs**, and select a Route Target node.
3. From the Fabric Connect toolbar, click **Delete**.

SPBm Multicast Route table

When you select the SPBm Multicast Route from the Fabric-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.

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.

CFM Globals

CFM Globals table supports configuration of autogenerated CFM MEPs for both B-vlans and C-vlans. This support is provided in the Fabric-centric view.

The following figure shows the CFM Globals table.

Device IP	Device SysNa...	B-Vlan CFM...	B-Vlan M...	B-Vlan MEP Id	C-Vlan CFM...	C-Vlan M...	C-Vlan MEP Id
10.133.13...	BLR-ERS59xx	<input checked="" type="checkbox"/>	4	235			
10.133.13...	VSP-4850GTS	<input checked="" type="checkbox"/>	4	81	<input type="checkbox"/>	4	1
10.133.13...	BLR-VSP70xx	<input checked="" type="checkbox"/>	4	102			
10.133.13...	VSP-7254XTQ	<input type="checkbox"/>	4	1			
10.133.13...	BLR-ERS48xx	<input checked="" type="checkbox"/>	4	207			
10.133.13...	BLR-VSP44xx	<input checked="" type="checkbox"/>	4	85	<input type="checkbox"/>	4	1
10.133.13...	INBLRLABC...	<input checked="" type="checkbox"/>	4	1	<input type="checkbox"/>	4	1

9 Rows

Figure 30: CFM Globals table

Fabric topology

The Fabric Connect Shortest Path Bridging MAC (SPBM) feature permits you to map and highlight SPBM meshes and trees. The default landing page for Fabric Connect is Fabric topology.

You can select the following views:

- Fabric topology view—default landing page that shows 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 image is an example of the Fabric Topology.

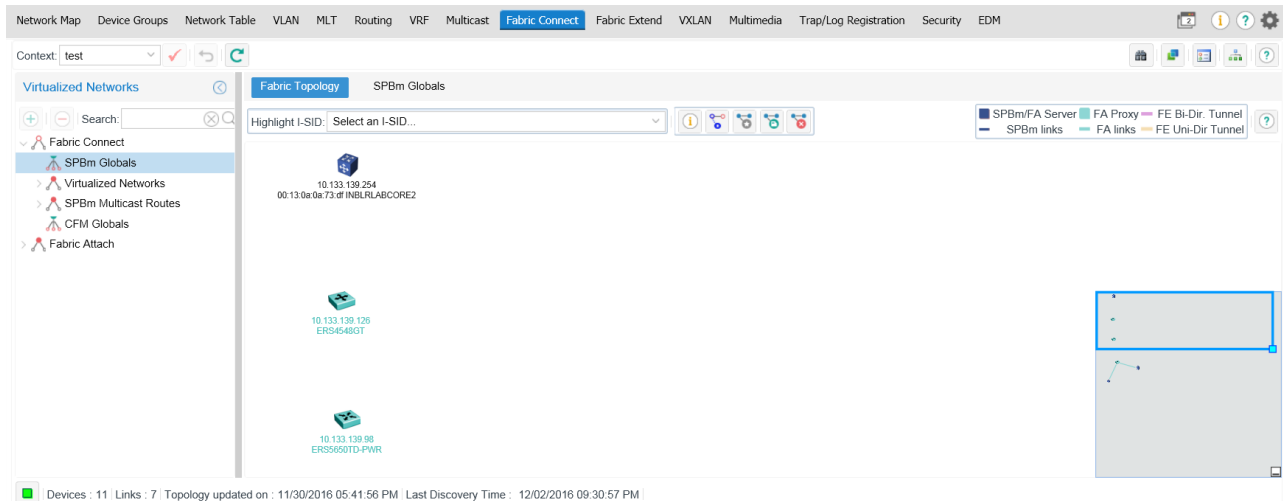


Figure 31: Fabric Topology

Fabric Topology color coding

The contents pane of the Fabric topology contains different colored nodes. These colors indicate whether the node is SPBM enabled, a Fabric Attach Server, or a Fabric Attach Proxy.

Fabric Topology uses color coding to show the following options:

- Highlight — Provides an option to select Fabric Attach which highlights the Fabric Attach Server and the Fabric Attach Proxy in different colors. Fabric Connect allows you to highlight the selected ISID in a particular color.
 - Dark blue — indicates SPBM enabled nodes
 - Light blue — indicates Fabric Attach Proxy
 - Purple — indicates Fabric Extend Bi-Directional Tunnel

- Yellow — indicates Fabric Extend Uni-Directional Tunnel

The following figure shows the Fabric Topology legend that indicates what colors are associated with each node in the contents pane.



Figure 32: Fabric Topology legend

- Port Status — Displays the port editor to show the Fabric Attach enabled ports in a different color. To display the port editor, right-click on the device in the contents pane.
 - Green — indicates the number of ports that are operating
 - Red — indicates the number of ports that are not operating
 - Blue — indicates the number of ports that are being tested
 - Light blue — indicates Fabric Attach ports that are enabled
 - Orange — indicates Fabric Attach ports that are disabled

The following figure shows the ports status for a device.

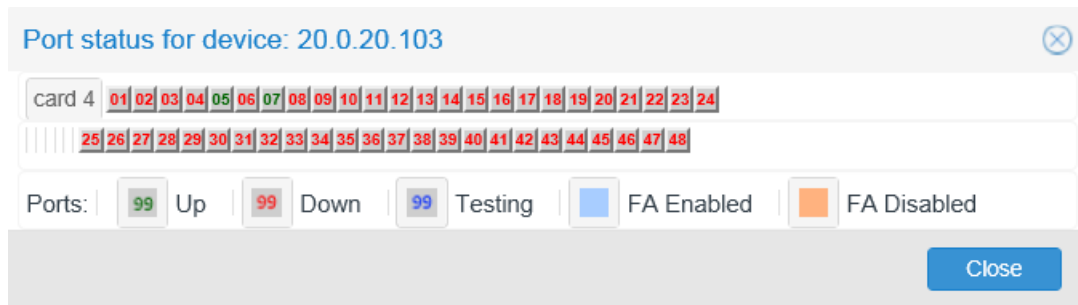


Figure 33: Fabric Attach port status

Fabric Topology icons

The Fabric Topology has the following icons.

Icon	Description
Toggle display of port names	Toggles the Fabric topology view with display or without display of port names.
Toggle display next one hop from SPBm nodes	Toggles the display between next hop from SPB network discovered, and back to the previous display to show only Fabric Connect and Fabric Attach nodes.
Clear all highlights	Clears all highlights you selected.
Save Topology	Saves changes you made to the Fabric Topology.
Clear saved Topology	Clears the topology you saved.

Refreshing the Fabric topology view

Perform the following procedure to refresh a Fabric topology view of all ISIS enabled devices discovered by the Fabric Connect view.

Procedure steps

1. From the menu bar, select **Configuration > Fabric Connect**.
Fabric Connect view performs a discovery, and then the Operation Result dialog box displays.
2. From the Fabric Connect tool bar, click **Show/Re-draw Fabric Topology**.

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. Refresh the Fabric topology view. Refer to [Refreshing the Fabric topology view](#) on page 255.
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. Refresh the Fabric topology view. Refer to [Refreshing the Fabric topology view](#) on page 255.
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. Refresh the Fabric topology view. Refer to [Refreshing the Fabric topology view](#) on page 255.
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 menu bar, select **Configuration > Fabric Connect**.
2. From the Fabric Connect toolbar, click **Show/Re-draw Fabric Topology**.
The Fabric topology view appears in 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 menu bar, select **Configuration > Fabric Connect**.
2. From the Fabric Connect toolbar, click **Show/Re-draw Fabric Topology**.
The Fabric Topology view appears in the contents pane.
3. From the Fabric Connect 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 Fabric topology, the Fabric Connect 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 menu bar, select **Configuration > Fabric Connect**.
Fabric Connect view performs a discovery, and the Operation Result dialog box appears.
2. Click **Ok**.
3. From the Fabric Connect toolbar, click **Show/Re-Draw Fabric Topology**.
The Fabric Topology view appears in 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 Fabric Topology map.

Option	Description
Primary B-VLAN	<p>Displays the primary VLAN map highlighting options.</p> <p>The options are:</p> <ul style="list-style-type: none"> • Multicast Path • Multicast Path by ISID • Unicast Path • Compare Unicast Path • L2 Trace Route

Table continues...

Option	Description
	<ul style="list-style-type: none"> • L2 Ping
Secondary B-VLAN	<p>Displays the secondary VLAN map highlighting options.</p> <p>The options are:</p> <ul style="list-style-type: none"> • Multicast Path • Multicast Path by ISID • Unicast Path • Compare Unicast Path • L2 Trace Route • L2 Ping
SPB Multicast Tree	<p>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.</p>
Private Vlan Ports	<p>Displays Private VLAN ports as promiscuous, isolated, or trunk ports.</p>
Show Connections	<p>Displays the connections between a device and the device neighbors.</p>
Properties...	<p>Displays the description of the device.</p>
Launch Element Manager	<p>Use this option to launch the element manager for the selected device.</p>
Port Status	<p>Displays the status of all ports on a device.</p>
Close	<p>Closes the menu.</p>
Multicast Path	<p>Displays the SPF tree view; the path to all devices.</p>
Multicast Path by ISID	<p>Highlights the path from the selected device to all other members of the selected ISID group. For example, if the selected ISID is 500, the system highlights the path from the selected device to all members of the ISID group 500.</p>
Unicast Path	<p>Displays the configured Unicast path between two selected devices.</p>
Compare Unicast Path	<p>Compares the configured Unicast path defined on two selected devices.</p>
L2 Trace Route	<p>Performs an L2 Trace Route between two selected devices.</p>
L2 Ping	<p>Performs an L2 Ping between two selected devices.</p>

Fabric Attach

Fabric Attach (FA) extends Fabric technology benefits to network elements or hosts that are not SPB-capable. Fabric Attach is implemented within the Fabric Connect view.

You can enable Fabric Attach on the following switches:

- FA Server — for VOSS, ERS 49xx v5.9.2 and later, ERS 4850 v5.9.2 and later, and ERS 59xx series devices
- FA Proxy (client proxy) — for ERS 35xx, ERS 48xx, ERS 49xx, ERS 55xx, ERS 56xx, ERS 59xx, and VSP 70xx series devices
- FA Standalone Proxy (client proxy) — for ERS 35xx, ERS 48xx, ERS 55xx, ERS 56xx, ERS 59xx, and VSP 70xx series devices

The following operations are supported in Fabric Attach.

Discovery and launching

The system discovers FA server and proxy capable devices, and FA configurations on FA enabled devices.

Fabric topology

The system discovers FA Proxy with FA Server capable devices that appear in the topology, port information, and CVID between the FA Server and FA Proxy. The Fabric topology supports Highlight and Port Status functions. After you right-click on a device, the selection of port status displays the port editor where the FA enabled ports are highlighted in a different color.

Configuration

FA configurations to add, delete, and edit are supported in the following views within Fabric Connect.

- Fabric-centric view — Use this view to configure FA Globals for devices, such as FA Service, Element Type, Proxy Mode, and Uplink configurations.
- Device-centric view — Use this view to configure FA Ports, FA ISID-VLAN assignments, and FA Elements.
 - FA Ports — Provide the Fabric Attach mapping at the port level, and provide the configuration to enable or disable Fabric Attach on ports.
 - FA ISID-VLAN Assignments — Provide the discovery of ISID-VLAN mapping that determines the mapping between the following options:
 - FA Server and FA Proxy
 - FA Server and FA Standalone Proxy
 - FA Proxy and FA Client
 - FA Server and FA Client
 - FA Elements — Provide information about the locally connected Fabric Attach elements that the system discovers.

Flex UNI

Flex UNI is a new service within L2 VSN UNI that creates Fabric Attach end points. The system supports this service for VOSS devices with software versions 5.0 and later.

Fabric Attach Ports

FA Ports provides the Fabric Attach mapping at the port level. With FA Ports, you can perform the following actions:

- Enable or disable Fabric Attach on the ports.
- Enable or disable the message authentication status on the ports.
- Configure the message authentication key on the ports.
- Configure the management ISID on FA Servers that are VOSS devices only.
- Configure the management CVID on FA Servers that are VOSS devices only.

The following figure shows the FA Ports table.

Port	State	RowStatus	MsgAuthKey	MsgAuthStatus	MgmtIsid	MgmtCvid
1/5	enabled	active	****	disabled	16	4096
1/6	enabled	active	****	disabled	16	4096
1/7	enabled	active	****	disabled	16	4096
1/8	enabled	active	****	disabled	16	4096
1/13	enabled	active	****	disabled	14	4096
1/14	enabled	active	****	disabled	14	4096
1/24	enabled	active	****	disabled	24	4096

Figure 34: FA Ports table in the Device-centric view

Use the following procedures to add a port or MLT, delete a port or MLT, and edit a ports table for a Fabric Attach Server or Fabric Attach Proxy.

Adding a port or MLT for a Fabric Attach Server or Proxy

Use this procedure to add a port or MLT to a server or proxy that supports Fabric Attach.

*** Note:**

You can add ports and MLTs on VOSS devices only.

Before you begin

You must be in the Device-centric view.

Procedure

1. Select **Configuration > Fabric Connect**.
2. In the navigation pane, select **Fabric Attach**.

3. Select **FA Server**, then select a VOSS device (VSP 4xxx, VSP 72xx, or VSP 8xxx).
4. Select the **FA Ports** tab.
5. In the contents pane, click **Add**.
6. Select **Port** or **Mlt**.
 - To add a port, click **port**, select port members, then click **Save**.
 - To add an Mlt, enter an MLT ID, or select an MLT ID from the drop-down list.
7. Click **Add**.

Job aid

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

Field	Description
Port	Indicates the current port attribute of the Fabric Attach Port table.
State	Indicates the current port state, from a Fabric Attach perspective, about whether Fabric Attach TLVs are included in LLDPDUs generated on the port. The values are enabled or disabled.
RowStatus	Provides access to create, delete, or modify entries in the FA Ports table.
MsgAuthKey	Provides access to the Fabric Attach message authentication key for the associated interface, where you can establish a new key of length from 1 to 32 octets. After a query, the system returns a zero-length string.
MsgAuthStatus	Controls the current Fabric Attach message authentication status for the associated interface.
Mgmtlsid	Indicates the Fabric Attach management i-sid for the associated interface. Zero indicates that the management i-sid feature is not enabled.
MgmtCvid	Indicates the Fabric Attach management customer VID for the associated interface. <ul style="list-style-type: none"> • Zero indicates that the management i-sid feature is not enabled. • The number 4096 indicates that the management i-sid is untagged.

Deleting a port or MLT from a Fabric Attach Server or Proxy

Use this procedure to delete a port or MLT from a server or proxy that supports Fabric Attach.

 **Note:**

You can delete ports and MLTs on VOSS devices only.

Before you begin

You must be in the Device-centric view.

Procedure

1. Select **Configuration > Fabric Connect**.
2. In the navigation pane, select **Fabric Attach**.
3. Select **FA Server**, then select a VOSS device (VSP 4xxx, VSP 72xx, or VSP 8xxx).
4. Select the **FA Ports** tab.
5. In the contents pane, select a port or mlt, then click **Delete**.
6. Click **Ok**.

Job aid

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

Field	Description
Port	Indicates the current port attribute of the Fabric Attach Port table.
State	Indicates the current port state, from a Fabric Attach perspective, about whether Fabric Attach TLVs are included in LLDPDUs generated on the port. The values are enabled or disabled.
RowStatus	Provides access to create, delete, or modify entries in the FA Ports table.
MsgAuthKey	Provides access to the Fabric Attach message authentication key for the associated interface, where you can establish a new key of length from 1 to 32 octets. After a query, the system returns a zero-length string.
MsgAuthStatus	Controls the current Fabric Attach message authentication status for the associated interface.
Mgmtlsid	Indicates the Fabric Attach management i-sid for the associated interface. Zero indicates that the management i-sid feature is not enabled.
MgmtCvid	Indicates the Fabric Attach management customer VID for the associated interface. <ul style="list-style-type: none"> • Zero indicates that the management i-sid feature is not enabled. • The number 4096 indicates that the management i-sid is untagged.

Editing the Fabric Attach ports table

Use this procedure to modify the existing ports table for a Fabric Attach server or proxy.

Before you begin

You must be in the Device-centric view.

* Note:

The shaded cells are read-only.

Procedure

1. Select **Configuration > Fabric Connect**.
2. In the navigation panel, select **Fabric Attach**, and then perform one of the following actions.
 - Select **FA Server**, and then select a device.
 - Select **FA Proxy**, and then select a device.
3. Click the **FA Ports** tab.
4. Configure the required fields by double-clicking on a cell and then enter, or select by clicking the down arrow, the required value. You can configure the following cells:
 - State — select enabled or disabled.
 - MsgAuthKey — enter a value.
 - MsgAuthStatus — select enabled or disabled.
 - Mgmtlsid — enter a value for FA Servers that are VOSS devices only.
 - MgmtCvid — enter a value for FA Servers that are VOSS devices only.
5. Click **Apply**.

Job aid

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

Field	Description
Port	Indicates the current port attribute of the Fabric Attach Port table.
State	Indicates the current port state, from a Fabric Attach perspective, about whether Fabric Attach TLVs are included in LLDPDUs generated on the port. The values are enabled or disabled.
RowStatus	Provides access to create, delete, or modify entries in the FA Ports table.
MsgAuthKey	Provides access to the Fabric Attach message authentication key for the associated interface, where you can establish a new key of length from 1 to 32 octets. After a query, the system returns a zero-length string.

Table continues...

Field	Description
MsgAuthStatus	Controls the current Fabric Attach message authentication status for the associated interface.
MgmtIsid	Indicates the Fabric Attach management i-sid for the associated interface. Zero indicates that the management i-sid feature is not enabled.
MgmtCvid	Indicates the Fabric Attach management customer VID for the associated interface. <ul style="list-style-type: none"> • Zero indicates that the management i-sid feature is not enabled. • The number 4096 indicates that the management i-sid is untagged.

Fabric Attach ISID-VLAN Assignments

FA ISID-VLAN Assignments provides the discovery of ISID-VLAN mapping that determines the mapping between the following options:

- FA Server, and FA Proxy or FA Standalone Proxy
- FA Proxy and FA Client
- FA Server and FA Client

To view updated data on the FA ISID-VLAN Assignments table for the device selected, click the **Refresh** button.

The following data is discovered on the device centric view for FA ISID-VLAN Assignments:

- ISID
- VLAN
- Port
- ServiceName
- State
- Origin

The FA ISID-VLAN Assignments table is read only. ISID-VLAN data is pushed by the FA Client on to the FA Server, or FA Proxy, using various methods such as the Radius Server.

The following figure shows the FA ISID-VLAN Assignments table.

Isid	Vlan	Port	ServiceName	State	RowStatus	Origin
7550	755	1/8		active		faClient
790	790	1/9		active		faProxy

Figure 35: FA ISID-VLAN Assignments table in the Device-centric view

Viewing Fabric Attach server I-SID-VLAN assignments

Use this procedure to view server information for Fabric Attach enabled devices.

Before you begin

You must be in the Device-centric view.

Procedure

1. Select **Configuration > Fabric Connect**.
2. From the navigation panel, select **Fabric Attach > FA Server**.
3. Expand **FA Server**, and then select a device.
4. In the contents panel, select the **FA ISID-VLAN Assignments** tab.

Job aid

The following table describes the fields in the FA ISID-VLAN Assignments table.

Field	Description
Isid	Indicates the I-SID component of the I-SID-VLAN assignment.
ServiceName	Indicates the service name of the ISID.
Vlan	Indicates the VLAN ID component of the I-SID-VLAN assignment.
Port	Indicates the port, or interface identifier, component of the I-SID-VLAN assignment.
State	Indicates the state of the Fabric Attach I-SID-VLAN assignment.
RowStatus	Provides access to create and delete entries in the Fabric Attach ISID-VLAN Assignments table.
Origin	Indicates origin information for the Fabric Attach I-SID-VLAN assignment.

Viewing Fabric Attach Proxy I-SID-VLAN assignments

Use this procedure to view proxy information for Fabric Attach enabled devices.

Before you begin

You must be in the Device-centric view.

Procedure

1. Select **Configuration > Fabric Connect**.
2. From the navigation panel, select **Fabric Attach > FA Proxy**.
3. Expand **FA Proxy**, and then select a device.
4. In the contents panel, select the **FA ISID-VLAN Assignments** tab.

Job aid

The following table describes the fields in the FA ISID-VLAN Assignments table.

Field	Description
Isid	Indicates the I-SID component of the I-SID-VLAN assignment.
ServiceName	Indicates the service name of the ISID.
Vlan	Indicates the VLAN ID component of the I-SID-VLAN assignment.
Port	Indicates the port, or interface identifier, component of the I-SID-VLAN assignment.
State	Indicates the state of the Fabric Attach I-SID-VLAN assignment.
RowStatus	Provides access to create and delete entries in the Fabric Attach ISID-VLAN Assignments table.
Origin	Indicates origin information for the Fabric Attach I-SID-VLAN assignment.

Fabric Attach Elements

The FA Elements table provides information about the locally connected Fabric Attach elements that the system has discovered. FA Elements provides the following information:

- Port — the port through which the Fabric Attach element represented by this entry is discovered.
- Element type — the Fabric Attach element type as advertised through LLDP.
- Element VLAN — the Fabric Attach element VLAN as advertised through LLDP.
- Element ID — exports the chassis ID associated with the discovered Fabric Attach element as advertised through LLDP.
- Element state — exports the state flag data associated with the discovered Fabric Attach element as advertised through LLDP.
- Authentication status — authentication status of a discovered element.
- Operational authentication status — current operational Fabric Attach elements authentication status for the associated interface.

- Assignment authentication status — the assignment authentication status.
- Assignment operational authentication status — current operational Fabric Attach assignment authentication status for the associated interface.

The FA Elements table is read only.

The following figure shows the FA Elements table.

Port	Type	Vlan	Id	State	Auth	OperAuth...	AsgnsOp...	AsgnsOp...
1/7	faClientVi...	0	10.cd.ae:...	trafficTag...	notAuthe...	successN...	notAuthe...	successN...
1/8	faClientVi...	0	10.cd.ae:...	trafficTag...	notAuthe...	successN...	notAuthe...	successN...
1/37	faClientVi...	0	10.cd.ae:...	trafficTag...	notAuthe...	successN...	notAuthe...	successN...
1/38	faClientVi...	0	10.cd.ae:...	trafficTag...	notAuthe...	successN...	notAuthe...	successN...
1/41	faClientVi...	0	10.cd.ae:...	trafficTag...	notAuthe...	successN...	notAuthe...	successN...
1/42	faClientVi...	0	10.cd.ae:...	trafficTag...	notAuthe...	successN...	notAuthe...	successN...

Figure 36: FA Elements table in the Device-centric view

Viewing Fabric Attach Server elements

Use this procedure to view the elements that are connected to the server. This information is read only.

Before you begin

You must be in the Device-centric view.

Procedure

1. Select **Configuration > Fabric Connect**.
2. From the navigation panel, select **Fabric Attach > FA Server**, and then select a device.
3. In the contents pane, select **FA Elements**.

Job aid

The following table describes the fields in the FA Elements table.

Field	Description
Port	Identifies the port through which the Fabric Attach element represented by this entry is discovered.
Type	Identifies the Fabric Attach element type as advertised through LLDP.
Vlan	Identifies the Fabric Attach element VLAN as advertised through LLDP.

Table continues...

Field	Description
Id	Exports the chassis ID associated with the discovered Fabric Attach element as advertised through LLDP.
State	Exports the state flag data associated with the discovered Fabric Attach element as advertised through LLDP.
Auth	Indicates the discovered element authentication status.
OperAuthStatus	Indicates the current operational Fabric Attach elements authentication status for the associated interface.
AsgnsOperAuth	Indicates the assignment authentication status.
AsgnsOperAuthStatus	Indicates the current operational Fabric Attach assignment authentication status for the associated interface.

Viewing Fabric Attach Proxy elements

Use this procedure to view the elements that are connected to the proxy. This information is read only.

Before you begin

You must be in the Device-centric view.

Procedure

1. Select **Configuration > Fabric Connect**.
2. From the navigation panel, select **Fabric Attach > FA Proxy**, and then select a device.
3. In the contents pane, select **FA Elements**.

Job aid

The following table describes the fields in the FA Elements table.

Field	Description
Port	Identifies the port through which the Fabric Attach element represented by this entry is discovered.
Type	Identifies the Fabric Attach element type as advertised through LLDP.
Vlan	Identifies the Fabric Attach element VLAN as advertised through LLDP.
Id	Exports the chassis ID associated with the discovered Fabric Attach element as advertised through LLDP.

Table continues...

Field	Description
State	Exports the state flag data associated with the discovered Fabric Attach element as advertised through LLDP.
Auth	Indicates the discovered element authentication status.
OperAuthStatus	Indicates the current operational Fabric Attach elements authentication status for the associated interface.
AsgnsOperAuth	Indicates the assignment authentication status.
AsgnsOperAuthStatus	Indicates the current operational Fabric Attach assignment authentication status for the associated interface.

Configuring Fabric Attach devices globally

Before you begin

You must be in the Fabric-centric view.

Procedure

1. Select **Configuration > Fabric Connect**.
2. In the navigation panel, select **Fabric Attach > FA Globals**.
3. Select a cell that is you can configure, and double-click on the cell.
You cannot configure the cells that are greyed out.
4. Enter a new value, and click **Apply**.

Job aid

The following table describes the fields in the FA Globals table.

Field	Description
Device IP	Indicates the IP address of the device.
Device Name	Indicates the SysName of the device.
Device Type	Indicates the device type of the device.
FA Service	Exports the status of the Fabric Attach service. You can modify the information in this field for VOSS devices only.
FA Element Type	Exports the Fabric Attach element type indicating the services supported by the system. For platforms that support a single element type only, the information may be read-only. You can modify the information for ERS 49xx, ERS 59xx, and ERS 48xx v5.9.2 and later devices.

Table continues...

Field	Description
FA Proxy Mode	Indicates the FA proxy mode as Standalone, Client, or None. You cannot edit this field for VOSS devices (VSP 4xxx, VSP 72xx, and VSP 8xxx).
UplinkPort	The static uplink port identifier attribute. You cannot edit this field for VOSS devices (VSP 4xxx, VSP 72xx, and VSP 8xxx).
UplinkTrunk	The static uplink trunk ID or MLT ID identifier attribute. You cannot edit this field for VOSS devices (VSP 4xxx, VSP 72xx, and VSP 8xxx).
ZeroTouchService	Controls the status of the Fabric Attach Zero Touch service. You cannot edit this field for VOSS devices (VSP 4xxx, VSP 72xx, and VSP 8xxx).
PrimaryServerID	Exports primary server ID data on a FA Proxy if a primary server has been selected. A zero length string indicates that a primary server does not currently exist. This entry applies to FA Proxy devices only.
PrimaryServerDescr	Exports a primary server description on a FA Proxy if a primary server has been selected. This entry applies to FA Proxy devices only.
Provision Mode	Exports the Fabric Attach provision mode. The options are: disabled, spbm, or vlan.

Viewing Fabric Attach devices

Use this procedure to view all Fabric Attach enabled devices in the current device group context. This table is read-only.

Before you begin

You must be in the Device-centric view.

Procedure

1. Select **Configuration > Fabric Connect**.
2. In the navigation pane, select **Fabric Attach**.
3. Select the **VSN Home** tab.

Job aid

The following table describes the fields in the Fabric Attach VSN Home table.

Field	Description
IPAddress	Indicates the IP address of the Fabric Attach enabled device.

Table continues...

Field	Description
SysName	Indicates the system name of the Fabric Attach enabled device.
ElementType	Indicates the element type of the Fabric Attach enabled device. The elements types are: <ul style="list-style-type: none"> • Server • Proxy • Standalone Proxy

Viewing Fabric Attach Servers

Use this procedure to view Fabric Attach servers. This information is ready-only.

Before you begin

You must be in the Device-centric view.

Procedure

1. Select **Configuration > Fabric Connect**.
2. In the navigation pane, select **Fabric Attach > FA Server**.
3. Select the **VSN Home** tab.

Job aid

The following table describes the fields in the FA Server VSN Home table.

Field	Description
IPAddress	Indicates the IP address of the Fabric Attach server.
SysName	Indicates the System name of the Fabric Attach server.

Viewing Fabric Attach Proxies

Use this procedure to view Fabric Attach proxies. This information is read-only.

Before you begin

You must be in the Device-centric view.

Procedure

1. Select **Configuration > Fabric Connect**.
2. In the navigation pane, select **Fabric Attach > FA Proxy**.
3. Click the **VSN Home** tab.

Job aid

The following table describes the fields in the FA Proxy VSN Home table.

Field	Description
IPAddress	Indicates the IP address of the Fabric Connect Proxy.
SysName	Indicates the system name of the Fabric Connect Proxy.

Chapter 14: Managing Fabric Extend

About Fabric Extend

Fabric Extend provides the ability to extend Fabric Connect across non-SPB networks and devices. Using this feature you can merge multiple isolated SPB clouds into a single SPB network by creating VXLAN tunnels between Backbone Edge Bridges (BEBs). The configuration application in Extreme Networks's network management solutions supports enabling Fabric Extend using the Fabric Extend view.

Overview

The Fabric Extend view provides a graphical management interface for administrators to configure fabric extensions.

Every Fabric Extend network deployment involves creating numerous bidirectional tunnels. Fabric Extend view automates the provisioning of these tunnels by using Fabric Extend domains. When you add nodes to a Fabric Extend domain, Fabric Extend view automatically creates tunnels between the nodes belonging to the same domain. Fabric Extend view also ensures error-free bidirectional tunnel provisioning.

The Fabric Extend feature views the fabric extension as a bidirectional tunnel consisting of two compatible unidirectional tunnels one each configured on the two concerned devices. Thus Fabric Extend view manipulates the tunnels as bidirectional tunnels.

Note:

The fabric can be extended using layer-2 Vlan or SPBoIP. Fabric Extend view supports only SPBoIP tunnels.

Fabric Extend functions

Fabric Extend view provides the following functions:

- Identifies Fabric Extend capable switches.
- Provides an easy way to group and manage a set of Fabric Extend capable switches using domains characterized by the type of topology the group forms. For example: Mesh, Hub-and-Spoke.
- Provides an easy way to configure and manage point-to-point fabric extensions.

Fabric Extend domains

Fabric Extend domains represent a topological arrangement or grouping of Fabric Extend capable devices. There are two types of Fabric Extend domains:

- **Mesh** – This type of domain creates full-mesh tunnels between all nodes (switches). If you add a switch to a mesh domain, Fabric Extend automatically builds Fabric Extend tunnels to all the other switches in the domain.
- **Hub-and-Spoke** – This type of domain identifies each node as either a hub or a spoke.
 - Hub nodes automatically establish bidirectional tunnels with all nodes in the domain.
 - Spoke nodes automatically establish bidirectional tunnels only with the hub nodes in the domain.

Point-to-Point tunnels

You can use Fabric Extend view to provision your own tunnels between Fabric Extend-capable nodes. You must specify the tunnel configuration for both ends of the tunnels.

For more information on Fabric Extend, see .

User interface

This section identifies the components of the user interface for Fabric Extend view.

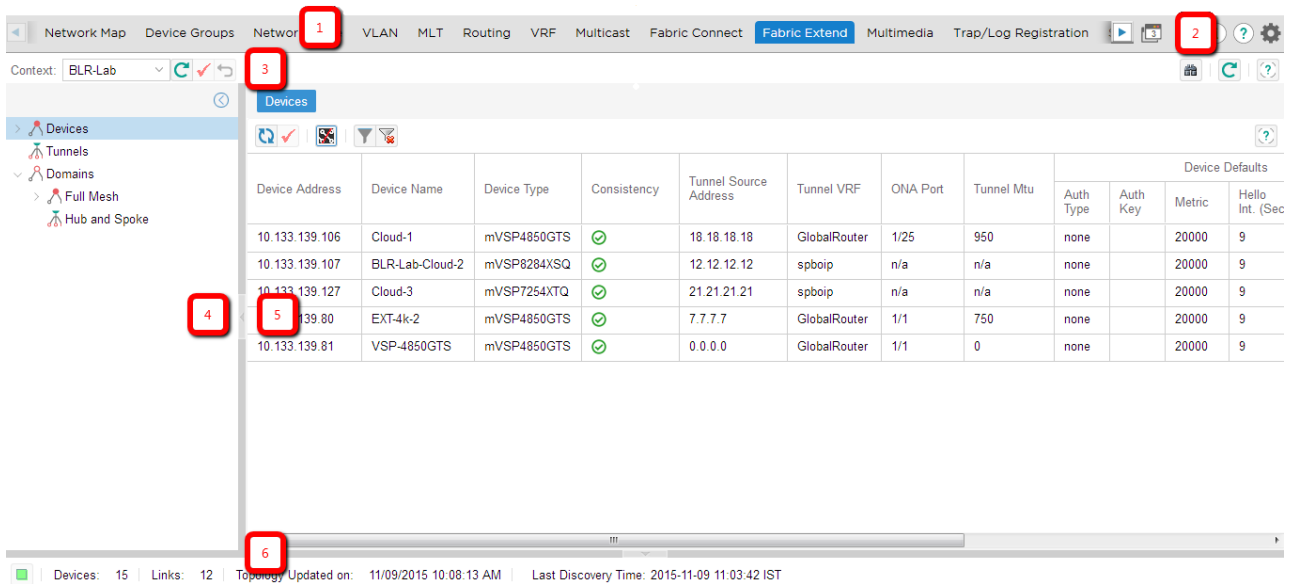


Figure 37: Fabric Extend view user interface








The following table explains the areas of the Fabric Extend view.

Number	Name	Description
1	Menu bar	Provides the navigation options for the system.
2	Quick access toolbar	Provides quick access to commonly used commands.

Table continues...

Number	Name	Description
3	Fabric Extend toolbar	Provides access to operations that apply to the entire Fabric Extend view.
4	Fabric Extend navigation pane	Provides the navigation options to configure Fabric Extend devices, tunnels, and domains.
5	Contents pane	Provides the work area for Fabric Extend configuration. This information is contextual based on the selection you make in the Fabric Extend navigation pane.
6	Message bar	Provides status messages, information about the last discovery time, and ro or rw access.

The following table identifies the available options in the Fabric Extend toolbar.

Tool	Toolbar button or field	Description
Context	Context: <input type="text" value="subnet139"/> 	Use this option to select the available groups assigned to the current logged in user. After you change the context, a notification is sent to all opened configuration views in the system with the same logged in user. All opened views are refreshed after receiving this notification.
Refresh/Reload Context values		Refreshes data for the device group context.
Save/update Current Context		Saves or updates the current device group context.
Revert		Reverts to the current device group context.
Discover		Discovers Fabric Extend devices and existing tunnels. Discovery occurs within the current device group context.
Refresh view		Reloads the entire Fabric Extend view.
Help		Opens online Help.

Views

Fabric Extend provides three types of tunnel configuration views:

- Devices
- Tunnels
- Domains

*** Note:**

All Fabric Extend tunnel configuration views show respective data for the current device group context only.

Devices view

This view provides a device-centric view. You can view device-level configuration of Fabric Extend.

Tunnels view

This view shows all bidirectional tunnels that exist between devices belonging to the current device group context. You can create two types of tunnels:

- Tunnels that do not belong to any domain — You can create a bidirectional tunnel (point-to-point tunnel) manually using this view.
- Tunnels that belong to one or more domains — If you add a new device to a domain, the system automatically creates tunnels between devices in the domain using the default domain values. The number of tunnels created depends on the domain topology.

Domains view

This view shows domain-level configuration and all tunnels for an individual domain.

You can group devices (there by tunnels) into domains based on the required topology: Full Mesh topology or Hub and Spoke topology.

*** Note:**

The domain feature exists only in Fabric Extend view. No such feature exists on the device.

Supported products

This section identifies the products that support the Fabric Extend feature. The following table also indicates the earliest product release to support Fabric Extend.

Product	Fabric Extend support introduced in product Release
Virtual Services Platform 4000 Series This device does not support Fabric Extend natively and requires Open Networking Adapter (ONA). For more information, see .	5.0
Virtual Services Platform 7200 Series	5.0
Virtual Services Platform 8200	5.0
Virtual Services Platform 8400	5.0

For information about the Fabric Extend implementation on a specific product, see the product documentation.

Fabric Extend view

The following sections provide the procedures to configure Fabric Extend tunnels. Fabric Extend provides three views for configuration:

- Devices view
- Tunnels view
- Domains view

Opening Fabric Extend view

Use this procedure to open Fabric Extend view.

Procedure

1. Log in.
2. From the menu bar, click **Configuration > Fabric Extend**.

If the Fabric Extend discovery is already completed for the current context, the information is displayed. Otherwise, a dialog box displays informing the user of a fresh discovery before starting the discovery.

Setting or changing the current context

Set the current context to select the device group to configure using Fabric Extend view. The user interface automatically refreshes to show the device view of the current context.

Procedure

1. Open the Fabric Extend view.
2. In the Fabric Extend toolbar, select the name of the device group in the **Context** field.
3. Click **Save/update Current Context**.

If this is the first time you have selected the chosen context, the system informs you that a fresh discovery is required, and the discovery starts automatically. If you have previously performed a discovery for the chosen context, that data immediately displays in the user interface.

Rediscovering tunnels

Use this procedure to explicitly rediscover existing Fabric Extend tunnels between devices in the selected device group context.

Before you begin

- Open Fabric Extend view.
- Set the current device group context.
- Configure Fabric Extend view preferences.

Procedure

1. In the Fabric Extend toolbar, click **Discover**.



2. After the discovery is complete, view the status and any error or warning messages in the progress bar.
3. Click **OK** to close the progress bar.

The user interface automatically updates to display the discovered devices and tunnels. Also, the Last Discovery Time is updated in the message bar.

If discovery fails for any device, the data that corresponds to the previous discovery of that device, if any, displays. If no such data exists, no data displays for the device.

Devices view configuration

This section includes procedures to configure an individual device that supports the Fabric Extend feature.

Configuring Fabric Extend on a device

Configure Fabric Extend to modify the existing tunnel configuration for a specific device.

About this task

The Devices table shows all Fabric Extend capable devices in the current context. You can edit all fields except for the following:

- Device Address
- Device Name
- Device Type
- Consistency
- Domain
- Discovered On

Some fields provide values configured on the device while others are default values saved in the Fabric Extend view to be used as default values for the tunnels created using Fabric Extend view.

VSP 7200, VSP 8200, and VSP 8400 Series support Fabric Extend natively while VSP 4000 Series requires an Open Networking Adapter (ONA). The columns ONA Port and Tunnel Mtu are required and editable only for VSP 4000 devices. For other devices, these fields are marked 'n/a' and non-editable. For more information, see the Fabric Extend documentation for the specific Extreme Networks product.

Procedure

1. In the Fabric Extend navigation pane, click **Devices**.
2. To change the value of an editable field in the contents pane, double-click the table cell, and then modify the entry either by selecting from the available options or entering new values.

3. In the contents pane toolbar, click **Save the changes to the Device**.



Devices field descriptions

The following table describes the fields in the Devices table. The tooltips on the column headers in the table provide useful descriptions about each column.



Name	Description
Device Address	Specifies the IP address of the Fabric Extend capable device.
Device Name	Specifies the name of the Fabric Extend capable device.
Device Type	Specifies the type of Fabric Extend capable device.
Consistency	<p>Indicates whether the device passes the consistency check. The device is considered to fail the consistency check if it meets either of the following conditions:</p> <ul style="list-style-type: none"> • If it does not exist anymore in the Configuration inventory. • If the Tunnel Source Address is not 0.0.0.0 and there exists in the Configuration inventory other devices with the same Tunnel Source Address. <p> indicates the device passes the consistency check.</p> <p> indicates the device fails the consistency check.</p>
Tunnel Source Address	<p>Specifies the IS-IS IPv4 tunnel source address, which is a CLIP address or a Brouter interface address.</p> <p>The associated editor displays the addresses of the CLIP and Brouter interface belonging to the VRF selected in the "Tunnel VRF" column.</p>
Tunnel VRF	The VRF whose CLIP or Brouter interface address you want to choose as the Tunnel Source Address.
ONA Port Applies to VSP 4000 only.	<p>Specifies the device port that connects to the ONA.</p> <p>This field is editable for VSP 4000 devices. The format for this field is "slot/port". The value is 'n/a' for other devices.</p>
Tunnel Mtu Applies to VSP 4000 only.	Specifies the size of the maximum transmission unit (MTU).

Table continues...

Name	Description
	This field is editable for VSP 4000 devices. The value is 'n/a' for other devices.
Default Auth Type	Specifies the authentication type for IS-IS interface authentication. Value saved locally in Fabric Extend view to be used as default value while creating tunnels.
Default Auth Key	Specifies the key value for IS-IS interface authentication. Value saved locally in Fabric Extend view to be used as default value while creating tunnels.
Default Metric	Configures the link metric to overwrite the default metric value. Value saved locally in Fabric Extend view to be used as default value while creating tunnels.
Default Hello Int. (Sec)	Specifies how often IS-IS Hello packets are sent.
Default Hello Mult.	Specifies how many Hellos the device must miss before it considers the adjacency with a neighboring device down. Value saved locally in Fabric Extend view to be used as default value while creating tunnels.
Domain	Specifies the domain name. This field displays as a button. If you click the button, a dialog box appears that contains a list of the domains to which the device belongs.
Discovered On	Displays the last discovery timestamp for the fabric extend device. A significant older value in this value compared to the Last Discovery Time displayed in the message bar indicates that the last discovery failed for the device.

Adding a CLIP interface

Add a Circuitless IP (CLIP) interface to use as the Tunnel Source Address for a Fabric Extend device or a VXLAN device.

 **Note:**

Tunnel Source IP Address is either a CLIP interface address or a router interface address. In EFO, Fabric Extend and VXLAN support the creation of the required CLIP interface address only.

You can use the Add CLIP dialog box to add as many CLIP interfaces as you need to any device before you close the dialog box.

Procedure

1. Perform one of the following actions:
 - To add a CLIP interface with Fabric Extend, select **Configuration > Fabric Extend**, and in the navigation pane, select **Devices**.
 - To add a CLIP interface with VXLAN, select **Configuration > VXLAN**, and select **Avaya Devices**.
2. In the contents pane toolbar, click **Add a CLIP IP Addr.**
3. Select the device for which you want to create the interface.
4. Select an interface Id.
5. Select a VRF.
6. Enter a CLIP IP address.
7. Enter a CLIP Mask address.
8. Click **Add**.
9. **(Optional)** Repeat steps 3 through 8 to add more CLIP interfaces.
10. Close the **Add Circuitless IP Interface** dialog box.

Add Circuitless IP interface field descriptions

The following table describes the fields in the Add Circuitless IP Interface dialog box.

Name	Description
Select Device	Specifies the device for which to create a CLIP interface.
Interface ID	Assigns a number to the CLIP interface. The value must be between 1 and 255. The field is automatically populated with the next available number.
Select VRF	Associates the CLIP interface with a VRF. The default value is GlobalRouter. If you want to use the created CLIP interface as the Tunnel Source Address, associate the CLIP interface to the VRF selected in the table view.
CLIP IP	Specifies the IP address.
CLIP Mask	Specifies the mask.

Viewing tunnels on a device

Use this procedure to view Fabric Extend unidirectional tunnels for a specific device.

About this task

The information displayed in the Device Tunnels table is for unidirectional tunnels and is read-only. Use the bidirectional tunnels view to add, modify, or delete tunnels.

Before you begin

- Open Fabric Extend view.
- Set the current device group context.

Procedure

1. In the Fabric Extend navigation pane, expand **Devices**.
2. Click on the device.
3. View the tunnel information that appears in the contents pane.

Device Tunnels field descriptions

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

Name	Description
Tunnel ID	Specifies the tunnel ID.
Tunnel Name	Specifies the tunnel name.
Dest Device Addr	Specifies the IP address of the destination device.
Tunnel Dest Addr	Specifies the IP address for the tunnel destination.
Auth Type	Specifies the authentication type for IS-IS interface authentication.
Auth Key	Specifies the key value for IS-IS interface authentication.
Default Metric	Configures the link metric to overwrite the default metric value.
Default Hello Int. (Sec)	Specifies how often IS-IS Hello packets are sent.
Default Hello Mult.	Specifies how many Hellos the device must miss before it considers the adjacency with a neighboring device down.

Tunnels view configuration

This section includes procedures to create and configure Fabric Extend tunnels.



Viewing or editing tunnel information

Use this procedure to view or edit information about bidirectional tunnels within the current context. The Tunnels table includes information for the following types of tunnels:

- tunnels that do not belong to any domain
- tunnels that belong to one or more domains

In the Tunnels table, you cannot edit tunnel information for tunnels that belong to a domain; you can only edit tunnels that do not belong to any domain.

About this task

In the contents pane toolbar, use the show or hide tunnel parameters toggle buttons ( ) to view either summary or detailed tunnel information. This table is read-only in the summary view.

The Tunnels table shows the tunnel information for both directions, left-to-right and right-to-left.

*** Note:**

The two unidirectional tunnels that comprise of a bidirectional tunnel are named LeftToRight tunnel and RightToLeft tunnel for convenience only. There is no concept of left-to-right or right-to-left direction for the tunnels. Further for consistency, in the Tunnels table, the device with the lexically lower IP address is considered the left device. For example, 10.133.139.106 is lower than 10.133.139.222, which is lower than 10.133.139.88 because 8 appears after 1 and 2 in alphanumeric comparison.

The Tunnels table also displays the partial bidirectional tunnels whose both end devices belong to the current device group context. In partial bidirectional tunnels, only one end device is configured. The data for the unidirectional tunnel that is missing, is usually empty except for the device name and IP address.

Procedure

1. In the Fabric Extend navigation pane, click **Tunnels**.
2. View the summary tunnel information that appears in the contents pane.
3. To view detailed tunnel information, in the contents pane toolbar, click **Show the Tunnel Parameters**.
4. View the tunnel information that appears in the contents pane.
5. To change the value of an editable field, double-click the table cell, and then modify the entry.
6. In the content pane toolbar, click **Apply**.

Tunnels field descriptions

The following table describes the fields in the Tunnels table.




Name	Description
Complete?	Indicates whether the bidirectional tunnel is one of the following: <ul style="list-style-type: none"> •  indicates both devices are configured. •  indicates only one of the two devices has been configured. •  indicates the tunnel belongs to one or more domains. You cannot edit this tunnel in this view.
Tunnel Id	Specifies the tunnel ID on the device at one end of the tunnel. This information appears for both tunnel directions. This field appears only in the Detailed view.

Table continues...

Name	Description
Tunnel Name	<p>Specifies the name of the tunnel as configured on the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p>
Device Name	<p>Specifies the name of the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p>
Device Address	<p>Specifies the IP address of the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p>
Destination Address	<p>Specifies the destination IP address of the device at one end of the tunnel..</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view.</p>
Auth Type	<p>Specifies the authentication type for IS-IS interface authentication on the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view. You can edit this field.</p>
Auth Key	<p>Specifies the key value for IS-IS interface authentication on the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view. You can edit this field.</p>
Metric	<p>Configures the link metric to overwrite the default metric value on the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view. You can edit this field.</p>
Hello Interval (Sec)	<p>Specifies how often IS-IS Hello packets are sent on the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view. You can edit this field.</p>
Hello Multiplier	<p>Specifies how many Hellos the device at one end of the tunnel must miss before it considers the adjacency with a neighboring device down.</p>

Table continues...

Name	Description
	This information appears for both tunnel directions. This field appears only in the Detailed view. You can edit this field.
Domain	Specifies the domain name to which the tunnel belongs. This field displays as a button. If you click the button, a dialog box appears that contains a list of the domains to which the device belongs.

Creating a bidirectional tunnel

Use this procedure to manually create a bidirectional tunnel within the current context.

About this task

To create a bidirectional tunnel, configure complimentary unidirectional tunnels on both of the selected devices.

* Note:

The system creates bidirectional tunnels on a best effort basis. If the creation of the unidirectional tunnel fails on one of the devices, the operation is continued to create the unidirectional tunnel on the other device.

Procedure

1. In the Fabric Extend navigation pane, click **Tunnels**.
2. In the contents pane toolbar, click **Add a Bi-Directional Tunnel**.
3. Enter a name for the tunnel.
The name can be a maximum of 16 characters. The same name applies to both unidirectional tunnels.
4. Select the two devices between which to create the tunnel.
5. **(Optional)** Configure tunnel parameters to use a value other than the default.
The same parameter values apply to both unidirectional tunnels.
6. Click **Create**.
7. To create more tunnels, repeat steps 3 to 6.
8. Click **Close**.

Add Bi-directional Tunnel field descriptions

The following table describes the fields in the Add Bi-directional Tunnel dialog box.

Name	Description
Tunnel Name	Specifies a unique name for the tunnel.

Table continues...

Name	Description
Device Selection	Specifies the IP address for both the left and right devices that form the tunnel.
Parameters Option	Specifies the tunnel parameters. The options are Device Defaults and Override.
Auth Type	Specifies the authentication type for IS-IS interface authentication.
Auth Key	Specifies the key value for IS-IS interface authentication.
Metric	Configures the link metric to overwrite the default metric value.
Hello Interval (sec)	Specifies how often IS-IS Hello packets are sent.
Hello Multiplier	Specifies how many Hellos the device must miss before it considers the adjacency with a neighboring device down.

Deleting a bidirectional tunnel that does not belong to a domain

Use this procedure to delete a tunnel that does not belong to a domain from the current context.

About this task

 **Note:**

You cannot delete tunnels that belong to a domain.

Before you begin

- Open Fabric Extend view.
- Set the current device group context.
- Configure Fabric Extend view preferences.

Procedure

1. In the Fabric Extend navigation pane, click **Tunnels**.
2. In the contents pane, select the table row for the tunnel you want to delete.
3. In the contents pane toolbar, click **Delete a Bi-Directional Tunnel**.
4. When prompted to confirm the removal, click **Yes**.

Completing a partial tunnel

Use this procedure to create the missing unidirectional tunnel in a partial tunnel.

Before you begin

- Open Fabric Extend view.
- Set the current device group context.

Procedure

1. In the Fabric Extend navigation pane, click **Tunnels**.
2. In the contents pane, select a partial tunnel.
3. In the contents pane toolbar, click **Complete a Bi-Directional Tunnel**.

Domains view configuration

This sections includes procedures to create and configure domains.

Creating a domain

Use this procedure to create a new domain within the current context.

Before you begin

- Open Fabric Extend view.
- Set the current device group context.

Procedure

1. In the Fabric Extend navigation pane, click **Domains**.
2. In the contents pane toolbar, click **Add a new Domain**.
3. Enter a name for the domain.
The domain name must be unique across all device group contexts.
4. Select the domain topology: **Hub and spoke** or **Full Mesh**.
5. **(Optional)** Select the device in the **Available** list, and then use the navigation arrows to move the device to the **Selected** list.

Note:

The name of the select device area depends on the domain topology. A Full Mesh domain does not show the **Select Hub Device(s)** or **Select Spoke Device(s)** areas.

- a. For a Full Mesh domain, select the devices.

OR

- b. For a Hub and Spoke domain, select the hub and spoke devices separately.
6. **(Optional)** Specify default parameters to use for tunnels automatically created for the domain.
You can customize these parameters by editing individual tunnels even after their creation.
 7. Click **Create** to create the domain or click **Cancel** to close the dialog without creating the domain.

Add Domain field descriptions

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

Name	Description
Domain Name	<p>Specifies an identifying name for the domain.</p> <p>The domain name must be unique across all device group contexts.</p>
Topology Type	<p>Specifies the domain topology. A Hub and Spoke domain identifies each node as either a hub or a spoke. A Full Mesh domain creates full-mesh tunnels between all nodes.</p> <p>Full Mesh is the default topology for a new domain.</p>
Select Device(s), Select Spoke Device(s), or Select Hub Device(s)	<p>Selects devices to add to the domain. If the domain topology is Hub and Spoke, you can specify which devices are the Hub devices.</p>
Auth Type	<p>Specifies the authentication type for IS-IS interface authentication.</p> <p>This value is the default for all automatically-created tunnels in the domain.</p> <p>The default is none.</p>
Auth Key	<p>Specifies the key value for IS-IS interface authentication.</p>
Metric	<p>Configures the link metric to overwrite the default metric value.</p> <p>This value is the default for all automatically-created tunnels in the domain.</p> <p>The default is 20000.</p>
Hello Interval(sec)	<p>Specifies how often IS-IS Hello packets are sent.</p> <p>This value is the default for all automatically-created tunnels in the domain.</p> <p>The default is 9 seconds.</p>
Hello Multiplier	<p>Specifies how many Hellos the device must miss before it considers the adjacency with a neighboring device down.</p> <p>This value is the default for all automatically-created tunnels in the domain.</p> <p>The default is 3.</p>

Viewing or editing domain information

Use this procedure to view or edit information about all domains within the current context. To create or delete a domain, see the following tasks:

- [Creating a domain](#) on page 287
- [Deleting a domain](#) on page 291

 **Note:**

The updated domain default parameters are applied only to the future tunnels created for the domain. To change values for already existing tunnels, you must update them individually using the Domains Tunnel view.

Before you begin

- Open Fabric Extend view.
- Set the current device group context.

Procedure

1. In the Fabric Extend navigation pane, click **Domains**.
2. View the domain information that appears in the contents pane.
3. To change the value of an editable field, double-click the table cell, and then modify the entry.
4. In the contents pane toolbar, click **Save the changes you made to the Domain Summary Table**.

Domains field descriptions

The following table describes the fields in the Domains table.




Name	Description
Domain Name	Specifies the domain name.
Topology	Specifies the domain type: full mesh or hub and spoke.
No. of Devices	Indicates the number of nodes (devices) in the domain.
Consistent?	<p>Indicates whether the domain is consistent.</p> <p> Note:</p> <p>A consistent domain has the following characteristics:</p> <ul style="list-style-type: none"> • Contains devices. • Contains devices that belong to the same device group only. • Contains all required bidirectional tunnels (based on domain topology). <p>Fabric Extend view marks a domain as inconsistent if any of the above characteristics is broken or any of the domain tunnel is partial.</p> <ul style="list-style-type: none"> •  Specifies the device passes the consistency check.

Table continues...

Name	Description
	<ul style="list-style-type: none">  Specifies the device fails the consistency check.
Default Auth. Type	Specifies the authentication type for IS-IS interface authentication. This value is the default for all automatically-created tunnels in the domain.
Default Auth. Key	Specifies the key value for IS-IS interface authentication.
Default Metric	Configures the link metric. This value is the default for all automatically-created tunnels in the domain.
Default Hello Int. (Sec)	Specifies how often IS-IS Hello packets are sent. This value is the default for all automatically-created tunnels in the domain.
Default Hello Mult.	Specifies how many Hellos the device must miss before it considers the adjacency with a neighboring device down. This value is the default for all automatically-created tunnels in the domain.
Created By	Shows the user account that created the domain.
Creation Timestamp	Shows the date and time the domain was created.

Viewing or editing domain information by topology type

Use this procedure to view or edit information about all domains of a specific topology type. To create or delete a domain, see the following tasks:

- [Creating a domain](#) on page 287
- [Deleting a domain](#) on page 291

 **Note:**



The updated domain default parameters are applied only to the future tunnels created for the domain. To change values for already existing tunnels, you must update them individually using the Domains Tunnel view.

Procedure

1. In the Fabric Extend navigation pane, expand **Domains**.
2. Click **Full Mesh** or **Hub and Spoke**.
3. View the domain information that appears in the contents pane.
4. To change the value of an editable field, double-click the table cell, and then modify the entry.
5. Click **Apply**.

Topology Domains field descriptions

The following table describes the fields in the Full Mesh Domains and Hub and Spoke Domains tables.

Name	Description
Domain Name	Specifies the domain name.
Topology	Specifies the domain type: full mesh or hub and spoke.
No. of Devices	Specifies the number of nodes (devices) in the domain.
Consistent?	<p>Specifies whether the device passes the consistency check. The device is considered to fail the consistency check if it meets either of the following conditions:</p> <ul style="list-style-type: none"> • The devices are removed from the device group context after they are added to the domain. • A fresh network discovery is performed after adding a device to the domain, and the domain device is not discovered by the discovery service. •  Specifies the device passes the consistency check. •  Specifies the device fails the consistency check.
Default Auth. Type	Specifies the authentication type for IS-IS interface authentication. This value is the default for all automatically-created tunnels in the domain.
Default Auth. Key	Specifies the key value for IS-IS interface authentication.
Default Metric	Configures the link metric. This value is the default for all automatically-created tunnels in the domain.
Default Hello Int. (Sec)	Specifies how often IS-IS Hello packets are sent. This value is the default for all automatically-created tunnels in the domain.
Default Hello Mult.	Specifies how many Hellos the device must miss before it considers the adjacency with a neighboring device down. This value is the default for all automatically-created tunnels in the domain.
Created By	Shows the user account that created the domain.
Creation Timestamp	Shows the date and time the domain was created.

Deleting a domain

Use this procedure to delete a domain from the current context.

 **Note:**

Deleting a domain does not delete the tunnels belonging to the domain. The tunnels are only disassociated with the domain. Use Tunnels View to delete a tunnel that is not associated with any domain.

Procedure

1. In the Fabric Extend navigation pane, click **Domains**.
2. In the contents pane, select the table row for the domain you want to delete.
3. In the contents pane toolbar, click **Remove a Domain and associated Tunnels**.
4. When prompted to confirm the removal, click **Yes**.

Fixing inconsistent domains

Use this procedure to remove inconsistent domains.

About this task

A consistent domain has the following characteristics:

- Contains devices.
- Contains devices that belong to the same device group only.
- Contains all required bidirectional tunnels (based on domain topology).

Fabric Extend view marks a domain as inconsistent if any of the above characteristics is broken or any of the domain tunnel is partial.

Note:

This procedure attempts to automatically fix as many inconsistencies with the selected domain as possible. It may not be possible to fix all the inconsistencies automatically using this procedure.

Procedure

1. In the Fabric Extend navigation pane, click **Domains**.
2. In the contents pane, select the inconsistent domain.
3. In the contents pane toolbar, click **Analyze and Fix a Domain inconsistency**.

Viewing domain members

Use this procedure to view the nodes (devices) that belong to a domain. To add or remove nodes from a domain, see the following tasks:

- [Adding nodes to a domain](#) on page 293
- [Removing nodes from a domain](#) on page 295

Before you begin



- Open Fabric Extend view.
- Set the current device group context.

Procedure

- In the Fabric Extend navigation pane, expand one of the following folders:
 - **Domains > Full Mesh > <domain name>**
 - **Domains > Hub and Spoke > <domain name>**
- View the information that appears in the contents pane.

Domain Devices field descriptions

The following table describes the fields in the Domain Devices table.

Name	Description
Device Address	Specifies the IP address of the Fabric Extend capable device.
Device Name	Specifies the name of the Fabric Extend capable device.
Node Type	Specifies the node type. In a Hub and Spoke topology, this field identifies if the device is a hub device or a spoke device.
Tunnel Source Addr	Specifies the IS-IS IPv4 tunnel source address.
VRF	Specifies the VRF name associated with the IP tunnel. VRF is an optional parameter. If you do not configure a VRF, Fabric Extend uses the global router.
Consistent?	<p>Specifies whether the device passes the consistency check. The device is considered to fail the consistency check if it meets either of the following conditions:</p> <ul style="list-style-type: none"> • The devices are removed from the device group context after they are added to the domain. • A fresh network discovery is performed after adding a device to the domain, and the domain device is not discovered by the discovery service. •  Specifies the device passes the consistency check. •  Specifies the device fails the consistency check.

Adding nodes to a domain

Use this procedure to add nodes to a domain. You can only add nodes that belong to the current context.

About this task

The system automatically creates bidirectional tunnels between devices when you add a new node to a domain.

It uses the following conventions to name the tunnels that belong to a domain:

- If the combined length of the device names of the two concerned devices is less than 16 characters, then the tunnel name is <device-1 name>-<device-2 name>.
- Otherwise, the tunnel name is <last 2 octets of IP addr of device-1>-<last 2 octets of IP addr of device-2>.

Where, device-1 is the device with lexically lower IP address of the two devices.

* Note:

- This Add or Remove Devices from <domain> dialog box can be used for both adding and removing devices from the domain by appropriately moving devices between the available devices and selected devices lists.
- Depending on the number of devices in the domain and the number of devices being added, this operation may take a while to complete due to creation of all the required tunnels. If a required tunnel already exists (created manually or because of another domain), the existing tunnel is used without any changes to its parameters.

Before you begin

- Open Fabric Extend view.
- Set the current device group context.

Procedure

1. In the Fabric Extend navigation pane, expand one of the following folders:
 - **Domains > Full Mesh > <domain name>**
 - **Domains > Hub and Spoke > <domain name>**
2. In the contents pane toolbar, click **Add/Edit**.
3. Select the device in the **Available** list, and then use the navigation arrows to move the device to the **Selected** list.

* Note:

The name of the select device area depends on the domain topology. A Full Mesh domain does not show the **Select Hub Device(s)** area or **Select Spoke Device(s)** areas.

Moving a device from the **Selected** list to the **Available** list removes the device from the domain.

- a. For a Full Mesh domain, select the devices.

OR

- b. For a Hub and Spoke domain, select the hub and spoke devices separately.

4. Click **Save**.

Add or Remove Devices field descriptions

The following table describes the fields in the Add or Remove Devices from <domain> dialog box.

Name	Description
Domain Name	Specifies an identifying name for the domain. Domain name is pre-populated with the selected domain and is read-only.
Topology Type	Specifies the domain topology. A Hub and Spoke domain identifies each node as either a hub or a spoke. A Full Mesh domain creates full-mesh tunnels between all nodes. Topology Type is pre-populated with the topology type of the selected domain and is read-only.
Select Device(s) , Select Hub Device(s), or Select Spoke Device(s)	Selects devices to add to, or remove from, the domain. If the domain topology is Hub and Spoke, you can specify which devices are the hub devices.
Auth Type	Specifies the authentication type for the IS-IS interface authentication. The value configured for the domain is displayed here as read-only.
Auth Key	Specifies the key value for IS-IS interface authentication. The value configured for the domain is displayed here as read-only.
Metric	Configures the link metric to overwrite the default metric value. The value configured for the domain is displayed here as read-only.
Hello Interval(sec)	Specifies how often IS-IS Hello packets are sent. The value configured for the domain is displayed here as read-only.
Hello Multiplier	Specifies how many Hellos the device must miss before it considers the adjacency with a neighboring device down. The value configured for the domain is displayed here as read-only.

Removing nodes from a domain

Use this procedure to remove nodes from a domain.

About this task

Removing a device from a domain does not delete the tunnels belonging to the domain. The tunnels are only disassociated with the domain. Use Tunnels View to delete a tunnel that is not associated with any domain.

You can also remove a device from a domain by using the Add or Remove Devices from <domain> dialog box. For more information, see [Adding nodes to a domain](#) on page 293.

Before you begin

- Open Fabric Extend view.
- Set the current device group context.

Procedure

1. In the Fabric Extend navigation pane, expand one of the following folders:
 - **Domains > Full Mesh > <domain name>**
 - **Domains > Hub and Spoke > <domain name>**
2. In the contents pane, select the device.
3. In the contents pane toolbar, click **Remove**.
4. When prompted to confirm the removal, click **Yes**.

Viewing or editing tunnel information for a domain



Use this procedure to view or edit detailed information for tunnels of a domain.

Note:

The tunnels that belong to a domain cannot be deleted, hence there is no delete option in the Tunnel View.

About this task

The Domain Tunnels table shows the tunnel information for both directions, left-to-right and right-to-left.

In the contents pane toolbar, use the show or hide tunnel parameters toggle buttons ( ) to view either summary or detailed tunnel information. The information in the summary view is read-only.

Before you begin

- Open Fabric Extend view.
- Set the current device group context.

Procedure

1. In the Fabric Extend navigation pane, expand one of the following folders.
 - **Domains > Full Mesh > <domain name>**
 - **Domains > Hub and Spoke > <domain name>**

2. Click **Tunnels**.
3. View the information that appears in the contents pane.
4. In the contents pane, click **Show the Tunnel Parameters** to change to the detailed view.
5. View the information that appears in the contents pane.
6. To change the value of an editable field, double-click the table cell, and then modify the entry.
7. In the contents pane toolbar, click **Save**.

Domain Tunnels field descriptions

The following table describes the fields in the Domain Tunnels table.



Name	Description
Complete?	<p>Indicates whether the bidirectional tunnel is one of the following:</p> <ul style="list-style-type: none"> •  indicates both devices are configured. •  indicates only one of the two devices has been configured. <p>For information about completing a partial tunnel, see Completing partial tunnel on page 286.</p>
Tunnel ID	<p>Specifies the tunnel ID on the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view.</p>
Tunnel Name	<p>Specifies the name of the tunnel as configured on the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p>
Device Name	<p>Specifies the name of the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p>
Device Address	<p>Specifies the IP address of the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p>
Destination Address	<p>Specifies the destination IP address of the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view.</p>

Table continues...

Name	Description
Auth Type	<p>Specifies the authentication type for IS-IS interface authentication on the device at one end of the tunnel.</p> <p>Change this value to customize a tunnel from the default domain configuration.</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view.</p>
Auth. Key	<p>Specifies the key value for IS-IS interface authentication on the device at one end of the tunnel.</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view.</p>
Metric	<p>Configures the link metric to overwrite the default metric value on the device at one end of the tunnel.</p> <p>Change this value to customize a tunnel from the default domain configuration.</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view.</p>
Hello Interval (Sec)	<p>Specifies how often IS-IS Hello packets are sent on the device at one end of the tunnel.</p> <p>Change this value to customize a tunnel from the default domain configuration.</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view.</p>
Hello Multiplier	<p>Specifies how many Hellos the device at one end of the tunnel must miss before it considers the adjacency with a neighboring device down.</p> <p>Change this value to customize a tunnel from the default domain configuration.</p> <p>This information appears for both tunnel directions.</p> <p>This field appears only in the Detailed view.</p>

Chapter 15: Managing VXLAN

About VXLAN

Virtual Extensive Local Area Network (VXLAN) is a protocol for running a Layer 2 network, and stretching it over a Layer 3 network. This functionality is referred to as a VXLAN segment or tunnel that uses MAC-in-UDP encapsulation. With VXLAN you can separate, abstract, and decouple the physical topology from a logical or virtual topology by using encapsulated tunneling.

VXLAN is an overlay networking protocol that disassociates workloads from physical networks, allowing for possible transition to cloud-based providers.

VXLAN uses VTEP to perform the following gateway functions:

- VXLAN to VLAN
- VXLAN to VXLAN
- VXLAN to SPBm

VXLAN gateway functionality is available in two modes: Base Interworking mode, and Full interworking mode. By default the Base interworking mode is enabled, and Full interworking mode is disabled. VXLAN Gateway uses Head End replication for BUM packets to replicate packets to all VTEPs in a VNID. VXLAN Gateway functionality is supported along with the Fabric Extend feature for both the L2 and L3 cores.

With VXLAN, you can extend the SPB fabric to devices and networks across non-SPB capable or enabled networks, and allows you to integrate or merge multiple isolated SPB clouds, or SPB islands, into a single SPB network. When you use the SPBm-VxLAN gateway, you can merge two SPB clouds without a SPBoIP tunnel.

Devices supported

VXLAN is a feature available on the following devices:

- VSP72xx, v6.0
- VSP8xxx, v6.0

VXLAN is a premium feature which requires a feature level licence.

Features

The VXLAN manager can perform the following actions:

- Discover devices that are capable of supporting VXLAN, based on the logged in user device group context.

- Discover all existing VTEPs and VNIDs based on the logged in user device group context.
- Display VTEP operational mode (basic or full internetworking) of VXLAN capable device.
- Create and delete VTEPs.
- Auto-create or auto-delete remote VTEPs on the neighbor devices.
- Create, modify and delete VNIDs.
- Auto map VNID to I-SID.
- Add VTEPs to the existing VNIDs.
- Support Read-only and Read-write based on logged in user RBAC mechanism.
- Add, update or delete non-Avaya VTEPs to the VXLAN manager.
- Map the non-Avaya VTEPs to an existing VNID.

VXLAN Network

VXLAN Manager discovers all VXLAN capable devices, which include VSP 8000 and VSP 7200 versions 6 and later devices.

The following image demonstrates the configurations that VXLAN Manager performs.

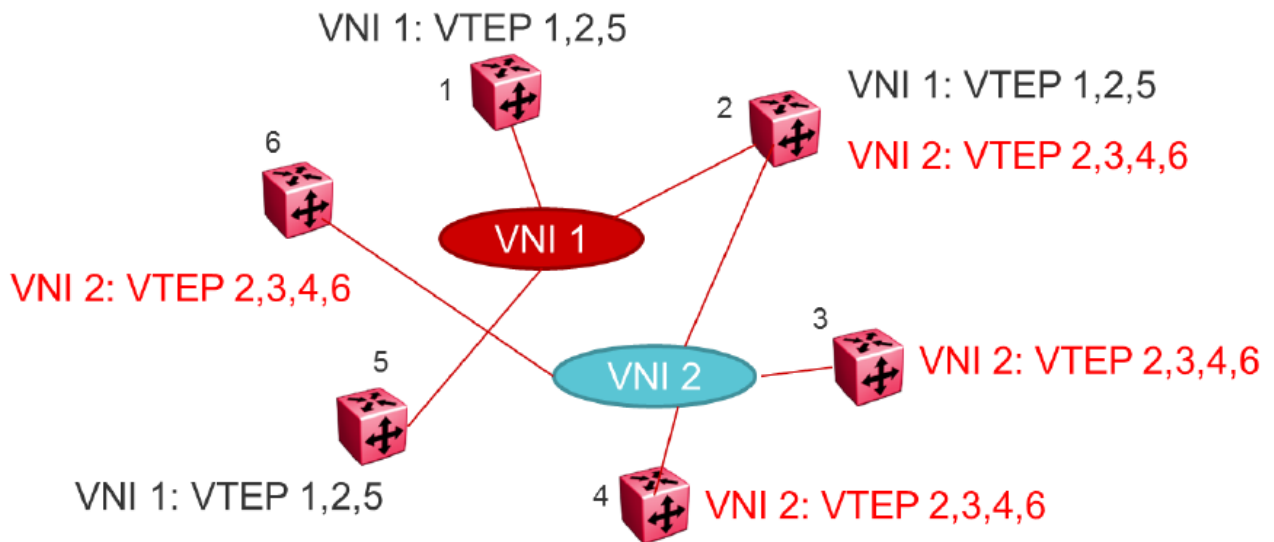


Figure 38: Example of the VXLAN Network topology

1. Discovery of VTEPs

VXLAN Managers recognizes the VTEPs as part of the initial discovery. You can view the preconfigured VTEPs.

2. Enabling VTEP Source Address

Before you configure VXLAN tunnels, you must configure the VTEP source address. With VXLAN Manager, you can enable the VTEP source address by selecting the already configured CLIP address on a particular device.

If you want to configure a new CLIP address, you can add a new CLIP address with the function **Add a new CLIP Address**.

3. Configuring remote VTEPs on a device

You can manually add remote VTEPs on a particular device with the **Add Remote VTEP** option available in the VTEP level summary screen.

If you have already added a neighboring VXLAN capable device VTEP source address, then the system uses the preconfigured VTEP details to map the VTEP to a particular VNI during the VNI creation workflow.

4. Discovery of VNIs

As part of the initial discovery, VXLAN Manager recognizes all VNIs. You can view the preconfigured VNIs for a device.

5. Configuring VNIs on a Device

You can manually add a VNI on a particular device with the **Add VNI** option available in the VNI summary screen.

VXLAN Manager pushes all VNI configurations to a selected set of switches, and forms a full mesh of tunnels for that sub set of switches for this VNI.

The VNI configuration process occurs in one of the following operational modes:

- Base interworking mode

The VNID and I-SID cannot be of the same value. When VNID is mapped to an I-SID, VXLAN always internally creates an I-SID. An I-SID associated with a VNID in the base interworking mode has no significance.

Under VNID, Flex UNI end points, VXLAN ELAN end points, or VTEP tunnel end points are created.

- Full interworking mode

The VNID and I-SID can have the same value. If the I-SID is nonexistent, VXLAN Manager internally creates an I-SID of type Flex UNI and map the I-SID to the VNI.

You can also create an I-SID using Fabric Connect, and use the same I-SID value to map it to a VNI during the VNI creation process.

In this mode, you can also create the I-SID before it is associated with a VNID. Flex UNI end points are created under I-SID, and VXLAN ELAN end points or VTEP tunnel end points are associated with VNID.

VXLAN Manager keeps track of all removal of configurations, and cleans the VTEPs on the neighboring switches.

6. Mapping the VTEPs to a VNI on a Device

Before you can directly map an Avaya VTEP to a VNI, you must add the VNI on a VTEP. After the configuration of a VNI on a device, VXLAN Manager first pushes the VNI configuration on the selected switch, and then maps the VNI to VTEPs.

After you map the VNI to the VTEPs, VXLAN Manager performs the prerequisite configurations, such as adding the VTEP details in the Remote VTEPs table of the neighboring switches which contains the VNI, and then forms a full mesh of tunnels for that sub set of switches for this VNI.

Before you can directly map a non-Avaya VTEP to a VNI, you must add the details of the non-Avaya VTEP.

After the non-Avaya VTEP details are available, you can select a VNI on a device that you want to configure. You can then select a non-Avaya VTEP. VXLAN manager internally adds the non-Avaya VTEP details as remote VTEPs only on the device, and then maps the non-Avaya VTEP to the VNI on the device.

After you map the VNI to a non-Avaya VTEP, VXLAN manager does not perform operations on the non-Avaya VTEP. VXLAN manager uses only the details of the non-Avaya VTEP that you provided during the creation of the non-Avaya VTEP.

VXLAN view navigation pane toolbar

The following table lists the navigation pane toolbar options in the VXLAN view.

Button	Description
Context	Use this option to select the available groups assigned to the current logged in user. After you change the context, a notification is sent to all opened configuration views in the system with the same logged in user. All opened views are refreshed after receiving this notification.
Refresh/reload Context values	Use this option to refresh data for the device group context.
Save Context	Use this option to save the context.
Revert to Current Context	Use this option to revert to the current context.
Discover	Manually starts the VXLAN discovery process.
Refresh View	Reloads the entire VXLAN view.
Help	Launches help for the current view.

VXLAN 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 fields vary in accordance with the resource you select in the navigation pane and in the content pane tab, if applicable.

Button	Description
Refresh	Refreshes the view in the contents pane.
Apply Changes	All changes are applied and saved.
Add	Adds an entry.
Delete	Deletes an entry.
Add a CLIP IP Addr.	Adds a Circuitless IP Interface to a device.
Run Analysis	Runs an analysis to check for inconsistencies in the vST configuration, and VTEP source address configurations.
Show filter data for the store	Shows the field details and columns on which you applied the search filter.
Clear all filters	Clears all the filters that you applied on the column search.

Starting VXLAN view

Use the following procedure to launch the VXLAN view.

Procedure

Select **Configuration > VXLAN**

VXLAN Manager view

The VXLAN Manager user interface provides two types of views:

- VTEP — a device-centric view that you can use to view the device level settings for VXLAN.
- VNI — a VNID-centric view that you can use to view the VNI configured in the discovered devices in the network.

VXLAN Manager device view

The VTEP view displays a summary of all VXLAN capable devices in the current context. Fields, except for VTEP VRF and VTEP Source Address, are read only.

The following image is an example of the VXLAN Manager VTEP view.

Device Name	Device Address	Device Type	Operational Mode	vIST Peer	vIST VLAN IP	VTEP VRF	VTEP Source Address	Remote VTEPs	Discovered On
BLR-VSP-8284XSQ	10.133.139.107	mVSP8284XSQ	Base Interworking	0.0.0.0		I3core	192.107.107.107	...	2016-11-18 15:22:17 IST
BLR-VSP-7254XTQ	10.133.139.127	mVSP7254XTQ	Full Interworking	9.9.9.1	99 (9.9.9.2)	I3core	192.127.127.127	...	2016-11-18 15:22:17 IST

Editing the VTEPs Avaya Devices table

Use this procedure to make changes to the VETPs Avaya Devices table using inline editing. You can change the information for VTEP VRF and VTEP Source Address only.

Procedure

1. Select **Configuration > VXLAN**.
2. To edit the VTEP VRF field, double-click in the cell, and enter a value.
3. To edit the VTEP Source Address field, double-click in the cell, and enter a value.
4. Click **Save the changes to the Device**.

Avaya devices table field descriptions

Name	Description
Device Address	Specifies the IP address of the device.
Device Name	Specifies the name of the device.
Device Type	Specifies the type of device.
Operational Mode	Specifies the VXLAN gateway current operation mode. The options are: <ul style="list-style-type: none"> • Base interworking • Full Interworking
vIST Peer	Specifies the virtual IST Peer IP address.
vIST VLAN IP	Specifies the virtual IST VLAN IP address.
VTEP VRF	Specifies the VRF to which the VTEP source address belongs to.
VTEP Source Address	Specifies the VXLAN tunnel end point source IP address which can be a CLIP or Brouter. To disable VXLAN tunnels, enter the value 0.0.0.0.
Remote VTEP	Lists the remote VTEPs.
Discovered On	If the last discovery failed for a device, the timestamp will be older than the last discovery time shown in the status bar.

Adding a CLIP interface

Add a Circuitless IP (CLIP) interface to use as the Tunnel Source Address for a Fabric Extend device or a VXLAN device.

*** Note:**

Tunnel Source IP Address is either a CLIP interface address or a router interface address. In EFO, Fabric Extend and VXLAN support the creation of the required CLIP interface address only.

You can use the Add CLIP dialog box to add as many CLIP interfaces as you need to any device before you close the dialog box.

Procedure

1. Perform one of the following actions:
 - To add a CLIP interface with Fabric Extend, select **Configuration > Fabric Extend**, and in the navigation pane, select **Devices**.
 - To add a CLIP interface with VXLAN, select **Configuration > VXLAN**, and select **Avaya Devices**.
2. In the contents pane toolbar, click **Add a CLIP IP Addr.**
3. Select the device for which you want to create the interface.
4. Select an interface Id.
5. Select a VRF.
6. Enter a CLIP IP address.
7. Enter a CLIP Mask address.
8. Click **Add**.
9. **(Optional)** Repeat steps 3 through 8 to add more CLIP interfaces.
10. Close the **Add Circuitless IP Interface** dialog box.

Add Circuitless IP interface field descriptions

The following table describes the fields in the Add Circuitless IP Interface dialog box.

Name	Description
Select Device	Specifies the device for which to create a CLIP interface.
Interface ID	Assigns a number to the CLIP interface. The value must be between 1 and 255. The field is automatically populated with the next available number.

Table continues...

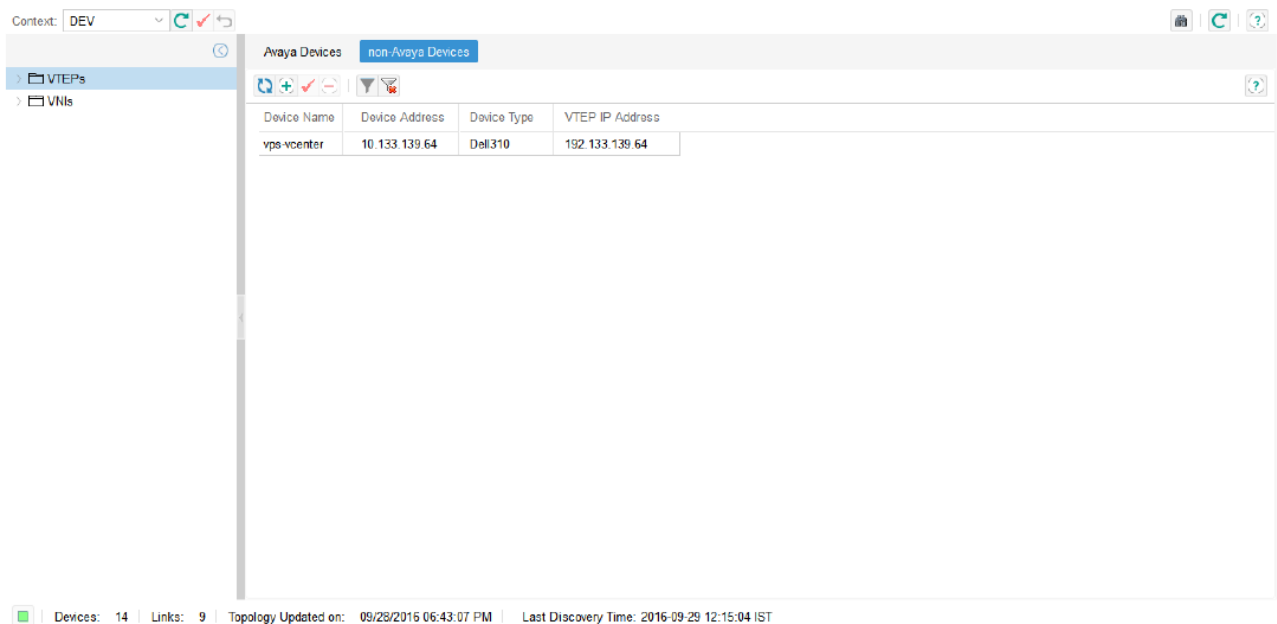
Name	Description
Select VRF	Associates the CLIP interface with a VRF. The default value is GlobalRouter. If you want to use the created CLIP interface as the Tunnel Source Address, associate the CLIP interface to the VRF selected in the table view.
CLIP IP	Specifies the IP address.
CLIP Mask	Specifies the mask.

VXLAN Manager non Avaya device view

VTEP IP Address of the non-Avaya VTEPs will be used in configuring the Remote VTEPs on Avaya Devices. In this view, You can add, update or delete VTEPs.

*** Note:**

The VXLAN Manager does not provide any validation on reachability of non Avaya devices. The following image is view of the the list of non-Avaya VTEPs configured by the administrator.



Non Avaya device view table field descriptions

Name	Description
Device Address	Specifies the IP address of the non-Avaya device.
Device Name	Specifies the name of the non-Avaya device.

Table continues...

Name	Description
Device Type	Specifies the type of device.
VTEP IP Address	Specifies the VTEP IP address of the non-Avaya device.

Adding a non Avaya VTEP

Use the following procedure to add a non Avaya VTEP with VXLAN Manager.

Procedure

1. Select **Configuration > VXLAN**.
2. Select the **non-Avaya Devices** tab.
3. Click **Add a non Avaya Device**.
4. Enter the device address.
5. Enter the device name.
6. Enter the device type
7. Enter the VTEP IP address.
8. Click **Add**.

Add non-Avaya device dialog box field descriptions

Field	Description
Device Address	Specifies the IP address of the non-Avaya device.
Device Name	Specifies the name of the non-Avaya device.
Device Type	Specifies the type of device.
VTEP IP Address	Specifies the VTEP IP address of the non-Avaya device.

Viewing a remote VTEP

Use the following procedure to view the remote VTEPs configured in a device.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, expand the **VTEPs** folder, and select a device.
3. Select the **Remote VTEPs** tab.

Remote VTEPs table field descriptions

Field	Description
VTEP ID	Specifies the VTEP ID that uniquely identifies the VXLAN tunnel endpoint.
VTEP IP	Specifies the destination IP address of the VTEP tunnel.
VTEP Name	Specifies the name that is assigned, by the administrator, for the VXLAN tunnel endpoint. The default name is VTEP-<#ID>-.
Next Hop VRF Name	Specifies the next hop VRF name to reach the remote VTEP
Device Name	Specifies the name of the device.
Device Type	Specifies the device type.
Device Address	Specifies the IP address of the device.

Adding a remote VTEP

Use the following procedure to add a VXLAN capable device as a remote VTEP on a selected VTEP.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VTEPs** folder, and select a device.
3. Select the **Remote VTEPs** tab.
4. Click **Add a Remote VTEP**.
5. Select a VTEP ID.
6. Select a device.
7. Enter a VTEP Name.
8. Click **Add**.

Add remote VTEP dialog box field descriptions

Field	Description
VTEP ID	Enter a VTEP ID that uniquely identifies the VXLAN tunnel end point.
Select Device	Specify a device to which you want to add a remote VTEP.
VTEP Name	Enter a VTEP name for the VXLAN tunnel end point.

Viewing VTEP VNI ELAN end points

Use the following procedure to view the VTEP VNI ELAN end points configured on a device. The information in this table is read-only.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VTEPs** folder, and select a device.
3. Select the **VNIs** tab.

VTEP VNI ELAN end points table field descriptions

Field	Description
VNID	Specifies the VNID of the VXLAN tunnel end point.
ISID	Specifies the I-SID of the VXLAN end point.
Remote VTEPs	Specifies the remote VTEPs associated with the VNID and ISID mapping.

Viewing a VNI

Use the following procedure to view VNIs configured on a discovered VXLAN capable device.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VNIs** folder.

VNIs table field descriptions

Field	Description
VNID	Specifies the VNID of the VXLAN tunnel end point.
I-SID	Specifies the I-SID of this VXLAN end point.
Device List	Specifies the devices on which VNID is configured.

Adding a VNID on a device

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VNIs** folder.
3. Click **Add a VNID**.

4. Enter or select a VNID.
5. In the Devices table, click in the ISID field and enter a value.
You can select one device, or more than one device to add to the VNI you create.
6. Click **Create**.

Add VNID dialog box field descriptions

Name	Description
VNID	Specifies the VNID of the VXLAN tunnel end point.
ISID	Specifies the I-SID of the VXLAN end point.
Devices	Specifies the devices on which VNID is configured.

Deleting a VNID from a device

Use the following procedure to delete a VNID from a device. The VXLAN manager internally unmaps the VNID to the I-SID mappings on the device and then deletes the VNID from the device.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VNIs** folder, and select a VNID folder.
3. In the VNIs table, select a VNID.
4. Click **Delete VNID**.
5. To confirm deletion of the VNID, click **Yes**.

Viewing VNID configured devices

Use this procedure to view devices that have VNID configured on VXLAN capable devices. From this view, you can also fix VNID inconsistencies, and run a diagnostic for loop detection.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VNIs** folder, and select a VNID folder.
3. **(Optional)** To fix VNID inconsistencies, click **Fix any VNID inconsistency**.
4. **(Optional)** To run a diagnostic for loop detection, click **Run Diagnostics for loop detection**.

VETPs table field descriptions

Field	Description
ISID	Specifies the ISID of the VXLAN end point.
Device Address	Specifies the IP address of the device that is VNID configured.
Device Name	Specifies the name of the device that is VNID configured.
ISIS Area	Specifies the manually configured ISIS area address for this system.
VTEP Source Address	Specifies the VXLAN tunnel end point source IP address.
vIST Peer IP	Specifies the Virtual IST Peer IP address configured on the device. If the value is not configured, the default is 0.0.0.0.
vIST VLAN IP	Specifies the Virtual IST VLAN ID and IP address of the IP interface configured for the VLAN ID. If the value is not configured, the default is blank.
Remote VETPs	Specifies the remote VETPs associated with the VNID and ISID mapping.
Consistent?	Specifies whether or not the device passes the VNID consistency check.

Adding an Avaya device to a VNID

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VNIs** folder, and select a VNID folder.
3. Click **Add a Avaya VTEP to VNID**.
4. Select a device.
5. Enter or select an ISID.
6. Click **Add**.

Add VNID on Device dialog box field descriptions

Name	Description
Select Device	Select a device on which to create the VNID and map the ISID to the VNID.
ISID	A value that uniquely identifies the ISID of this Vxlan end point, and that you want mapped to the VNID.

Deleting an Avaya VTEP from a VNID

Use this procedure to remove an Avaya VTEP device to the mapped VNID of the device.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VNI**s folder, and select a VNID folder.
3. In the VTEPs table, click **Delete a Avaya VTEP from VNID**.

Example

Next steps

Adding a non Avaya VTEP to a VNID

Use the following procedure to add a non Avaya VTEP to the VNID. The VTEP you select is added to the existing VNID which is mapped to the VTEP on a device.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VNI**s folder, and select a VNID folder.
3. In the VTEPs table, click **Add non-Avaya VTEP to VNID**.
4. Select a device.
5. Click **Add**.

Add non-Avaya VTEP dialog box field descriptions

Field	Description
Select Device	Select the device to which you want to add the non-Avaya VTEP.

Deleting a non Avaya VTEP device from a VNID

Use the following procedure to remove a non Avaya VTEP device to the mapped VNID of the device.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VNI**s folder, and select a VNID folder.
3. In the VTEPs table, click **Delete non-Avaya VTEP from VNID**.

4. Select a VTEP.
5. Click **Remove**.

Remove non-Avaya VETP dialog box field descriptions

Field	Description
Select Device	Select the device for which you want to remove the non-Avaya VTEP.

Viewing VNID ELAN end points

Use the following procedure to view the VNI ELAN end points configured on the discovered VXLAN capable devices, and view information about the selected device operational mode, base or full internetworking.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VNIs** folder, and select a VNID sub folder.
3. Select a device.

VNI ELANs table field descriptions

Name	Description
C-VID / C-VLAN	Specifies the customer VID of this elan end point. The number 4095 is not used. The number 4096 is reserved for an untagged case.
Port Number	Specifies the port of this elan end point.
MLT	Specifies the MLT of this elan end point.

Adding ELAN end points to the VNID

Use this procedure to add ELAN end points to the VNID on a device.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, select the **VNIs** folder, and select a VNID folder.
3. Select a device.
4. Click **Add a Elan to VNID**.
5. Enter or select a C-VID, or enter the number 4096 for sending untagged packets.

6. Perform one of the following actions. You cannot enter both an MLT and a port number.
 - Enter or select an MLT
 - Enter a port number.
7. Click **Add**.

Add VNID ELAN dialog box field descriptions

Name	Description
C-VID	Specifies the customer VID of this ELAN end point. The number 4095 is not used. You can use the number 4096 to send untagged packets.
Select MLT	Select an MLT, which is already configured on the device located in the left navigation pane, that you want associated with the C-VID.
Port Number	Enter the port number that you want associated with the C-VID. The port number must be a number separated by a backward slash (/).

Deleting an ELAN from a VNID

Use the following procedure to delete an ELAN endpoint from a VNI on a device.

Procedure

1. Select **Configuration > VXLAN**.
2. In the navigation pane, expand the VNIs folder, and select a VNID folder.
3. Select a device.
4. Click **Delete**.
5. To confirm deletion of the ELAN, click **Yes**.

Chapter 16: Managing Multimedia

About Multimedia

The Multimedia manages Auto Detection/Auto Configuration (ADAC) and 802.1ab parameters of the 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.

The Multimedia view supports the following 802.1ab parameters:

- LLDP: Global, Port Configuration, and Neighbor
- Port dot1: Local Port, Local Vlan Protocol, and Local Vlan Name
- Port dot3: Local Power, Local Link Aggregate, and Local Max Frame
- Port med: Local Media Policy, Local Location, Local XPoE PSE Port, Neighbor Capabilities, and Neighbor Inventory

Multimedia requires one or more of the following approved vendor devices:

- ERS 2500 v4.1.0
- ERS 4500 v5.1.0
- ERS 55xx v5.0.0
- ERS 8300 v3.0
- E0/470 v3.6
- VSP 7000 v10.2 and above
- ERS 3500 v5.1 and above

Multimedia view

You launch the Multimedia view from the Configuration tab.

After you select the Multimedia for the first time, the Multimedia performs a discovery of devices, and displays the progress of the discovery.

The Multimedia UI is composed of two parts, presented side by side.

- The Multimedia navigation tree—Displays on 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 Content Panel—Displays to the right of the Multimedia navigation tree. After you select a node in the Multimedia navigation tree, information about the node displays in the Multimedia content pane.

Starting the Multimedia

Perform the following procedure to launch the Multimedia.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. Click **Ok** to view Multimedia tab.

OR

3. Click **Details** to view errors or warnings, if any exist.

Actions

With the Multimedia view, you can perform manager actions and table actions.





Manager actions

You can perform the following actions in the Multimedia context. The following table identifies the available manager actions in the Multimedia.

Tool	Toolbar button	Description
Context		Selects the available groups assigned to the current logged in user.
Save Context		Saves or updates the current device group context.
Revert to Current Context		Reverts to the current device group context.
Refresh Groups		Refreshes data for the device group context.
Discover Multimedia		Discovers device information.
Preferences		Configures Multimedia preferences.
Help		Opens online help.

Table actions

You can perform the following actions in the Multimedia single table context. Not all operations are available for all tables. The following table identifies the available table actions in the Multimedia.

Tool	Toolbar button	Description
Add new entry		Adds a new entry.
Delete entry		Deletes an entry.
Apply changes		Applies changes.
Revert changes		Reverts changes.

Performing a Multimedia discovery

Perform the following procedure to discover devices in the Multimedia view.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Multimedia menu bar, mouse over the buttons on the top right, and click **Discover Multimedia**.

The Multimedia discovery progress bar appears.

3. To view details of the discovery, click **Details**.
4. After the discovery is complete, click **OK**.

Selecting preferences for the Multimedia

Perform the following procedure to manage user preferences for the Multimedia.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Multimedia menu bar, mouse over the buttons on the top right, and click **Preferences**.

The Multimedia Preferences dialog box appears.

3. 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 the Multimedia preferences are:
 - Manage by device family—Allows you to choose the supported device families.
 - 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.

4. Click **OK**.

Adding a table row

Perform the following procedure to add a table row in the Multimedia ADAC MAC Address Ranges table.

 **Note:**

Not all operations are available for all tables.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the navigation pane, select **Multimedia Networks > ADAC**.
3. Select the device, from which you want to add a new entry, from the **ADAC** tree.
4. Click on **MAC Address Ranges**.
5. In the toolbar below, mouse over the icons, and click **Add new entry**.

The Add New Entry dialog box appears.

6. In the **Low End Index** field, enter a value.
7. In the **High End Index** field, enter a value.
8. Click **Save**.

Deleting a table row

Perform the following procedure to delete a table row in the Multimedia ADAC MAC Address Ranges table.

 **Note:**

Not all operations are available for all tables.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the navigation pane, select **Multimedia Networks > ADAC**.
3. Select the device, from which you want to delete an entry, from the **ADAC** tree.
4. Click on **MAC Address Ranges**.
5. Click on the device you want to delete.
6. In the toolbar below, mouse over the icons, and click **Delete entry**.

7. In the Remove dialog box, click **Yes**.

Navigation tree structure

The navigation tree of the Multimedia contains the Multimedia Networks root node. The Multimedia Networks node contains the following sub-nodes.

- ADAC—Displays nodes for discovered devices that have Auto Detection/Auto Configuration (ADAC) enabled.
- 802.1ab—Displays the information by dividing the information into sub-nodes for the following network Layer 2 discovery protocols: 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.

Using tables to change device configuration

The Multimedia data for a device appears in tables in the contents pane.

To access the Multimedia 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.

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 have configuration information for the parts of the ADAC tables.

Configuring the Multimedia ADAC Global table

Use the following procedure to display and configure nodes with Auto Detection/Auto Configuration (ADAC) enabled in the Global table.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > ADAC**.
3. Select the device you want to view by clicking on the device.

A table appears to the right of the tree.

4. Click **Global** to view the Global table.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Global table

The following table describes the parts of the ADAC Global table.

Table 70: Global table

Part	Details
Admin Enable	<p>Administratively enables or disables ADAC. The values are True (1) for enabled, and False (2) for disabled.</p> <p>ADAC can be disabled operationally even if it is enabled administratively. To determine if ADAC is enabled operationally, see OperEnable.</p>
Operating Mode	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>If VoiceVlan has the value 0, or if both CallServerPort and UplinkPort have the value 0, you cannot select the untaggedFramesAdvanced and taggedFrames.</p>
Voice VLAN	<p>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.</p>
Notification Control Enable	<p>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.</p>
Call Server Port List	<p>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.</p>
Uplink Port List	<p>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.</p>

Table continues...

Part	Details
	Usually applies if the Call Server is not connected directly to the current module/stack.
MAC Address Range Control	Returns a value of none (1) to indicate that no option is selected. The options are: <ul style="list-style-type: none"> • 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.
Operator Enable	Indicates if ADAC is enabled operationally. The values are True (1) for enabled, and False (2) for disabled. This is a read only parameter. 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.

Configuring the Multimedia ADAC Ports table

Use the following procedure to display and configure nodes with Auto Detection/Auto Configuration (ADAC) enabled in the Ports table.

Procedure

1. S elect **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > ADAC**.
3. Select the device you want to view by clicking on the device.
A table appears to the right of the tree.
4. Click **Ports**.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Ports table

The following table describes the parts of the ADAC Ports table.

Table 71: Ports table

Part	Details
Port	Specifies the port on the interface.
Admin Enable	Enables or disables ADAC on the port. The values are True (1) for enabled, and False (2) for disabled.
Config Status	Status of auto configuration on the port. The values are: <ul style="list-style-type: none"> • configApplied (1)—indicates that the ADAC configuration has been applied

Table continues...

Part	Details
	<ul style="list-style-type: none"> • configNotApplied (2)—indicates ADAC configuration has not been applied.
Tagged Frames Pvid	<p>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.</p> <p>For example:</p> <ul style="list-style-type: none"> • AdminEnable is True • OperatingMode, ADAC table, is set to taggedFrames
Tagged Frames Tagging	<p>The tagging value that auto configuration applies to a port. The options are:</p> <ul style="list-style-type: none"> • tagAll - 1 • tagPvidOnly - 2 • untagPvidOnly - 3 • noChange - 4 <p>The port must have auto detection enabled, and must be running in Tagged-Frames operational mode.</p> <p>For example:</p> <ul style="list-style-type: none"> • AdminEnable is True • OperatingMode, ADAC table, is set to taggedFrames
Type	<p>ADAC classification of the port. The options are:</p> <ul style="list-style-type: none"> • 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
Operator Enable	<p>Indicates if auto detection is enabled operationally. The values are True (1) for enabled, and False (2) for disabled.</p>
MAC Detection Enable	<p>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.</p> <p>If auto detection is enabled, and AdminEnable is True, MacDetectionEnable cannot be set to False unless another detection mechanism is enabled on the port.</p> <p>For example: LldpDetectionEnable.</p>
LLDP Detection Enable	<p>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</p>

Table continues...

Part	Details
	<p>detection is enabled, and AdminEnable is True, LldpDetectionEnable cannot be set to False unless another detection mechanism is enabled on the port.</p> <p>For example: MacDetectionEnable.</p>

Configuring the Multimedia ADAC MAC Address Ranges table

Use the following procedure to display and configure nodes with Auto Detection/Auto Configuration (ADAC) enabled in the MAC Address Ranges table.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > ADAC**.
3. Select the device you want to view by clicking on the device.
A table appears to the right of the tree.
4. Click **MAC Address Ranges**.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Mac Address Ranges table

The following table describes the parts of the ADAC Mac Address Ranges table.

Table 72: Mac Ranges table

Part	Details
Low End Index	The low end of the MAC Address range supported by ADAC.
High End Index	The high end of the MAC Address range supported by ADAC.

Resetting the Multimedia ADAC MAC Address Ranges

Perform the following procedure to reset the Multimedia ADAC MAC ranges.

Procedure

1. Select **Configuration > Multimedia** to start the Multimedia view.
2. From the Navigation pane, select **Multimedia Networks > ADAC**.
3. Select the device you want to view by clicking on the device.
4. Click **Global**.
5. In the MAC Address Range Control column, click the down arrow, and select **clearTable**.
6. Click **Apply Changes**.

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 73: ADAC configuration options for devices

Device	Version	Configuration options
ERS 2500	v4.1.0 and later	<ul style="list-style-type: none"> • 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 later	<ul style="list-style-type: none"> • Global and port-by-port. • Port settings override global settings. • ADAC, ADAC Mac Ranges, and ADAC-Ports tables available.
ERS 55xx	v5.0.0	<ul style="list-style-type: none"> • By port only. • ADAC-Ports table available.
ERS 55xx	v5.1.1 and later	<ul style="list-style-type: none"> • Global and port-by-port. • Port settings override global settings. • ADAC, ADAC Mac Ranges, and ADAC-Ports tables available.
ERS 8300	all versions	<ul style="list-style-type: none"> • By port only. • ADAC-Ports table available.
ES 460	v3.6.0	<ul style="list-style-type: none"> • Global and port-by-port. • Port settings override global settings. • ADAC and ADAC-Ports tables available.
ES 470	v3.6.0	<ul style="list-style-type: none"> • Global and port-by-port. • Port settings override global settings. • ADAC and ADAC-Ports tables available.
ES 460	v3.7.0	<ul style="list-style-type: none"> • Global and port-by-port. • Port settings override global settings. • ADAC, ADAC Mac Ranges, and ADAC-Ports tables available.
ES 470	v3.7.0	<ul style="list-style-type: none"> • Global and port-by-port. • Port settings override global settings.

Table continues...

Device	Version	Configuration options
		<ul style="list-style-type: none"> ADAC, ADAC Mac Ranges, and ADAC-Ports tables available.
VSP 7000	v10.2 and later	<ul style="list-style-type: none"> Global and port-by-port. Port settings override global settings. ADAC, ADAC Mac Ranges, and ADAC-Ports tables available.
ERS 35xx	v5.1 and later	<ul style="list-style-type: none"> Global and port-by-port. Port settings override global settings. ADAC, ADAC Mac Ranges, and ADAC-Ports tables available. <p> Note: Functionality for 802.1ab Port dot1 tables and 802.1ab Port dot3 tables is not supported.</p>
All	All	<ul style="list-style-type: none"> A port can support an unlimited number of IP Phones.

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.

Configuring the Multimedia 802.1ab LLDP Global table

Use the following procedure to display and configure the 802.1ab LLDP Global table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > LLDP**.
3. Select the device you want to view by clicking on the device.
A table appears to the right of the tree.
4. Click **Global**.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Global table

The following table describes the LLDP Global table.

Table 74: LLDP Global table

Part	Details
Tx Interval	The interval at which LLDP frames are transmitted on behalf of this LLDP agent.
Tx Hold Multiplier	The time-to-live value expressed as a multiple of Tx Interval.
Reinit Delay	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.
Tx Delay	Indicates the delay, in seconds, between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.
Statistics Remote Tables Last Change Time	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.
Statistics Remote Tables 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.
Statistics Remote Tables 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.
Statistics Remote Tables 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.
Statistics Remote Tables Ageouts	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.
XMed Fast Start Repeat Count	The number of times the fast start LLDPDU are being sent during the activation of the fast start mechanism defined by LLDP-MED.
Notification Interval	Controls the transmission of LLDP notifications.

Configuring the Multimedia 802.1ab LLDP Port Configuration table

Use the following procedure to display and configure the 802.1ab LLDP Port Configuration table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > LLDP**.
3. Select the device you want to view by clicking on the device.

A table appears to the right of the tree.

4. Click **Port Configuration**.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Port Configuration table

The following table describes the LLDP Port Configuration table.

Table 75: LLDP Ports table

Part	Details
Port Number	The index value used to identify the port component, contained in the local chassis with the LLDP agent, associated with the entry.
Admin Status	The administratively desired status of the local LLDP agent. The options are: <ul style="list-style-type: none"> • txOnly (1) • rxOnly (2) • txAndRx (3) • disabled (4)
Notification Enable	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.
TLVs Tx 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.
Xdot1 Vlan Tx Enable	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.
Xdot3 TLVs Tx Enable	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.
XMed Cap Supported	The options are: <ul style="list-style-type: none"> • capabilities • networkPolicy • location • inventory
XMed TLVs Tx Enable	The options are: <ul style="list-style-type: none"> • capabilities

Table continues...

Part	Details
	<ul style="list-style-type: none"> • networkPolicy • location • extendedPSE • extendedPD • inventory
XMed Notify Enable	The options are: <ul style="list-style-type: none"> • true • false

Configuring the Multimedia 802.1ab LLDP Neighbor table

Use the following procedure to display and configure the 802.1ab LLDP Neighbor table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > LLDP**.
3. Select the device you want to view by clicking on the device.
A table appears to the right of the tree.
4. Click **Neighbor**.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Neighbor table

The following table describes the LLDP Neighbor table.

Table 76: LLDP Remote table

Part	Details
Time Mark	A TimeFilter for this entry.
Local Port Number	The index value used to identify the port component, contained in the local chassis with the LLDP agent, associated with this entry. Local Port Number 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.
Chassis Id Subtype	The type of encoding used to identify the chassis associated with the remote system.

Table continues...

Part	Details
Chassis Id	The string value used to identify the chassis component associated with the remote system.
System Cap Supported	The bitmap value used to identify which system capabilities are supported on the remote system.
System Cap Enabled	The bitmap value used to identify which system capabilities are enabled on the remote system.
System Name	The string value used to identify the system name of the remote system.
System Description	The string value used to identify the system description of the remote system.
Port Id Subtype	The type of port identifier encoding used in the associated Port Id.
Port Id	The string value used to identify the port component associated with the remote system.
Port Description	The string value used to identify the description of the given port associated with the remote system.

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 dot1** folder in the navigation tree.

The following sections list and describe the 802.1ab Port dot1 tables.

Configuring the Multimedia 802.1ab Port dot1 Local Port table

Use the following procedure to display and configure the 802.1ab Port dot1 Local Port table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > Port dot1**.
3. Select the device you want to view by clicking on the device.
A table appears to the right of the tree.
4. Click **Local Port**.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Local Port Id table

The following table describes the Local Port Id table.

Table 77: Local VLAN Id table

Part	Details
Port Number	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
Vlan Id	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.

Configuring the Multimedia 802.1ab Port dot1 Local Vlan Protocol table

Use the following procedure to display and configure the 802.1ab Port dot1 Local Vlan Protocol table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > Port dot1**.
3. Select the device you want to view by clicking on the device.
A table appears to the right of the tree.
4. Click **Local Vlan Protocol**.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Local Vlan Protocol table

The following table describes the Local Vlan Protocol table.

Table 78: Local Protocol VLAN table

Part	Details
Port Number	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
Vlan Id	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
Supported	The truth-value that indicates if the given port, associated with the local system, supports port and protocol VLANs.
Enabled	The truth-value that indicates if the port and protocol VLANs are enabled on the given port associated with the local system.
Tx Enable	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.

Configuring the Multimedia 802.1ab Port dot1 Local Vlan Name table

Use the following procedure to display and configure the 802.1ab Port dot1 Local Vlan Name table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > Port dot1**.
3. Select the device you want to view by clicking on the device.
A table appears to the right of the tree.
4. Click **Local Vlan Name**.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Local VLAN Name table

The following table describes the Local VLAN Name table.

Table 79: Local VLAN Name table

Part	Details
Port Number	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
Vlan Id	The integer value that identifies the IEEE 802.1Q VLAN IDs with which the given port is compatible.
Name	The string value that identifies the VLAN name identified by the Vlan Id associated with the given port on the local system. VLAN name must contain the value of the dot1QVLANStaticName object, as defined in IETF RFC 2674, identified with the given VlanId.
Tx Enable	The Boolean value that indicates if the corresponding Local System VLAN name instance is transmitted on the port defined by the given VLAN name.

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.

The sections list and describe the 802.1ab Port dot3 tables.

Configuring the Multimedia 802.1ab Port dot3 Local Power table

Use the following procedure to display and configure the 802.1ab Port dot3 Local Power table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > Port dot3**.
3. Select the device you want to view by clicking on the device.
A table appears to the right of the tree.
4. Click **Local Power**.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Local Power table

The following table describes the 802.1ab Port dot3 Local Power tables.

Table 80: Power tables

Table	Details
Port Number	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
Port Class	The value that identifies the port Class of the given port associated with the local system.
MDI Supported	The truth-value that indicates if the MDI power is supported on the given port associated with the local system.
MDI Enabled	The truth-value that identifies if MDI power is enabled on the given port associated with the local system.
Pair Controllable	Contains the value of the pethPsePortPowerPairs object, as defined in IETF RFC 3621, associated with the given port on the local system.
Pairs	Contains the value of the pethPsePortPowerPairs object, as defined in IETF RFC 3621, associated with the given port on the local system.
Class	Contains the value of the pethPsePortPowerClassifications object, as defined in IETF RFC 3621, associated with the given port on the local system.

Configuring the Multimedia 802.1ab Port dot3 Local Link Aggregate table

Use the following procedure to display and configure the 802.1ab Port dot3 Local Link Aggregate table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > Port dot3**.
3. Select the device you want to view by clicking on the device.
A table appears to the right of the tree.

4. Click **Local Link Aggregate**.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Local Link Aggregate table

The following table describes the 802.1ab Port dot3 Local Link Aggregate table.

Table 81: Local Link aggregate table

Part	Details
Port Number	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
Status	The bitmap value contains the link aggregation capabilities and the current aggregation status of the link.
Port Id	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.

Configuring the Multimedia 802.1ab Port dot3 Local Max Frame table

Use the following procedure to display and configure the 802.1ab Port dot3 Local Max Frame table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > Port dot3**.
3. Select the device you want to view by clicking on the device.
A table appears to the right of the tree.
4. Click **Local Max Frame**.
5. Click in the cell you wish to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes you make.

Local Max Frame table

The following table describes the 802.1ab Port dot3 Local Max Frame table.

Table 82: Local Max Frame table

Part	Details
Port Number	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
Max Frame Size	An integer value that indicates the maximum supported frame size in octets on the given port of the local system.

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.

The following sections list and describe the 802.1ab Port med tables.

Displaying Multimedia 802.1ab Port med Local Media Policy table

Use the following procedure to display the 802.1ab Port med Local Media Policy table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > Port med**.
3. Select the device you want to view by clicking on the device.

A table appears in the contents pane.

4. Click **Local Media Policy** to display the Local Media Policy table.

Local Media Policy table

The following table describes the Local Media Policy table.

Table 83: Policy table

Part	Details
Port Number	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
Application type	Specifies the application type.
Vlan Id	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.
Priority	Contains the value of the 802.1p priority, which is associated with the given port on the local system.
Differentiated Service Code Point	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.
Unknown	Indicates whether or not the network policy for the specified application type is currently unknown. The values are: <ul style="list-style-type: none"> • 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), the system ignores the VLAN ID, the layer 2 priority, and the DSCP value fields.

Table continues...

Part	Details
Tagged	<p>Indicates whether or not the application is using a tagged VLAN. The values are:</p> <ul style="list-style-type: none"> • 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. <p>If the value is False (2), the system ignores the VLAN ID and the Layer 2 priority fields, and only the DSCP value has relevance.</p>

Displaying Multimedia 802.1ab Port med Local Location table

Use the following procedure to display the 802.1ab Port med Local Location table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > Port med**.
3. Select the device you want to view by clicking on the device.
A table appears in the contents pane.
4. Click **Local Location** to display the Local Location table.
5. **(Optional)** Click in the **Info** to update.
6. Click **Apply Changes** button, on the top left of the table, to apply the changes.

Local Location table

The following table describes the Local Location table.

Table 84: Location table

Part	Details
Port Number	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
Subtype	The location subtype advertised by the local device.
Info	The location information. Parsing of the location information is dependent upon the location subtype, as defined by the value of the LocationSubtype.

Displaying Multimedia 802.1ab Port med Local XPoE PSE Port table

Use the following procedure to display the 802.1ab Port med Local XPoE PSE Port table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.

2. From the Navigation pane, select **Multimedia Networks > 802.1ab > Port med.**
3. Select the device you want to view by clicking on the device.

A table appears in the content pane.

4. Click **Local XPoE PSE Port** to display the Local XPoE PSE Port table.

Local XPoE PSE Port table

The following table describes the Local XPoE PSE Port table.

Table 85: PoE PSE table

Part	Details
Port Number	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry.
Power Available	Contains the value of the power available from the PSE from this port, expressed in units of 0.1 watts.
PD Priority	Reflects the PD power priority that is advertised on this PSE port. The values are: <ul style="list-style-type: none"> • unknown - 1 • critical - 2 • high - 3 • low - 4

Displaying Multimedia 802.1ab Port med Neighbor Capabilities table

Use the following procedure to display the 802.1ab Port med Neighbor Capabilities table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > Port med.**
3. Select the device you want to view by clicking on the device.

A table appears in the contents pane.

4. Click **Neighbor Capabilities** to display the Neighbor Capabilities table.

Neighbor Capabilities table

The following table describes the Neighbor Capabilities table.

Table 86: Capabilities table

Part	Details
Time Mark	A TimeFilter for this entry. For more information, see the TimeFilter textual convention in IETF RFC 2021.
Local Port Number	The index value that identifies the port component, contained in the local chassis with the LLDP agent, associated with the entry. The IldpRemLocalPortNum 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.
Supported	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.
Current	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.
Device Class	Device Class as advertised by the device remotely connected to the port.

Displaying the Multimedia 802.1ab Port med Neighbor Inventory table

Use the following procedure to display the 802.1ab Port med Neighbor Inventory table information.

Procedure

1. Select **Configuration > Multimedia** to start Multimedia.
2. From the Navigation pane, select **Multimedia Networks > 802.1ab > Port med**.
3. Select the device you want to view by clicking on the device.

A table appears in the contents pane.

4. Click **Neighbor Inventory** to display the Neighbor Inventory table.

Neighbor Inventory table

The following table describes the Neighbor Inventory table.

Table 87: Inventory table

Part	Details
Time Mark	A TimeFilter for the entry. For more information, see the TimeFilter textual convention in IETF RFC 2021.

Table continues...

Part	Details
Local Port Number	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.
Index	Represents an arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated remote system.
Hardware Revision	The vendor-specific hardware revision string as advertised by the remote endpoint.
Firmware Revision	The vendor-specific firmware revision string as advertised by the remote endpoint.
Software Revision	The vendor-specific software revision string as advertised by the remote endpoint.
Serial Number	The vendor-specific serial number as advertised by the remote endpoint.
Manufacturer Name	The vendor-specific manufacturer name as advertised by the remote endpoint.
Model Name	The vendor-specific model name as advertised by the remote endpoint.
Asset Id	The vendor-specific asset tracking identifier as advertised by the remote endpoint.

Chapter 17: Managing Trap and Log Registration

About Trap/Log Registration

You can use the Trap/Log Registration view to configure and view traps, notifications, and the system log. The Trap/Log Registration view combines the functionality of the original Trap Receiver and Log Manager, and also adds traps, notifications, and syslog configuration.

You can configure the network to which the traps are sent with the Trap/Log Registration. 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.

Starting Trap/Log Registration

Procedure

1. Select **Configuration > Trap/Log Registration**.

The system automatically launches the device discovery.

2. In the device discovery operation result dialog box, click **Ok** to view Trap/Log Registration tab.

Trap/Log Registration view

The following figure displays the Trap/Log Registration view.

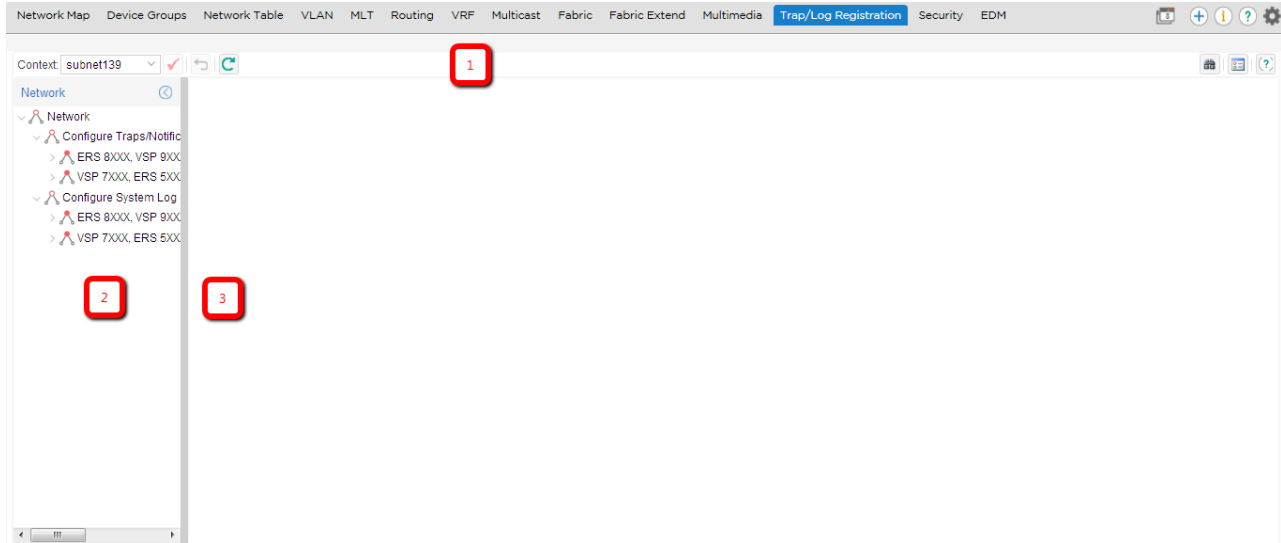


Figure 39: Trap/Log Registration

The following table describes the parts of the Trap/Log Registration view.




Table 88: Parts of the Trap/Log Registration view

Part	Description
1. Tool bar	Provides quick access to commonly used commands in the Trap/Log Registration view.
2. Navigation pane	Allows you to navigate to the settings for the current network devices.
3. Contents pane	Displays details of the folder selected on the navigation pane.

Trap/Log Registration toolbar

Icon	Name	Description
Context: subnet139	Context	Use this option to select the available groups assigned to the current logged in user. After you change the context, a notification is sent to all opened configuration views in the system with the same logged in user. All opened views are refreshed after receiving this notification.
✓	Save Context	Use this option to save the context.
↶	Revert to Current Context	Use this option to revert to the current context.

Table continues...





Icon	Name	Description
	Refresh Groups	Use this option to view the new groups added to the current logged in user.
	Discover Trap/Log	Use this option to discover the devices for the Trap/Log Registration.
	Preferences	Use this option to set the preferences for working with the Trap/Log Registration.

Trap/Log Registration navigation pane

The Trap/Log Registration navigation pane displays a hierarchical folder tree that you can use to navigate to the groups.

Trap/Log Registration contents pane

The contents pane displays detailed information for the element selected in the navigation pane.

Tool bar button	Tool	Description
	Add new entry	Adds a new entry.
	Delete entry	Deletes an entry.
	Apply changes	Applies changes.
	Revert changes	Reverts changes.

Discovering devices

About this task

You can discover the information in the Trap/Log Registration view 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 Registration.

Procedure

1. Select **Configuration > Trap/Log Registration**.
2. Click on the **Discover Trap/Log** button in the tool bar, on the top left.

Result

The system initiates the device discovery, and displays the operation result errors and warnings.

Displaying Preferences

About this task

You can select the specific set of assigned devices to be used in the Trap/Log Registration discovery process in the Trap/Log Registration Preferences dialog box, based on several criteria.

Procedure

1. Select **Configuration > Trap/Log Registration**.
2. Click **Preferences** in the tool bar, on the top right of the content pane.

Result

The Trap/Log Registration preferences dialog box displays.

For more information on editing the Preferences, see [Setting File Inventory preferences](#) on page 441.

Traps configuration

The following sections provide instructions on configuring traps for ERS, VSP, and WC devices.

Configuring Trap Receivers for ERS, VSP, and WC devices

About this task

Perform the following procedure to configure trap/logs for the following devices:

- ERS 8XXX
- APLS
- VSP 4XXX
- VSP 72XX
- VSP 8XXX
- VSP 9XXX
- VSP 7XXX
- ERS 5XXX/4XXX/35XX/36XX
- WC 8XXX

Procedure

1. Select **Configuration > Trap/Log Registration**.
2. In the Trap/Log Registration navigation tree, click **Configure Traps/Notifications**.
3. Select one of the following folders:
 - **VSP 7XXX, ERS 5XXX/4XXX/35XX/36XX, WC8XXX**

- **ERS 8XXX, APLS, VSP 4XXX, VSP 72XX, VSP 8XXX, VSP 9XXX**
4. Choose the device to configure trap receivers.
 5. In the contents pane, click the **Trap Receivers** tab.
 6. To add a trap receiver entry for a device, click **Add**.
 7. In the Insert Trap Receivers window, complete the fields as required.
 8. Click **Save**.
 9. **(Optional)** To edit the exiting **Trap Receivers** table information, click in the corresponding cell and modify the values.
 10. **(Optional)** Click **Apply changes** from the top left tool bar in the content pane.

Insert Trap Receiver field descriptions

Field	Description
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

About this task

Perform the following procedure to configure Target Address Table for the following devices:

- ERS 8XXX
- APLS
- VSP 4XXX
- VSP 72XX
- VSP 8XXX
- VSP 9XXX
- VSP 7XXX
- ERS 5XXX/4XXX/35XX/36XX
- WC 8XXX

Procedure

1. Select **Configuration > Trap/Log Registration**.
2. In the Trap/Log Registration navigation tree, click **Configure Traps/Notifications**.
3. Select one of the following folders:
 - **VSP 7XXX, ERS 5XXX/4XXX/35XX/36XX, WC8XXX**

• **ERS 8XXX, APLS, VSP 4XXX, VSP 72XX, VSP 8XXX, VSP 9XXX**

4. Choose the device for which you want to configure target addresses.
5. In the contents pane, click the **Target Address Table** tab.
6. To add a target address entry for a device, click the **Add** icon on the top left of the tool bar menu in the content pane.
7. In the Target Address Table window, enter the values in the fields as required.

Insert Target Address Table

Properties

Name: !

TargetAddress: ! [IP Address:port]

Timeout: [1/100 secs]

RetryCount: [0 - 255]

TagList: !

Params: !

StorageType:


Devices

<input type="checkbox"/>	Device
<input type="checkbox"/>	10.133.139.100
<input type="checkbox"/>	10.133.139.102
<input type="checkbox"/>	10.133.139.125

Save Cancel Help

8. Click **Save** to add the newly created Target Address entry to the table in the contents pane.
9. **(Optional)** To edit the existing **Target Address Table** information, click in the corresponding cell and modify the values in the fields as required.
10. **(Optional)** Click **Apply changes** from the top left tool bar in the content pane.

Target Address Table field descriptions

Name	Description
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.  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

About this task

Perform the following procedure to configure Target Params Table for the following devices:

- ERS 8XXX
- APLS
- VSP 4XXX
- VSP 72XX
- VSP 8XXX
- VSP 9XXX
- VSP 7XXX
- ERS 5XXX/4XXX/35XX/36XX
- WC 8XXX

Procedure

1. Select **Configuration > Trap/Log Registration**.
2. In the Trap/Log Registration navigation tree, click **Configure Traps/Notifications**.

3. Select one of the following folders:
 - **VSP 7XXX, ERS 5XXX/4XXX/35XX/36XX, WC8XXX**
 - **ERS 8XXX, APLS, VSP 4XXX, VSP 72XX, VSP 8XXX, VSP 9XXX**
4. Choose the device for which you want to configure target parameters.
5. In the contents pane, click the **Target Params Table** tab.
6. To add a target parameter entry for a device, click the **Add** icon on the top left of the tool bar menu in the content pane.
7. In the Target Params Table window, enter the values in the fields as required.

Insert Target Params Table

Properties

Name: ⓘ

MPModel:

SecurityModel:

SecurityName: ⓘ

SecurityLevel:

StorageType:

Devices

<input type="checkbox"/>	Device
<input type="checkbox"/>	10.133.139.100
<input type="checkbox"/>	10.133.139.102
<input type="checkbox"/>	10.133.139.125

Save Cancel Help

8. Click **Save** to add the newly created Target Params entry to the table in the contents pane.
9. **(Optional)** To edit the exiting **Target Params Table** information, click in the corresponding cell and modify the values in the fields as required.
10. **(Optional)** Click **Apply changes** from the top left tool bar in the content pane.

Target Params table field descriptions

Field	Description
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.
StorageType	Specifies the storage type. Default value is non-volatile.

Configuring Notify Table for ERS, VSP, and WC devices

About this task

Perform the following procedure to configure Notify Table for the following devices:

- ERS 5xxx/4xxx/35xx
- VSP 7xxx
- WC 8xxx

Procedure

1. Select **Configuration > Trap/Log Registration**.
2. In the Trap/Log Registration navigation tree, click **Configure Traps/Notifications**.
3. Select **VSP 7XXX, ERS 5XXX/4XXX/35XX/36XX, WC8XXX**.
4. Choose the device for which you want to configure notifications.
5. In the contents pane, click the **Notify Table** tab.

Result

The Notify Table window displays.

Adding a notification

Procedure

1. Select **Configuration > Trap/Log Registration**.

2. Click the **Add** icon in the tool bar.

3. In the Insert Notify Table window, complete the fields as required.
4. Click **Save**.
A row corresponding to the newly created notification is added to the table in the contents pane.
5. To edit the existing **Notify Table** information, click in the corresponding cell and modify the values as required.
6. Click **Apply changes** from the top left tool bar in the content pane.

Job aid

The following table describes the **Notify Table** fields.

Part	Description
Name	Specifies the name.
Tag	Specifies the tagging information.
Type	Specifies the type.
StorageType	Specifies the storage type.

System Log configuration

The Trap/Log Registration 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

About this task

Perform the following procedure to configure system log for the following devices:

- ERS 8XXX
- APLS
- VSP 4XXX
- VSP 72XX
- VSP 8XXX
- VSP 9XXX
- VSP 7XXX
- ERS 5XXX/4XXX/35XX/36XX
- WC 8XXX

Procedure

1. Select **Configuration > Trap/Log Registration**.
2. In the Trap/Log Registration navigation tree, click **Configure System Log**.
3. Select one of the following folders:
 - **VSP 7XXX, ERS 5XXX/4XXX/35XX/36XX, WC8XXX**
 - **ERS 8XXX, APLS, VSP 4XXX, VSP 72XX, VSP 8XXX, VSP 9XXX**
4. Choose the device for which you want to configure the system log.
5. Click **System Log Table** tab.
6. Click **Add** button on the tool bar.
7. Enter values in the fields as required.
8. Click **Save**.
9. To edit the exiting **System Log** information, click in the corresponding cell.
10. Enter the values in the fields as required.
11. Click **Apply changes** from the top left tool bar in the content pane.

Insert System Log Table field descriptions

Field	Description
Id	ID for the syslog host being created.
IpAddress	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.
Facility	The syslog host facility used to identify messages (LOCAL0 to LOCAL7).
Severity	The switch message severity for which syslog messages will be sent. Default value has all values enabled: info, fatal, warning and error.
MapInfoSeverity	The fields that map the switch severity levels to syslog severity. Default value is info.
MapWarningSeverity	The fields that map the switch warning severity levels to syslog severity. Default value is warning.
MapErrorSeverity	The fields that map Ethernet Routing Switch 8000 error severity levels to syslog severity. Default value is error.
MapFatalSeverity	The fields that map the switch 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 devices

About this task

Perform the following procedure to enable the system log for the following devices:

- ERS 8000
- ERS 5xxx/4xxx/35xx
- VSP 9xxx, VSP 7xxx, VSP 4xxx, VSP 8xxx
- WC 8xxx

Procedure

1. In the **Configure System Log** folder, choose a device to enable the system log.
2. In the **System Log** window, click in the **Enable** field, and select the check box.
3. Click **Apply Changes**.

Result

The value in the **Enable** field is updated to **true**.

Chapter 18: Managing Security

About Security

Security provides a centralized location where you can manage access to the devices in your network. You can use Security 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, and changing the passwords on the device itself.

 **Note:**

Security 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 a RADIUS server is not supported. The tab for IPv6 RADIUS server is present, but the add functionality filters out VSP devices.

Supported devices for Security view

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

Table 89: Devices supported for Security view

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
	VOSS (VSP82xx, VSP84xx, VSP72xx, VSP48xx)
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
	VOSS (VSP82xx, VSP84xx, VSP72xx, VSP48xx)
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
	VOSS (VSP82xx, VSP84xx, VSP72xx, VSP48xx)
	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

Table continues...

Type of access	Device type
	Ethernet Routing Switch 45xx/35xx/25xx
	Virtual Services Platform 9xxx/8xxx/7xxx/4xxx
	VOSS (VSP82xx, VSP84xx, VSP72xx, VSP48xx)
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
	VOSS (VSP82xx, VSP84xx, VSP72xx, VSP48xx)

Starting Security view

Procedure

1. Select **Configuration > Security**.
The Security discovery is triggered.
2. In the Security discovery result dialog box, click **Ok**.

Result

The Security view is launched and displayed in the content pane.

Security view

The following figure shows the Security view.

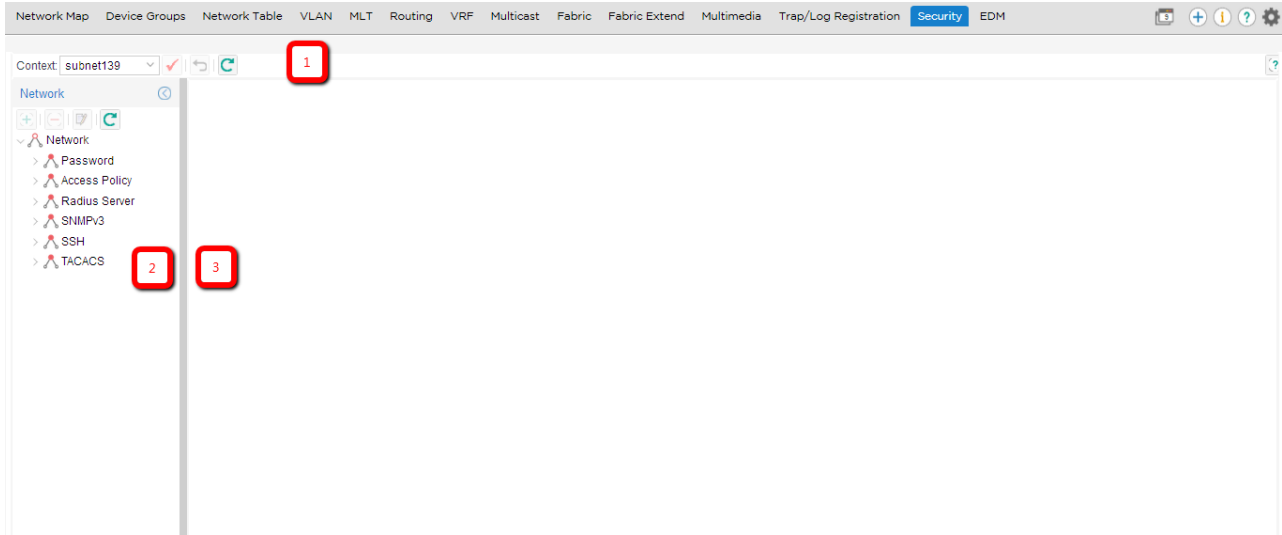


Figure 40: Security view

The following table describes the parts of the Security view.








Table 90: Parts of the Security view

Part	Description
1. Tool bar	Provides quick access to commonly used Security commands.
2. Navigation pane	Allows you to navigate security settings for the current network devices.
3. Contents pane	Displays elements of the folder or element selected on the navigation pane.

Security view toolbar

Icon	Name	Description
Context: subnet139	Context	Use this option to select the available groups assigned to the current logged in user. After you change the context, a notification is sent to all opened configuration views in the system with the same logged in user. All opened views are refreshed after receiving this notification.
✓	Save Context	Use this option to save the context.
↶	Revert to Current Context	Use this option to revert to the current context.

Table continues...

Icon	Name	Description
	Refresh Groups	Use this option to view the new groups added to the current logged in user.
	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.
	Edit	Modifies the current device list contained inside the security group.
	Reload Security Manager	Rediscovered the network and reloads Security with the latest information.
	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.

Security view navigation pane

The Security 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 view.

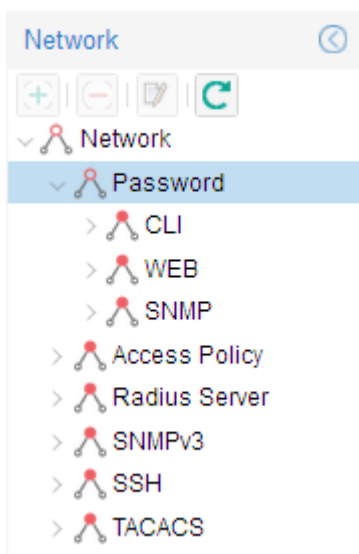


Figure 41: Security view navigation pane

*** Note:**

Not all device groupings are supported on all devices that the system 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.

Security contents pane

The contents 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, SysName, Version, and System Description.

Create and manage security groups

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

Creating security groups

Procedure

1. Select **Configuration > Security**.
2. In the navigation pane, select one of the following application folders and subfolders:
 - Password
 - **CLI, WEB, or SNMP**
 - Access Policy
 - Radius Server
 - SNMPv3
 - SSH
 - TACACS
3. On the toolbar, click **Add**.
4. In the Add Group window, type a new group name in the **Group Name** field.
5. In the device list, choose the devices to include in the new security group. **OR** Click the Device check box to select all devices at the same time.
6. Click **Save**.

Result

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

Add Group field descriptions

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

Adding new devices to a security group

Procedure

1. Select the **Configuration > Security**.
2. In the navigation pane, select one of the following application folders and subfolders:
 - Password
 - **CLI, WEB, or SNMP**
 - Access Policy
 - Radius Server
 - SNMPv3
 - SSH
 - TACACS
3. Click **Add**.

4. Enter the name of the group in the Group Name field.
5. Select the check box corresponding to the devices you want to add to the group.
6. 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 **Cancel**.

Add Group field descriptions

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

Security group settings

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

Reloading Security view

About this task

Security view 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 the Security view.

Procedure

1. Select the **Configuration > Security**.
2. On the Security tool bar, on the top left, click **Reload Security Manager**.
3. Click **Yes** when prompted to confirm reloading.

Result

The system reloads topology information from the network devices and refreshes the Security view with it.

Editing Security Groups

Procedure

1. Select **Configuration > Security**.
2. In the navigation pane, expand the Network folder and select one of the following application folders and subfolders:
 - Password
 - CLI, WEB, or SNMP

- Access Policy
 - Radius Server
 - SNMPv3
 - SSH
 - TACACS
3. Select an existing group under an application folder that requires editing.
 4. Click **Edit** from the toolbar at the top left.
 5. In the Edit group window, edit the name of the group.
 6. Click **Save**.

Deleting security groups

Procedure

1. Select **Configuration > Security**.
2. In the Security navigation pane, select the security group you want to delete.
3. On the toolbar to the top left, click **Delete**.
4. Click **Yes** when prompted to confirm the deletion.

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 view 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

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > Radius Server** folder in the navigation pane, click the folder for the security group for which you want to add a RADIUS server.
3. Click on the Radius Servers tab in the contents pane.
4. On the toolbar, click **Add**.

SM - New Radius Servers Entry
✕

Address	<input type="text"/>	
UsedBy	<input type="text" value="cli"/>	
Priority	<input type="text" value="10"/>	1..10
TimeOut	<input type="text" value="3"/>	1..20
Enable	<input type="text" value="true"/>	
MaxRetries	<input type="text" value="1"/>	0..6
UdpPort	<input type="text" value="1812"/>	1..65536
SecretKey	<input type="text"/>	
AcctEnable	<input type="text" value="true"/>	
AcctUdpPort	<input type="text" value="1813"/>	1..65536
SourceIpAddr	<input type="text"/>	

Devices

	Device
<input type="checkbox"/>	Device
<input checked="" type="checkbox"/>	10.133.139.81
<input type="checkbox"/>	10.133.139.1
<input type="checkbox"/>	10.133.139.95

! 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.

5. Configure the dialog box parameters as appropriate.
6. Click **OK**.

The Security creates a new entry on the **Radius Server** folder.

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

New Radius Servers Entry field descriptions

Field	Description
Address	Specifies the IP address of the new server.

Table continues...

Field	Description
UsedBy	Configures accesses for cli, igap, snmp and eap as they require RADIUS server authentication.
Priority	Specifies the priority between 1 and 10 of the new RADIUS server.
TimeOut	Specifies the number of seconds, between 1 and 10, between retransmissions from the client to the RADIUS server.
Enable	Enables the RADIUS server.
MaxRetries	Specifies the maximum number of retries, between 1 and 6, to allow requests to the server.
UdpPort	Specifies the UDP port number, between 1 and 65536, that the client will use to send requests to the server. 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.

Setting global RADIUS server parameters

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > Radius Server** folder in the navigation pane, open the folder for the security group to set global RADIUS server parameters.
3. In the contents pane, click the **Radius Global** tab.



4. In the Radius Global table, configure the parameters as appropriate.
5. On the Security tool bar, click **Apply Changes**.

Result

The Security view applies the changes only to the changed devices in the security group.

Radius Global tab field descriptions

Field	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

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > Radius Server** folder in the navigation pane, open the folder for the security group for which you want to remove a RADIUS server.
3. Click on the **Radius Servers** tab in the contents pane.
4. Click any cell of the entry for the RADIUS server that you want to remove.
5. On the Tool bar, click **Delete**.
6. Click **Yes** when prompted to delete the selected entry.

Result

The Security view deletes the selected entry from the RADIUS server table.

Configuring TACACS authentication

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

Enabling or disabling TACACS Global

About this task

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

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > TACACS** folder, click on the required security group.
3. Click **TACACS Global** tab.

- In the GlobalEnable column, select **True** to enable and **False** to disable the TACACS globally within the security group.

Adding TACACS servers

Procedure

- Select **Configuration > Security**.
- Under the **Network > TACACS** folder, click on the required security group.
- Select the required device.
- In the Contents pane, click the **TACACS Servers** tab.
- On the Toolbar, click **Insert**.

SM - New TACACS Servers Entry

AddressType	Ipv4	
Address		
PortNumber	49	0..655
ConnectionType	perSessionConnection	
Timeout	10	10..30
Key		
SourceIpInterfaceEnabled	false	
SourceIpInterfaceType	Ipv4	
SourceIpInterface		
Priority	1	

Devices

<input type="checkbox"/>	Device
<input checked="" type="checkbox"/>	10.133.139.1

Save Cancel Help

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

TACAS Server field descriptions

Field	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.
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

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > TACACS** folder, click on the required security group.
3. In the security group folder, click the desired device.
4. In the contents pane, click the **TACACS Servers** tab.
5. In the TACACS Servers table, click a cell of the TACACS Server you want to delete.
6. On the Toolbar, click **Delete**.
7. Click **Yes** when prompted to confirm deletion.

Configuring management access

You can use Security view 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.

SSH configuration

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

Creating SSH security groups

Procedure

1. Select **Configuration > Security**.
2. In the navigation pane, click the **SSH** folder.
3. From the SSH subtype domains, select **ERS8000, ES, ERS 5xxx/4xxx/3xxx/25xx, WC 8xxx, VSP**, or **APLS** compatible devices.
4. From the navigation pane toolbar, click **Add**.
5. In the Add Group window, type a new group name in the **Group Name** field.
6. Select devices.

 **Note:**

Not all SSH capable devices are in Devices list, just the ones filtered to be compliant to the current selected subgroup.

7. Click **Save**.

Result

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

Configuring SSH Bulk Passwords

About this task

In Security, 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 APLS, ERS 49xx, ERS 55xx/35xx/45xx/25xx, Ethernet Switch devices, VSP 4xxx, VSP 70xx, VSP 72xx, VSP 8xxx, 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.

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > SSH** folder in the navigation pane, click the folder for the security group to configure SSH access.
3. In the contents pane, click the **Change Password** tab.

The screenshot shows a web interface for changing passwords. At the top, there's a 'SSH' tab with a 'Change Password' sub-tab. Below this, there are two input fields: 'RWA User Name:' and 'RWA Password:'. Underneath, there are two tabs: 'CLI' (which is selected) and 'WEB'. The 'CLI' tab displays a table with the following columns: 'Access Level', 'User ID', 'Old Password', 'Confirm Old Pass...', 'New Password', and 'Confirm New Pas...'. The table contains two rows: 'RWA' and 'RW'. At the bottom of the interface, there are two buttons: 'Schedule' and 'Change Password'.

4. For ERS 8000 and VSP 9xxx devices, enter the current user name for the devices in the **RWA Username** field.
5. Enter the current password for the devices in the **RWA Password** field.
6. 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.

7. 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.

8. In the **Name** box, enter a name to assign to the task. The name distinguishes this task from other scheduled tasks for easy identification.9. 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.

10. In the **Date** box, set the date and time you want Scheduler Server to execute the task.11. Click **Set**.

Result

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

Schedule Password Change field descriptions

Field	Description
Task Name	Specifies the name of the task.
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.

Table continues...

Field	Description
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 Procedure

1. Select **Configuration > Security**.
2. Under the **Network > SSH** folder in the navigation pane, click the folder for the security group to configure SSH properties.
3. In the contents pane, click the **SSH** tab.
4. In the SSH table, modify the configurable fields as required, then click **Apply Changes**.

SSH table field descriptions

Name	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.

Table continues...

Name	Description
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, WC 8xxx, and Ethernet Switch security groups

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > SSH** folder in the navigation pane, click the folder for the security group to configure SSH properties.
3. In the contents pane, click the **SSH** tab.
4. Select and modify any of the fields in the table.
5. Click **Apply Changes**.

SSH tab field descriptions

Field	Description
MaxSession	Specifies the maximum number of sessions.
Address	Specifies the IP address of 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.
RsaAuth	Enables or disables RSA authentication. Default is enabled.
PassAuth	Enables or disables password authentication. Default is enabled.
DsaKeySize	Specifies the size of the Dsa Key. Default value is 1024.

Table continues...

Field	Description
RsaKeySize	Specifies the size of the Rsa key. Default value is 1024.

Deleting SSH security groups

Procedure

1. Select **Configuration > Security**.
2. From the **Network > SSH** folder, select the SSH security group to delete.
3. Click **Delete** from the toolbar on the top left.
4. Click **Yes** when prompted to confirm the deletion.

Configuring a security group for CLI access

About this task

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

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > Password > CLI** folder, click the folder for the security group to configure CLI access.
3. In the CLI access table, modify the fields of configurable properties as needed, then click **Apply Changes**.

Result

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

CLI Access table field descriptions

Field	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.

Table continues...

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

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

Configuring a security group for Web access

About this task

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

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > Password > WEB** folder, click the folder for the security group to configure Web access.
3. In the contents pane, click the **Web Access** tab.
4. In the Web access table, edit the Web access user names and passwords.

Important:

In Web Access only the ROPassword can be changed.

5. On the Security toolbar, click **Apply Changes**.

Result

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

Web Access table field descriptions

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

Configuring SNMP v1/v2c access for ERS 8xxx security group

About this task

You can use Security view to configure the SNMP community strings for all devices in a ERS 8xxx security group.

Procedure

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

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

SNMP Access tab field descriptions

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

Configuring security group for SNMP v3 access

You can use Security view to configure the SNMPv3 access for all of the devices in a security group.

Before you begin to use Security view to configure access parameters, you must configure SNMPv3 credentials on the device that you wish to manage. You must also enter the SNMPv3 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, the system allows users to connect to devices in a security group using SNMPv3. To manage the level of access for each user, you must configure the following parameters in Security view:

- Create the user in the USM table.
- Add the user to the VACM group.
- Assign access levels to the USM group.
- Create a VACM MIB view.

These parameters allow you to assign a user to a MIB view; when the user connects to a device through SNMPv3, 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

About this task

You can use Security view to configure User-based Security Model (USM) access for devices in a security group.

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > SNMPv3** folder in the navigation pane, click the folder for the security group to configure USM access.
3. In the security group folder, click the desired device.
4. In the contents pane, click the **USM Access** tab.
5. Enter the parameters for USM access.

USM access field descriptions

Field	Description
Engine ID	Indicates the administratively-unique identifier for the SNMP engine.
Name	Indicates 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

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > SNMPv3** folder, click the **USM Access** tab.
3. Click **Create Entry**.
4. In the **SM - New USM Access Entry** dialog box, edit the USM user names and passwords, as described in the table below.
5. 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.
6. Click **Ok**.

USM user field descriptions

Field	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.
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.
Save	Adds the devices to the security group and closes the dialog box.
Cancel	Closes the dialog box without applying your settings.
Help	Opens Online help for the current folder or tab.

Configuring VACM group access**Procedure**

1. Select **Configuration > Security**.
2. Under the **Network > SNMPv3** folder, click the folder for the security group to configure USM access.
3. Click the **VACM Group Access** tab.
4. Click **Create Entry**, which is the plus sign on the tool bar.
5. In the SM - New VACM Group Access Entry window, edit the VACM Group Access properties as required.

6. To apply the changes to multiple devices in the group, choose the devices from the **Devices** list.
7. Click **OK**.

Result

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

VACM group access field descriptions

Field	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: <ul style="list-style-type: none"> • 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.
Save	Adds the devices to the security group and closes the dialog box.
Cancel	Closes the dialog box without applying your settings.
Help	Opens Online help for the current folder or tab.

Configuring VACM group members

About this task

You can use Security view to configure VACM Group Members for devices in a security group.

Procedure

1. Select **Configuration > Security**.

2. Under the **SNMPv3** folder in the navigation pane, click the folder for the security group.
3. In the security group folder, click the desired device.
4. In the contents pane, click the **VACM Group Members** tab.
5. On the Toolbar, click **Create Entry**.
6. In the **SM - VACM Group Member Entry** dialog box, edit the VACM Group Member properties.
7. To apply the changes to multiple devices in the group, choose the devices from the **Devices** list.
8. Click **OK**.

VACM group field descriptions

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

Configuring the VACM MIB view

Procedure

1. Select **Configuration > Security**.
2. In the contents pane, click the **VACM MIB View** tab.
3. On the Toolbar, click **Create Entry**.
4. In the **SM - New VACM MIB View Entry** window, edit the VACM MIB View properties as needed.
5. To apply the changes to multiple devices in the group, choose the devices to apply the changes from the **Devices** list.
6. Click **OK**.

Result

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

VACM MIB view field descriptions

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

Accessing the VACM MIB view

You can use Security to display VACM Management Information Base (MIB) views for devices in a security group.

Procedure

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

VACM MIB view field descriptions

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

Viewing the community table

About this task

You can use Security view to configure the Community Table for devices in a security group.

Procedure

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

Community table field descriptions

Field	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

Procedure

1. Select **Configuration > Security**.
2. In the contents pane, click the **Community Table** tab.
3. On the Toolbar, click **Create Entry**.
4. In the **SM - New Community Table Entry** window, edit the Community Table properties, as required.
5. To apply the changes to multiple devices in the group, choose the devices from the **Devices** list.
6. Click **Ok**.

Result

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

Community table field descriptions

Field	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).

Viewing the target table

About this task

You can use Security view to display the Target Table for devices in a security group.

Procedure

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

Target table field descriptions

Field	Description
Name	The unique identifier to index this table.

Table continues...

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

Configuring the target table

Procedure

1. Select **Configuration > Security**.
2. In the contents pane, click the **Target Table** tab.
3. On the Toolbar, click **Create Entry**.
4. In the **SM - New Target Table Entry** window, edit the Target Table properties as needed.
5. To apply the changes to multiple devices in the group, choose the devices to apply the changes from the **Devices** list.
6. Click **OK**.

Result

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

Target table field descriptions

Field	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.

Table continues...

Field	Description
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 snmpTargetParametersTable entries.
Save	Adds the devices to the security group and closes the dialog box.
Cancel	Closes the dialog box without applying your settings.
Help	Opens the online Help for the current folder or tab.

Viewing the Target Params table

About this task

You can use Security view to display the Target Params Table for devices in a security group.

Procedure

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

Target Params table field descriptions

Field	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: <ul style="list-style-type: none"> • noAuthNoPriv • authNoPriv • authpriv

Configuring the Target Params table

Procedure

1. Select **Configuration > Security**.
2. Under the **SNMPv3** folder in the navigation pane, click the folder for the security group to configure USM access.
3. In the security group folder, click the desired device.
4. In the contents pane, click the **Target Params Table** tab.
5. On the Toolbar, click **Create Entry**.
6. In the **SM - New Target Params Table Entry** dialog box, edit the Target Params Table properties.
7. 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.
8. Click **OK**.

Target Params table field descriptions

Field	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: <ul style="list-style-type: none"> • noAuthNoPriv • authNoPriv • authpriv
Clear All	Deselects all devices on the device list.
Select All	Selects all devices on the device list.
Save	Adds the devices to the security group and closes the dialog box.
Cancel	Closes the dialog box without applying your settings.
Help	Opens the online Help for the folder or tab.

Viewing the notify table

About this task

You can use Security view to display the Notify Table for devices in a security group.

Procedure

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

Notify table field descriptions

Field	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: <ul style="list-style-type: none"> • trap • inform

Configuring the notify table

Procedure

1. Select **Configuration > Security**.
2. In the contents pane, click the **Notify Table** tab.
3. On the Toolbar, click **Create Entry**.
4. In the **SM - New Notify Table Entry** window, edit the Notify Table properties as needed.
5. To apply the changes to multiple devices in the group, choose the devices from the **Devices** list.
6. Click **OK**.

Result

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

Notify table field descriptions

Field	Description
Name	The community string for which a row in this table represents a configuration.

Table continues...

Field	Description
Tag	The tag value used to select the entries in snmpTargetAddrTable.
Type	The type assigned to the community string name. Choices are: <ul style="list-style-type: none"> • trap • inform
Clear All	Deselects all devices on the device list.
Select All	Selects all devices on the device list.
Save	Adds the devices to the security group and closes the dialog box.
Cancel	Closes the dialog box without applying your settings.
Help	Opens online Help for the current folder or tab.

Viewing the notify filter table

About this task

You can use Security view to display the Notify Filter Table for devices in a security group.

Procedure

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

Notify filter table field descriptions

Field	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

Procedure

1. Select **Configuration > Security**.

2. In the contents pane, click the **Notify Filter Table** tab.
3. Click **Create Entry** on the tool bar.
4. In the **SM - New Notify Filter Table Entry** window, edit the Notify Filter Table properties.
5. 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.
6. Click **OK**.

Result

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

Notify filter table field descriptions

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

Viewing the notify filter table

About this task

You can use Security view to display the Notify Filter Table for devices in a security group.

Procedure

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

Notify Filter Profile table field descriptions

Field	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.
Save	Adds the devices to the security group and closes the dialog box.
Cancel	Closes the dialog box without applying your settings.
Help	Opens online Help for the current folder or tab.

Configuring the notify filter profile table**Procedure**

1. Select **Configuration > Security**.
2. In the contents pane, click the **Notify Filter Profile Table** tab.
3. On the Toolbar, click **Create Entry**.
4. In the **SM - New Notify Filter Profile Table Entry** dialog box, edit the Notify Filter Profile Table properties.
5. To apply the changes to multiple devices in the group, choose the devices from the **Devices** list.
6. Click **Ok**.

Result

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

Notify Filter Profile table field descriptions

Field	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.
Save	Adds the devices to the security group and closes the dialog box.
Cancel	Closes the dialog box without applying your settings.
Help	Opens online Help for the current folder or tab.

Create and manage access policies

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

Security view allows you to enable and disable access policies at a variety of levels within a security group.

Enabling or disabling access policies for devices in a security group

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > Access Policy** folder in the navigation pane, open the folder for the security group for which you want to set access policies.
3. In the security group folder, click the desired device.
4. In the contents pane, click the **Access Policy SNMP Groups Table** tab for devices supporting SNMPv3.
5. Enter the **Policy Id**, **Name** and **Model** for the SNMP group.
6. In the contents pane, click the **Access Policy Enable** tab.
7. Click the drop-down box in the **Enable** column and choose **True** to enable access policies or **False** to disable access policies.
8. On the Security tool bar, click **Apply Changes** to save the changes.

Access Policy SNMP Groups table field descriptions

Access Policy SNMP Groups Table tab

Field	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.

Access Policy Enable tab

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



Enabling or disabling individual access policies

Procedure

1. Select **Configuration > Security**.
2. Under the **Network > Access Policy** folder in the navigation pane, open the folder for the security group for which you want to set access policies.
3. In the security group folder, click the desired device.

4. In the contents pane, click the **Access Policy Table** tab.
5. Select the access policy you want to enable or disable.
6. In the PolicyEnable column, click the entry for the access policy and choose **True** to enable the access policy or **False** to disable the access policy.
7. On the Security tool bar, click **Apply**.

Access Policy Table field descriptions

Field	Description
Id	Identifies the entry in the table.
Name	Displays the name of the policy.
Policy Enable	Activates or deactivates the access policy.
Mode	Indicates whether a packet having a source IP address that matches this entry should be permitted to enter the device or denied access.
Service	Selects the protocol to which this entry should be applied.
Precedence	Indicates the precedence of the policy. The lower the number, the higher the precedence (1 to 128).
NetInetAddressType	Specifies the source network IP address type.
NetInetAddress	Specifies the source network IP address.
NetInetAddressPrefixLen	Specifies the prefix length for the source network IP address.
TrustedHostInetAddress	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

Procedure

1. Select **Configuration > Security**.

2. Under the **Network > Access Policy** folder in the navigation pane, click the folder for the security group to delete an access policy.
3. In the security group folder, click the desired device.
4. In the contents pane, click the **Access Policy Table** tab.
5. On the **Access Policy Table** tab, click any cell of the access policy to delete.
6. On the toolbar, click **Delete**.
7. Click **Yes** to confirm deletion.

Chapter 19: Managing File Inventory

About File Inventory

File Inventory view has two primary functions—file management and inventory management. The following sections describe the capabilities provided by these functions.

File management features

The file management features of File Inventory view allows you to upload and download files to and from network devices. For all devices that support multiple devices, you can also use File Inventory view 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 File Inventory view.

Table 91: File Inventory view file management capabilities

Device family	Operation	Multiple devices	File types
APLS	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
ERS 3600	Download	Yes	Image, configuration, firmware image, or ASCII configuration file
	Upload	Yes	Configuration only
	Backup	Yes	Configuration
	Restore	Yes	Configuration
	Archive	Yes	Configuration
	Synchronize	Yes	Configuration

Table continues...

Device family	Operation	Multiple devices	File types
	Device upgrade	Yes	Image
	Compare runtime	Yes	Configuration
ERS 4900	Download	Yes	Image, configuration, firmware image, or ASCII configuration file
	Upload	Yes	Configuration only
	Backup	Yes	Configuration
	Restore	Yes	Configuration
	Archive	Yes	Configuration
	Synchronize	Yes	Configuration
	Device upgrade	Yes	Image
	Compare runtime	Yes	Configuration
ERS 5900	Download	Yes	Image, configuration, firmware image, or ASCII configuration file
	Upload	Yes	Configuration only
	Backup	Yes	Configuration
	Restore	Yes	Configuration
	Archive	Yes	Configuration
	Synchronize	Yes	Configuration
	Device upgrade	Yes	Image
	Compare runtime	Yes	Configuration
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		
Ethernet Routing Switch 55xx/35xx/45xx/25xx	Download	Yes	Image, configuration, firmware image, or ASCII configuration file
	Upload	Yes	Configuration only
	Backup	Yes	Configuration

Table continues...

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
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
OM 1000	Download	Yes	Image, configuration, firmware image, or ASCII configuration file
	Upload	Yes	Configuration only

Table continues...

Device family	Operation	Multiple devices	File types
	Backup	Yes	Configuration
	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 management station, or you can designate a separate machine as the TFTP server.

Inventory management features

The inventory management features of the File Inventory show you current information about the hardware and software discovered on your network.

- Device and chassis types
- Installed blades
- Serial and revision numbers
- Image and configuration file names and versions
- GBIC data

Starting File Inventory view

Before you begin

You must have the File Inventory user role assigned by the administrator.

About this task

Procedure

1. Select **Backup & Restore > File Inventory**.
2. Click **Reload / Discover** to reload or discover the Device Inventory.
3. Perform one of the following:
 - Click **Yes** to query the discovered devices for inventory information.
 - Click **No** to get inventory information from a previously saved inventory file. When prompted for the location of the inventory file, browse the file and click **Open Inventory**.
4. 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**.

Result

The **Inventory Manager** dialog box displays.

! Important:

The discovery process does not include devices without proper credentials assigned to them.

Using the File Inventory view

The following figure shows the File Inventory view.

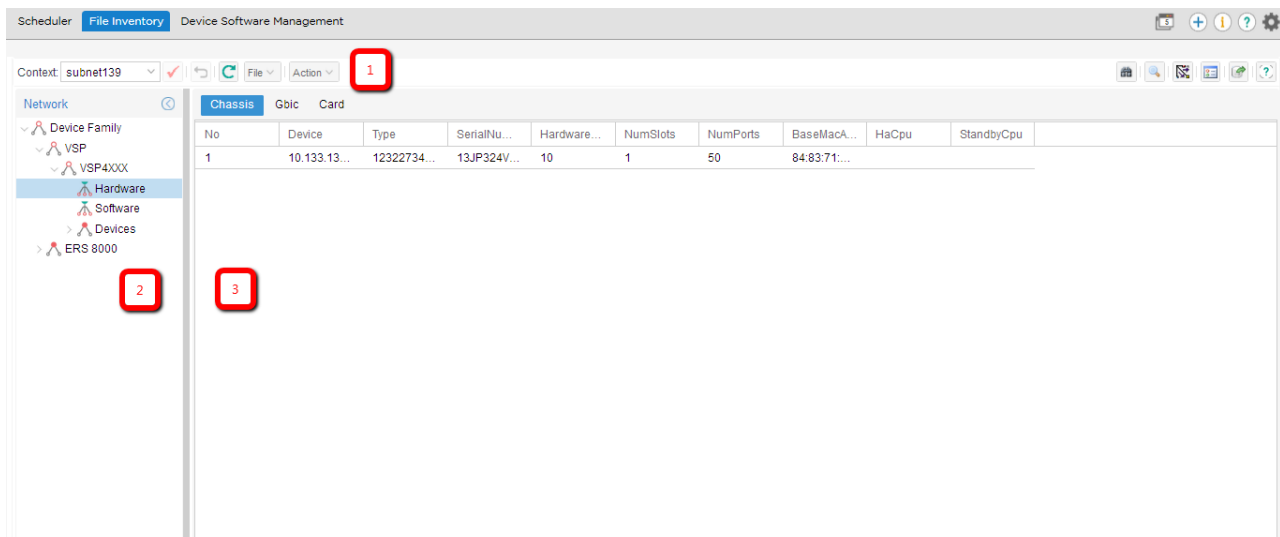







Figure 42: File Inventory view

The following table describes the parts of the File Inventory view.

Table 92: Parts of the File Inventory view

Part	Description
1. Tool bar	Provides quick access to commonly used Inventory commands.
2. Navigation pane	Allows you to navigate Inventory elements for devices discovered on the network.
3. Contents pane	Displays file and inventory information for the element selected on the Navigation pane.

File Inventory view toolbar

Icon	Name	Description
	Reload / Discover	Rediscovered the inventory information and reloads the File Inventory 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 topology map.
	Preferences	Filters devices based on Family or Capabilities.
	Export	Exports inventory information displayed in content panel grid in to a text file.
		Opens online Help for the current folder or tab.

File Inventory menu bar commands

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.

Table continues...

Command	Menu	Description
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 server to your local desktop or PC. The backup files are always on the 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.

File Inventory view navigation pane

The File Inventory view 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 File Inventory view navigation pane.

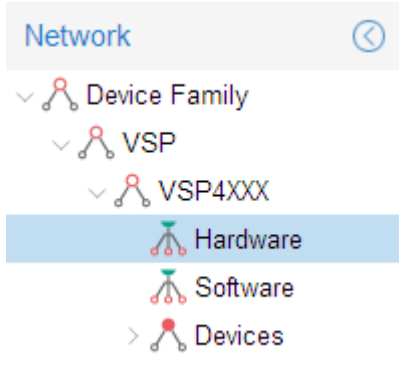


Figure 43: File Inventory view navigation pane

The following table describes the File Inventory view navigation pane. The navigation pane shows only the device families that are available in the system.

Table 93: File Inventory view navigation pane

Part	Description
Device Family folder	Specifies the root folder; contains all of the icons and folders in the Tree Panel.
APLS folder	Displays the information specific to APLS devices.
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: <ul style="list-style-type: none"> • 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. • VSP 72XX — Displays the information specific to VSP 72XX devices. • VSP 82XX — Displays the information specific to VSP 82XX devices.
Legacy BayStack folder	Displays the information specific to legacy baystack.
ERS 16XX folder	Displays the information specific to ERS 16XX devices.

Table continues...

Part	Description
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.
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 File Inventory navigation tree

Depending on the devices that are discovered, the File Inventory view may show folders that are not listed here, and may not show folders that are listed.

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 94: Parts of the ERS 5XXX/4XXX/35XX folder

Part	Description
ERS 5XXX/4XXX/35XX Hardware Table	Shows information about Ethernet Routing Switch 5XXX, 4XXX, and 35XX device hardware in the network inventory.
ERS 5XXX/4XXX/35XX Software Table	Shows information about software running on Ethernet Routing Switch 5XXX, 4XXX, and 35XX devices in the network inventory.
ERS 5XXX/4XXX/35XX Devices Folder	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 95: Parts of the ERS 5XXX/4XXX/35XX Hardware table

Part	Description
Stack Tab	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 96: 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	Shows 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 97: Parts of the ERS 5XXX/4XXX/35XX Software table

Part	Description
General tab	Shows general information about software running on Ethernet Routing Switch (legacy) 5XXX, 4XXX, and 35XX devices in the network inventory.
Image/Config tab	Shows information about software configuration settings.

General tab

Use the General tab of the ERS 5XXX/4XXX/35XX Software table 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 98: 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 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 99: 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.
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 File Inventory view displays the following tabs in the contents pane

Table 100: Parts of the ERS 5XXX/4XXX/35XX Devices folder

Tab	Part	Description
Hardware tab	Stack tab	Shows information about Ethernet Routing Switch 5XXX, 4XXX, and 35XX stack.
	Gbic tab	Shows information about the system that Ethernet Routing Switch 5XXX, 4XXX, and 35XX use to determine the device capabilities.

Table continues...

Tab	Part	Description
Software tab	General tab	Shows general information about software running on Ethernet Routing Switch 5XXX, 4XXX, and 35XX devices in the network inventory.
	Image/Config tab	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 to view information about Ethernet Routing Switch 5XXX, 4XXX, and 35XX Stack.

The following table describes the parts of the Stack tab.

Table 101: 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 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 102: 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.

Table continues...

Part	Description
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 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 103: 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 to view information about image and configuration files loaded on the device.

The following table describes the parts of the Image/Config tab.

Table 104: 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 105: Parts of the ERS 8000 folder

Part	Description
ERS 8000 Hardware table	Shows information about Ethernet Routing Switch 8000 device hardware in the network inventory.
ERS 8000 Software table	Shows information about software running on Ethernet Routing Switch 8000 devices in the network inventory.
ERS 8000 Devices Folder	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 106: Parts of the ERS 8000 Hardware table

Part	Description
Chassis tab	Shows information about Ethernet Routing Switch 8000 family chassis.
Mda tab	Shows information about MDAs installed in Ethernet Routing Switch 8000 family chassis.
Card tab	Shows information about cards installed in Ethernet Routing Switch 8000 family chassis.

Chassis tab

Use the Chassis tab of the ERS 8000 Hardware table to view information about Ethernet Routing Switch 8000 family chassis.

The following table describes the parts of the Chassis tab.

Table 107: 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.

Table continues...

Part	Description
StandbyCpu	Shows you whether the L2 Redundancy is enabled on the standby CPU. The possible states are: <ul style="list-style-type: none"> • hotStandbyCPU • warmStandbyCPU • standbyCPUNotPresent

Mda tab

Use the Mda tab of the ERS 8000 Hardware table 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 108: 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.
Description	Shows the MDA description. Possible values include: <ul style="list-style-type: none"> • 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 to view information about cards installed in Ethernet Routing Switch 8000 series chassis.

The following table describes the parts of the Card tab.

Table 109: 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.

Table continues...

Part	Description
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: <ul style="list-style-type: none"> • 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.

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 110: Parts of the ERS 8000 Software table

Part	Description
General tab	Shows general information about software running on Ethernet Routing Switch 8000 and Virtual Services Platform 9XXX family devices in the network inventory.
DeviceInfo tab	Shows information about the device.

General tab

Use the General tab of the ERS 8000 Software table 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 111: 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.
Contact	Shows the administrative contact for the device.

DeviceInfo tab

Use the DeviceInfo tab of the ERS 8000 Software table 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 112: 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 113: Parts of the ERS 8000 Devices folder

Tab	Part	Description
Hardware	Chassis tab	Shows information about the Ethernet Routing Switch 8000 family chassis.
	Card tab	Shows information about cards installed in the Ethernet Routing Switch 8000 series chassis.
Software	General tab	Shows general information about software running on Ethernet Routing Switch 8000 family devices in the network inventory.
Others	PcmciaFiles tab	Shows information about the PcmciaFiles.

Chassis tab

Use the Chassis tab of the ERS 8000 Devices folder to view information about the Ethernet Routing Switch 8000 device chassis.

The following table describes the parts of the Chassis tab.

Table 114: 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: <ul style="list-style-type: none"> • hotStandbyCPU • warmStandbyCPU • standbyCPUNotPresent
StandbyCpu	Shows the module type.

Card tab

Use the Card tab of the ERS 8000 Devices folder to view information about cards installed in Ethernet Routing Switch 8000 series chassis.

The following table describes the parts of the Card tab.

Table 115: 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 <ul style="list-style-type: none"> • 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 ERS 8000 Devices folder 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 116: 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 PcmciaFiles tab of the ERS 8000 Devices folder to view pcmcia file information of the selected Ethernet Routing Switch 8000 device.

The following table describes the parts of the PcmciaFiles tab.

Table 117: 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 File Inventory for VSP 4XXX, VSP 7024XLS, VSP 8XXX, VSP 72XX, VSP 7XXX, and VSP 9XXX.

VSP 4XXX folder

Use the VSP 4XXX folder to view information about VSP 4XXX hardware, software, and devices in the File Inventory.

The following table describes the parts of the VSP 4XXX folder.

Table 118: Parts of the VSP 4XXX folder

Part	Description
VSP 4XXX Hardware table on page 411	Shows information about VSP 4XXX device hardware in the File Inventory.

Table continues...

Part	Description
VSP 4XXX Software table on page 412	Shows information about software running on VSP 4XXX devices in the File Inventory.
VSP 4XXX Devices folder on page 413	Shows information about each of the VSP 4XXX devices discovered on the network.

VSP 4XXX Hardware table

Use the following VSP 4XXX Hardware table to view information about VSP 4XXX device hardware in the File Inventory.

Table 119: Parts of the VSP 4XXX Hardware table

Part	Description
Chassis tab on page 411	Shows information about the VSP 4XXX family chassis.
Card tab on page 412	Shows information about the cards installed in the VSP 4XXX family chassis.

Chassis tab

Use the Chassis tab of the VSP 4XXX Devices folder to view information about the VSP 4XXX family chassis.

The following table describes the parts of the Chassis tab.

Table 120: Parts of the Chassis tab of the VSP 4XXX 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: <ul style="list-style-type: none"> • hotStandbyCPU • warmStandbyCPU • standbyCPUNotPresent

Card tab

Use the Card tab of the VSP 4XXX Hardware table to view information about cards installed in the VSP 4XXX series chassis.

The following table describes the parts of the Card tab.

Table 121: Parts of the Card tab of the VSP 4XXX 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 VSP 4XXX 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: <ul style="list-style-type: none"> • 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.
BlackDateCode	Shows the back date code for the card.
BackDeviations	Shows the back deviations for the card.

VSP 4XXX Software table

Use the VSP 4XXX Software table to view information about software running on the VSP 4XXX devices in the File Inventory.

Table 122: Parts of the VSP 4XXX Software table

Part	Description
General tab on page 413	Shows general information about software running on VSP 4XXX family devices in the File Inventory.

General tab

Use the General tab of the VSP 4XXX Software table to view general information about software running on the VSP 4XXX family of devices on the network.

Table 123: Parts of the General tab of the VSP 4XXX 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 4XXX Devices folder

Use the VSP 4XXX Devices folder to view information about VSP 4XXX devices in the File Inventory.

For each device in the Devices folder, the File Inventory displays the following tabs in the Contents pane.

Table 124: Parts of the VSP 4XXX Devices folder

Tab	Part	Description
Hardware	Chassis tab on page 411	Shows information about the VSP 4XXX family chassis.
	Card tab on page 412	Shows information about the cards installed in the VSP 4XXX family chassis.
Software	General tab on page 413	Shows general information about software running on VSP 4XXX devices in the File Inventory.
Others	FlashFiles tab on page 414	Shows information about the files in the flash memory of VSP 4XXX family devices.

Important:

The Contents pane displays the tabs described in the preceding table only after you select a device from the device folder.

FlashFiles tab

Use the FlashFiles tab of the VSP 4XXX Devices folder to view information about the files in the flash memory of the selected VSP 4XXX device.

The following table describes the parts of the VSP 4XXX Software table FlashFiles tab.

Table 125: Parts of the FlashFiles tab of the VSP 4XXX Software table

Part	Description
No	Shows the row number of the table entry.
Device	Shows the IP address or host name of the device.
Slot	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.

VSP 7024XLS folder

Use the VSP 7024XLS folder to view information about VSP 7024XLS hardware, software, and devices in the File Inventory.

The following table describes the parts of the VSP 7024XLS folder.

Table 126: Parts of the VSP 7024XLS folder

Part	Description
VSP 7024XLS Hardware table on page 414	Shows information about VSP 7024XLS device hardware in the File Inventory.
VSP7024XLS Software table on page 416	Shows information about software running on VSP 7024XLS devices in the File Inventory.
VSP7024XLS Devices folder on page 417	Shows information about each of the VSP 7024XLS devices discovered on the network.

VSP 7024XLS Hardware table

Use the following VSP 7024XLS Hardware table to view information about VSP 7024XLS device hardware in the File Inventory.

Table 127: Parts of the VSP 7024XLS Hardware table

Part	Description
Stack tab on page 414	Shows information about the VSP 7024XLS Stacks.
Mda tab on page 415	Shows information about the VSP 7024XLS Mda.
Gbic tab on page 415	Shows information about the VSP 7024XLS Gbic.

Stack tab

Use the Stack tab of the VSP 7024XLS Devices folder to view information about the stacks.

The following table describes the parts of the Stack tab.

Table 128: Parts of the stack tab of the VSP7024XLS 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 a description of the device.
Ver	Shows the version number of the device.
SerNum	Shows the serial number for the device.
Location	Location Shows the location of the device.

Mda tab

Use the Mda tab of the VSP 7024XLS Devices folder to view information about the Mda.

The following table describes the parts of the Mda tab.

Table 129: Parts of the mda tab of the VSP7024XLS 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 a description of the device.

Gbic tab

Use the Gbic tab of the VSP 7024XLS Devices folder to view information about the Gbic.

The following table describes the parts of the Gbic tab.

Table 130: Parts of the Gbic tab of the VSP7024XLS Hardware table

Part	Description
No.	Shows the row number of the table entry.
Device	Shows the IP address or host name for the device.
Unit/PortNumber	Shows the port number of the device.
GBIC Type	Shows the gbic type. It follows the port number.
VendorName	Shows the gbic vendor name.
VendorOUI	Shows the company ID of the gbic vendor IEEE.
VendorPart	Shows the part number provided by gbic vendor.
VendorRevision	Shows the revision level for part number provided by vendor.

Table continues...

Part	Description
VendorSerial	Shows the serial number provided by the vendor.
HWOptions	Shows the hardware options for the gbic.
DateCode	Shows the manufacturing date code of the vendor.
VendorData	Shows the vendor specific data for gbic.
OrderCode	Shows the order code.

VSP 7024XLS Software table

Use the VSP 7024XLS Software table to view information about software running on the VSP 7024XLS devices in the File Inventory.

Table 131: Parts of the VSP 7024XLS Software table

Part	Description
General tab on page 416	Shows general information about software running on VSP 7024XLS family devices in the File Inventory.
Image/Config tab on page 416	Shows information about image and configuration files loaded on VSP 7024XLS devices in the File Inventory.

General tab

Use the General tab of the VSP7024XLS Software table to view general information about software running on the VSP7024XLS family of devices on the network.

Table 132: Parts of the General tab of the VSP7024XLS 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 VSP 7024XLS Software table to view information about image and configuration files loaded on VSP 7024XLS devices.

The following table describes the parts of the VSP 7024XLS Software table Image/Config tab.

Table 133: Parts of the Image/Config tab of the VSP7024XLS 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 7024XLS Devices folder

Use the VSP 7024XLS Devices folder to view information about VSP 7024XLS devices in the File Inventory.

For each device in the Devices folder, the File Inventory displays the following tabs in the Contents pane.

Table 134: Parts of the VSP 7024XLS Devices folder

Tab	Part	Description
Hardware	Stack tab on page 414	Shows information about the VSP 7024XLS stack.
	Mda tab on page 415	Shows information about Mda installed in VSP 7024XLS devices.
	Gbic tab on page 415	Shows information about Gbic installed in VSP 7024XLS devices.
Software	General tab on page 416	Shows general information about software running on VSP 7024XLS devices in the File Inventory.
	Image/Config tab on page 416	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.

VSP 8XXX folder

Use the VSP 8XXX folder to view information about VSP 8XXX hardware, software, and devices in the File Inventory.

The following table describes the parts of the VSP 8XXX folder.

Table 135: Parts of the VSP 8XXX folder

Part	Description
VSP8XXX Hardware table on page 418	Shows information about VSP 8XXX device hardware in the File Inventory.
VSP8XXX Software table on page 419	Shows information about software running on VSP 8XXX devices in the File Inventory.

Table continues...

Part	Description
VSP8XXX Devices folder on page 420	Shows information about each of the VSP 8XXX devices discovered on the network.

VSP 8XXX Hardware table

Use the following VSP 8XXX Hardware table to view information about VSP 8XXX device hardware in the File Inventory.

Table 136: Parts of the VSP 8XXX Hardware table

Part	Description
Chassis tab on page 418	Shows information about the VSP 8XXX family chassis.
Card tab on page 418	Shows information about the cards installed in the VSP 8XXX family chassis.

Chassis tab

Use the Chassis tab of the VSP 8XXX Devices folder to view information about the VSP 8XXX family chassis.

The following table describes the parts of the Chassis tab.

Table 137: Parts of the Chassis tab of the VSP8XXX 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: <ul style="list-style-type: none"> • hotStandbyCPU • warmStandbyCPU • standbyCPUNotPresent

Card tab

Use the Card tab of the VSP 8XXX Hardware table to view information about cards installed in the VSP 8XXX series chassis.

The following table describes the parts of the Card tab.

Table 138: Parts of the Card tab of the VSP8XXX 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 VSP 8XXX 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: <ul style="list-style-type: none"> • 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.

VSP 8XXX Software table

Use the VSP 8XXX Software table to view information about software running on the VSP 8XXX devices in the File Inventory.

Table 139: Parts of the VSP 8XXX Software table

Part	Description
General tab on page 419	Shows general information about software running on VSP 8XXX family devices in the File Inventory.

General tab

Use the General tab of the VSP8XXX Software table to view general information about software running on the VSP8XXX family of devices on the network.

Table 140: Parts of the General tab of the VSP8XXX 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 8XXX Devices folder

Use the VSP 8XXX Devices folder to view information about VSP 8XXX devices in the File Inventory.

For each device in the Devices folder, the File Inventory displays the following tabs in the Contents pane.

Table 141: Parts of the VSP 8XXX Devices folder

Tab	Part	Description
Hardware	Chassis tab on page 418	Shows information about the VSP 8XXX family chassis.
	Card tab on page 418	Shows information about the cards installed in the VSP 8XXX family chassis.
Software	General tab on page 419	Shows general information about software running on VSP 8XXX devices in the File Inventory.
Others	FlashFiles tab on page 421	Shows information about the files in the flash memory of VSP 8XXX family devices.

 **Important:**

The Contents pane displays the tabs described in the preceding table only after you select a device from the device folder.

FlashFiles tab

Use the FlashFiles tab of the VSP 8XXX Devices folder to view information about the files in the flash memory of the selected VSP 8XXX device.

The following table describes the parts of the VSP 8XXX Software table FlashFiles tab.

Table 142: Parts of the FlashFiles tab of the VSP8XXX Software table

Part	Description
No	Shows the row number of the table entry.
Device	Shows the IP address or host name of the device.
Slot	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.

VSP 72XX folder

Use the VSP 72XX folder to view information about VSP 72XX hardware, software, and devices in the File Inventory.

The following table describes the parts of the VSP 72XX folder.

Table 143: Parts of the VSP 72XX folder

Part	Description
VSP72XX Hardware table on page 421	Shows information about VSP 72XX device hardware in the File Inventory.
VSP72XX Software table on page 423	Shows information about software running on VSP 72XX devices in the File Inventory.
VSP72XX Devices folder on page 424	Shows information about each of the VSP 72XX devices discovered on the network.

VSP 72XX Hardware table

Use the following VSP 72XX Hardware table to view information about VSP 72XX device hardware in the File Inventory.

Table 144: Parts of the VSP 72XX Hardware table

Part	Description
Chassis tab on page 421	Shows information about the VSP 72XX family chassis.
Card tab on page 422	Shows information about the cards installed in the VSP 72XX family chassis.

Chassis tab

Use the Chassis tab of the VSP 72XX Devices folder to view information about the VSP 72XX family chassis.

The following table describes the parts of the Chassis tab.

Table 145: Parts of the Chassis tab of the VSP72XX 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: <ul style="list-style-type: none"> • hotStandbyCPU • warmStandbyCPU • standbyCPUNotPresent

Card tab

Use the Card tab of the VSP 72XX Hardware table to view information about cards installed in the VSP 72XX series chassis.

The following table describes the parts of the Card tab.

Table 146: Parts of the Card tab of the VSP72XX 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 VSP 72XX 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.

Table continues...

Part	Description
BackType	Shows the back type of the card. Possible values are: <ul style="list-style-type: none"> • 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.

VSP 72XX Software table

Use the VSP 72XX Software table to view information about software running on the VSP 72XX devices in the File Inventory.

Table 147: Parts of the VSP 72XX Software table

Part	Description
General tab on page 423	Shows general information about software running on VSP 72XX family devices in the File Inventory.

General tab

Use the General tab of the VSP72XX Software table to view general information about software running on the VSP72XX family of devices on the network.

Table 148: Parts of the General tab of the VSP72XX 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.

Table continues...

Part	Description
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 72XX Devices folder

Use the VSP 72XX Devices folder to view information about VSP 72XX devices in the File Inventory.

For each device in the Devices folder, the File Inventory displays the following tabs in the Contents pane.

Table 149: Parts of the VSP 72XX Devices folder

Tab	Part	Description
Hardware	Chassis tab on page 421	Shows information about the VSP 72XX family chassis.
	Card tab on page 422	Shows information about the cards installed in the VSP 72XX family chassis.
Software	General tab on page 423	Shows general information about software running on VSP 72XX devices in the File Inventory.
Others	FlashFiles on page 424	Shows information about the files in the flash memory of VSP 72XX family devices.

 **Important:**

The Contents pane displays the tabs described in the preceding table only after you select a device from the device folder.

FlashFiles tab

Use the FlashFiles tab of the VSP 72XX Devices folder to view information about the files in the flash memory of the selected VSP 72XX device.

The following table describes the parts of the VSP 72XX Software table FlashFiles tab.

Table 150: Parts of the FlashFiles tab of the VSP72XX Software table

Part	Description
No	Shows the row number of the table entry.
Device	Shows the IP address or host name of the device.
Slot	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 151: Parts of the VSP7XXX folder

Part	Description
VSP 7XXX Hardware table on page 425	Shows information about VSP 7XXX device hardware in the network inventory.
VSP 7XXX Software table on page 426	Shows information about software running on VSP 7XXX devices in the network inventory.
VSP 7XXX Devices folder on page 427	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.

Table 152: Parts of the VSP 7XXX Hardware table

Part	Description
Stack tab on page 425	Shows information about the Virtual Services Platform 7XXX stacks.
Mda tab on page 425	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 153: 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 154: Parts of the Mda tab of the VSP 7024XLS 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.

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.

The following table describes the parts of the VSP 7XXX Software table.

Table 155: Parts of the VSP 7XXX Software table

Part	Description
General Tab on page 426	Shows general information about software running on Virtual Services Platform 7XXX family devices in the network inventory.
Image Config Tab on page 426	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 156: 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.
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 157: 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 File Inventory view displays the following tabs in the Contents pane.

Table 158: Parts of the VSP 7XXX Devices folder

Tab	Part	Description
Hardware Tab	Stack tab on page 425	Shows information about the VSP 7XXX stack.
	Mda tab on page 425	Shows information about MDA installed in VSP 7XXX devices.
Software tab	General Tab on page 426	Shows general information about software running on VSP 7XXX devices in the network inventory.
	Image Config Tab on page 426	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.

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 159: Parts of the VSP 9XXX folder

Part	Description
VSP 9XXX Hardware table on page 428	Shows information about Virtual Services Platform 9XXX device hardware in the network inventory.
VSP 9XXX Software table on page 429	Shows information about software running on Virtual Services Platform 9XXX devices in the network inventory.
VSP 9XXX Devices folder on page 430	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.

The following table describes the parts of the VSP 9XXX Hardware table.

Table 160: Parts of the VSP 9XXX Hardware table

Part	Description
Chassis tab on page 432	Shows information about the Virtual Services Platform 9XXX family chassis.
Card tab on page 428	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 161: 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.

Table continues...

Part	Description
FrontDeviations	Shows front deviations for the card.
BackType	Shows the back type of the card. Possible values are: <ul style="list-style-type: none"> 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.

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.

The following table describes the parts of the VSP 9XXX Software table.

Table 162: Parts of the VSP 9XXX Software table

Part	Description
General tab on page 432	Shows general information about software running on Virtual Services Platform 9XXX family devices in the network inventory.

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 163: Parts of the General tab of the VSP 9XXX Devices folder

Part	Description
Contact	Shows the administrative contact for the device.

Table continues...

Part	Description
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.

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 164: Parts of the VSP 9XXX Devices folder

Tab	Part	Description
Hardware	Chassis tab on page 430	Shows information about the Virtual Services Platform 9XXX family chassis.
	Card tab on page 431	Shows information about cards installed in the Virtual Services Platform 9XXX series chassis.
Software	General tab on page 429	Shows general information about software running on Virtual Services Platform 9XXX family devices in the network inventory.
Others	FlashFiles tab on page 433	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 165: 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.

Table continues...

Part	Description
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: <ul style="list-style-type: none"> • 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 166: 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: <ul style="list-style-type: none"> • rc2kBackplane • rc2kSFM • rc2kBFM0 • rc2kBFM2 • rc2kBFM3 • rc2kBFM6 • rc2kBFM8 • rc2kMGsFM

Table continues...

Part	Description
	• 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 VSP 9XXX Software table to view general information about software running on Virtual Services Platform 9XXX family devices on the network.

Table 167: 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.

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 168: 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.

Table continues...

Part	Description
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: <ul style="list-style-type: none"> • 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 169: 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.

Reloading Inventory Manager

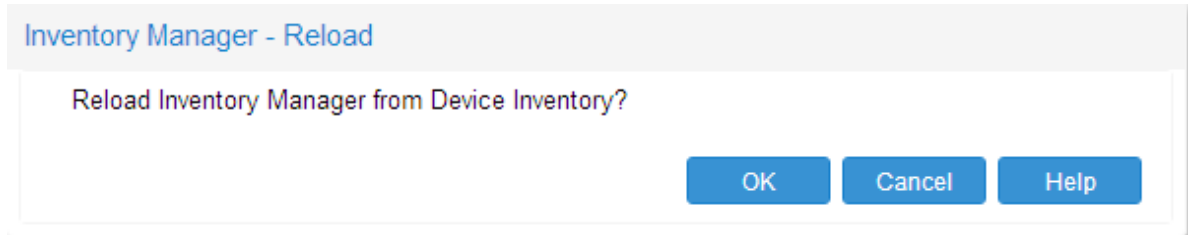
About this task

Perform the following procedure to reload the manager from the Device Inventory View.

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the File menu, select **Reload**.

The Inventory Manager-Reload window displays.



3. Click **OK**.
The Select Devices window displays.
4. Select the device or devices from the Available devices list.
5. Click **Query Now**.
6. Click **OK** when the inventory discovery operation completes.

Saving inventory information

About this task

Perform the following procedure to save inventory files that you can load again later.

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the File menu, select **Save Inventory Info**.
3. Select the location to save the file, and then click **OK**.

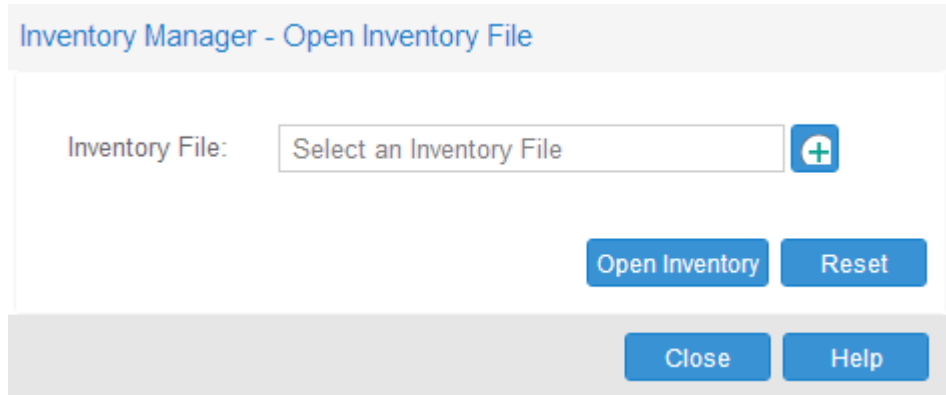
Opening an inventory file

About this task

Perform the following procedure to load saved inventory files.

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the File menu, select **Open Inventory File**.



3. In the Inventory Manager-Open Inventory File window, click the green icon to browse to the location of the saved inventory file.
4. Click **Open Inventory**.

Saving inventory file in a tab delimited text file

About this task

Perform the following procedure to save network inventory information in a tab-delimited text file.

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the File menu, select **Save Inventory in tab delimited text file**.
3. Click **Save**.

Downloading files to devices

About this task

Perform the following procedure to download configuration or image files or both to devices.

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the Action menu, select **Download File to Device(s)**.
The Inventory Manager-Download File to Device(s) window displays.
3. Type the **TFTP Server** information.
4. Type the **Source File Name** information.
5. Type the **Destination File Name** information.
6. Click **Yes** or **No** for **Prefix IP address for Source file**.

7. Select the device(s) from the list in Available Devices.
8. Click one of the following options:
 - a. **Schedule** to download the file to device(s) at a scheduled time.
 - b. **Download** to download the file to device(s) immediately.

Uploading file from device

About this task

Perform the following procedure to upload configuration or image files or both from devices.

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the Action menu, select **Upload File From Device(s)**.

The Inventory Manager – Upload File From Device(s) window displays.
3. Type the **TFTP Server** information.
4. Type the **Source File Name** information.
5. Type the **Destination File Postfix** information.
6. Select the device(s) from the list in Available Devices.
7. Click one of the following options:
 - a. **Schedule** to upload the file to device(s) at a scheduled time.
 - b. **Upload** to upload the file to device(s) immediately.

Backing up the configuration file

About this task

Perform this procedure to create backup configuration files that can be restored to devices in the event of a network failure.

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the Action menu, select **Backup Config File**.

The Inventory Manager — Backup Config File window displays.
3. Type the TFTP Server IP address.
4. Click **config.cfg** or **boot.cfg**.

config.cfg is selected by default.

5. Select the device(s) from **Available Devices**.
6. Click one of the following options:
 - a. **Schedule** to backup the .cfg file of the target device(s) at a scheduled time.
 - b. **Backup** to backup the .cfg file of the target device(s) immediately.

Saving backed up Config files locally

About this task

Perform this procedure to view, to download, or to copy files from the server to your local desktop or PC.

The backup files are always on the server. From a remote browser connection you can view the device files, or copy the device files locally.

Note:

This functionality is available only when a TFTP server is in use.

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the Action menu, select **Save Backed up Config Files to Local**.

The Download Files window displays the files that have been successfully backed up.
3. Select the files to download.
4. Select the location to save the file, and then click **OK**.

Restoring the configuration file

About this task

Perform this procedure to restore the configuration for the target device(s).

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the Action menu, select **Restore Config File**.

The Inventory Manager - Restore Config File window displays.
3. Type the TFTP Server information.
4. Click **config.cfg** or **boot.cfg**.

config.cfg is selected by default.
5. Select the device(s) from **Available Devices**.

6. Click one of the following options:
 - a. **Schedule** to restore the .cfg file of the target device(s) at a scheduled time.
 - b. **Restore** to restore the .cfg file of the target device(s) immediately.

Archiving the configuration file

About this task

Perform this procedure to archive the configuration for the target device(s).

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the Action menu, select **Archive Config File**.

The Inventory Manager - Archive Config File window displays.
3. Type the TFTP Server information.
4. Click **config.cfg** or **boot.cfg**.

config.cfg is selected by default.
5. Click **Archive Changed Config Only** to archive the changed config files only.
6. Select the device(s) from **Available Devices**.
7. Click one of the following options:
 - a. **Schedule** to archive the .cfg file of the target device(s) at a scheduled time.
 - b. **Archive** to archive the .cfg file of the target device(s) immediately.

Synchronizing the configuration file

About this task

Perform this procedure to synchronize the configuration for the target device(s).

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the Action menu, select **Synchronize Config File**.

The Inventory Manager - Synchronize Config File window displays.
3. Type the TFTP Server information.
4. Click **config.cfg** or **boot.cfg**.

config.cfg is selected by default.
5. Select the device(s) from **Available Devices**.

6. Click one of the following options:
 - a. **Schedule** to synchronize the .cfg file of the target device(s) at a scheduled time.
 - b. **Synchronize** to synchronize the .cfg file of the target device(s) immediately.

Performing a device upgrade

About this task

Perform the following procedure to upgrade devices.

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the Action menu, select **Device Upgrade**.

The Inventory Manager – Device Manager window displays.
3. Type the TFTP Server information.
4. Type the ImageFileName information.
5. Type the 450ImageFileName information.
6. Select the device(s) from **Available Devices**.
7. Click one of the following options:
 - a. **Schedule** to perform an upgrade at a scheduled time.
 - b. **DeviceUpgrade** to upgrade the device immediately.

Using the Device Upgrade Wizard

About this task

Perform this procedure to open the Device Upgrade Wizard form.

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the Action menu, select **Auto Upgrade Wizard**.

The Inventory Manager - Device Upgrade Wizard form displays.
3. Select the device(s) from Available Devices.
4. Select boot.cfg or config.cfg files or both to save to a specified location.
5. Select flash or TFTP Server as the backup location.
 - If you select flash, you can accept the default boot.cfg and config.cfg file names or type a new file names.

- If you select TFTP Server, type the TFTP Server IP address
6. Type the **CLI User Name** and **CLI Password**.
 7. Select one of the following locations to show the image file:
 - flash
 - PCMCIA
 - TFTP ServerType the TFTP Server IP address, if you select TFTP Server as the file location.
 8. Click one of the following options:
 - a. **Schedule** to apply the changes for the target device(s) at a scheduled time.
 - b. **Apply** to apply the changes for the target device(s) immediately.

Comparing Runtime configuration file

About this task

Perform the following procedure to compare the runtime configuration for the specified device(s) with the external configuration file.

Procedure

1. Select **Backup & Restore > File Inventory**.
2. From the Actions menu, select **Compare Runtime Config With Existing Config**.

The Compare Runtime Config With Existing Config window displays.

Compare Runtime Config with Existing Config

TFTP Server:

File Name For RuntimeConfig to be saved:

Existing Config to be Compared with: No file selected.

Select Device:

3. Type the TFTP Server information.
4. Type the file name for the RuntimeConfig file.
5. Click **Browse** to browse to the location where the existing configuration file to be compared is saved.
6. Select the applicable device from the list.

7. Click **Compare**.

Setting File Inventory preferences

You can set preferences for displaying and managing devices in the File Inventory view.

Setting device management preferences

Procedure

1. Select **Backup & Restore > File Inventory**.
2. Click **Preferences** icon from the tool bar.
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/3XXX, Eth.Switch/ERS25XX, Alteon, WLAN_AP, WC8180, APLS, VSP4XXX, VSP72XX, VSP8XXX, VSP9XXX, VSP7024XLS, VSP7024XT.
 - Manage by sub-network—allows you to insert or delete subnetworks. If you select this option, only the assigned devices in the selected subnetworks are used in the next discovery process.
 - Manage by network layers—allows you to manage devices based on the network layers: Layer-2 or Layer-3.
 - Manage by selected devices—allows you to manage a particular group of devices; you can select devices from the Available Devices. If you select this option, the File Inventory view 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 20: Viewing Audit Logs






About Audit Logs

All Configuration views send log messages to audit and debug logs. In the audit log, you can configure and perform the following audit log functions:

- export logs
- filter logs
- generate a report
- refresh logs
- archive logs

Audit Logs toolbar

The following table identifies the available options in the Audit Logs toolbar.

Tool	Toolbar button	Description
Show filter		Allows you to sort the logs by a specific time period, audit level, user, access type, source, device IP address, or log message.
Refresh		Refreshes the table of audit log messages.
Export		Exports to CSV or to TXT.
Report		Reports the logs based on a specific time period, audit level, user, access type, source, device IP address, or log message.
Help		Offers more background information on the use of Audit Logs.

Launching the Audit Log view

Procedure

Expand **Reports > Audit Logs**.

Result

The Audit Log view displays the audit log listings.

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 system 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, MLT, Multicast, Multimedia, Routing, Security, Trap/Log Registration, VLAN, VPN, VRF, and BCM.
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

Procedure

1. Select **Reports > Audit Logs**.
2. In the Audit Log dialog box, click **Export**.
3. From the Export drop-down menu, select **Export to CSV** or **Export to TXT**.
4. In the File Download dialog box, click **Save**.
5. In the Save As dialog box, click **Save in** to browse to the directory for saving the audit log file.
6. In the File name field, type a name for the audit log file.
7. Click **Save**.

Filtering audit logs

Procedure

1. Select **Reports > Audit Logs**.
2. In the Audit Log dialog box, click **Show Filter**.
3. In the Audit Log Filter dialog box, complete the fields as required.

The screenshot shows the 'Audit Log Filter' dialog box. It contains the following fields and values:

- Past:** Week
- From:** 09/05/2016 3:43 PM
- To:** 09/12/2016 3:43 PM
- Audit level:** INFO
- User:** (empty)
- Access type:** (empty)
- Source:** (empty)
- Device IP:** (empty)
- Log Message:** (empty)

At the bottom of the dialog are three buttons: **Apply**, **Clear**, and **Cancel**.

4. Click **Apply** to commit the changes or click **Cancel** to discard the changes.

Result

The audit log data displays according to the selected filters.

Audit Log Filter field descriptions

Field	Description
Past	Specifies the duration for which audit log messages are fetched. Settings are: Hour, Day, Week, Month, and Specific.
From	Specifies the start date for fetching audit log messages. This setting is enabled when the Past field is set to Specific.
To	Specifies the end date for fetching audit log messages. This setting is enabled when the Past field is set to Specific.

Table continues...

Field	Description
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

Procedure

1. Select **Reports > Audit Logs**.
2. In the Audit Log dialog box, click **Refresh**.

Result

The audit log details are refreshed.

Generating Audit Log reports

Procedure

1. Select **Reports > Audit Logs**.
2. In the Audit Log dialog box, click the **Report** icon.

3. In the Audit Log Report dialog box, select the required options.

4. Click **Generate Report**.

Result

The BIRT Report Viewer displays the generated report . The report can contain a maximum of 50 entries.

To navigate through the report, type a page number in the **Go to page** field, or click the forward and back buttons.

Next steps

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 field descriptions

Field	Description
Report Type	Specifies the type of report to be generated. The available reports are: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Hour • Day • Week • Month • Specific
From	Specifies the start date for audit log message collection. This field is enabled only if the Past field is set to Specific. Specifies the start time for audit log message collection. This field is enabled only if the Past field is set to Specific.
To	Specifies the end date for audit log message collection. This field is enabled only if the Past field is set to Specific. 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.
Log Message	Specifies whether audit log messages are to be filtered based on message contents.

Archiving audit logs

About this task

The system 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

1. From the main menu tab, click **Preferences**.
2. Click **Configuration**.
3. Click on the **Logging** tab.
4. 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.
5. Select **Archive audit logs before purging to**.

The audit logs are automatically saved to the following location: `/opt/avaya/smgr/com/log/Audit_Archives`.

6. Click the **Archive** button.
7. Click **OK**.
8. Click **Save Preferences**.
9. A dialog box displays indicating that the changes were saved.
10. Click **OK**.

Deleting audit logs

About this task

The 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

1. From the main menu tab, click **Preferences**.
2. In the Preferences window, click **Configuration > Logging**.
3. In the Logging window, 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 the **Archive** button.
6. Click **OK** to confirm the archiving.
7. Click **Save Preferences**.

Result

A confirmation dialog box displays indicating that the changes are saved successfully.

Chapter 21: Wizard

Wizard

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:

- Steps—Displays the current wizard step.
- Wizard Description—Displays 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, then you can also run VLAN Wizard. Similarly, the users who have access to MLT can also run SMLT Wizard.

VLAN wizard features

You can use VLAN wizard to configure spanning tree groups (STG) – Avaya STG and MSTP, and Switched UNI VLANs in multiple devices.

VLAN wizard provides the following features:

- Select STG type and Device(s)
- Add/Select STG
- Add VLAN: you can add one or more VLANs under selected STG
- Configure Port Members
- Configure Private VLAN Type
- Configuration and Template

VLAN wizard can run in standalone mode. The VLAN data, which is used in VLAN wizard, can be created or loaded from a VLAN template.

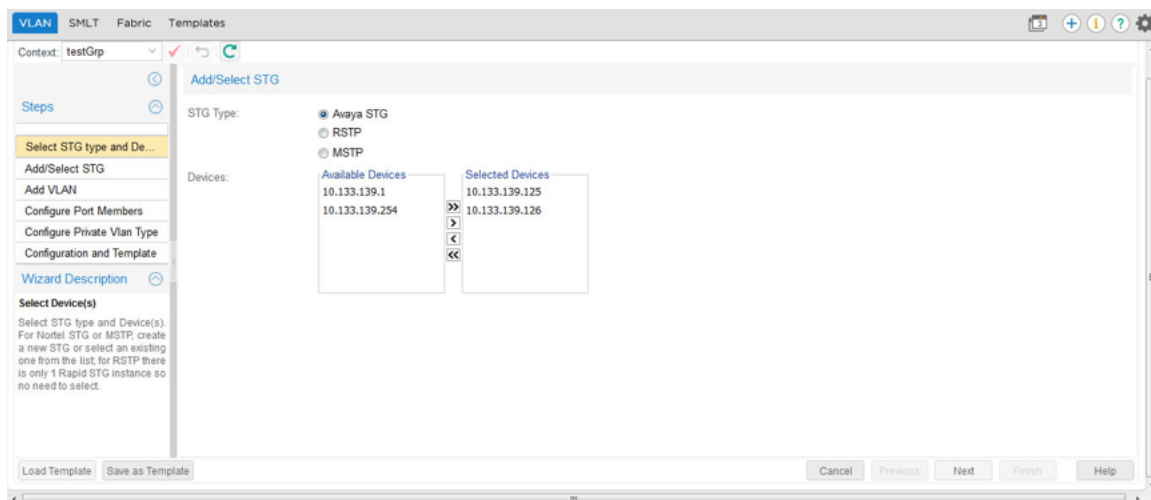
Selecting STG type and devices

Perform the following procedure to select an STG type and devices.

Procedure steps

1. Select **Wizard > VLAN**.

The VLAN Wizard dialog box displays.



2. In the Select STG type and Device(s) Steps section, in the Add/Select STG content pane, select the STG type.
3. Select the devices.
4. To move to the Add/Select STG page, click **Next**.

Adding or selecting an STG

Before you begin

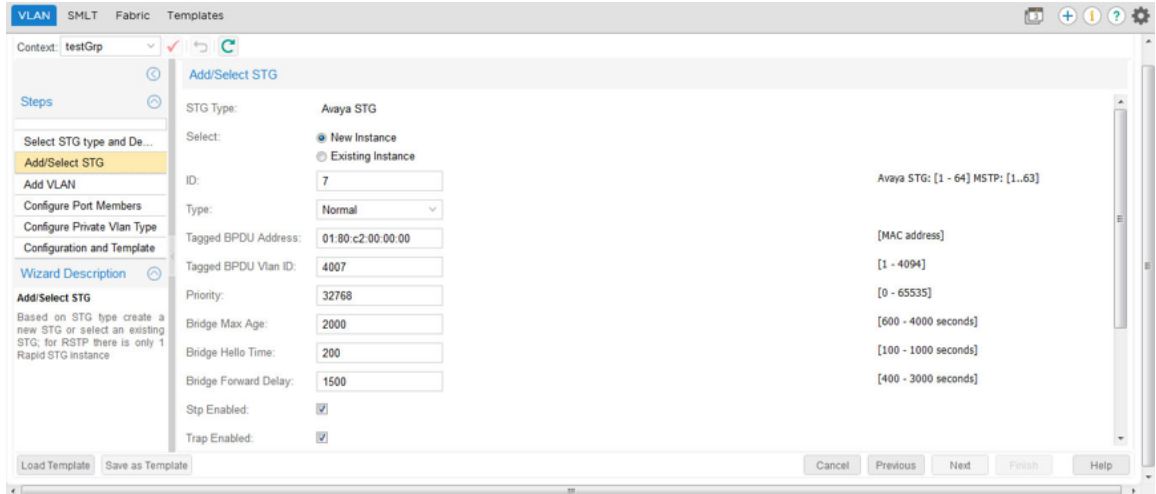
- Select **Wizard > VLAN**.
- Perform the procedure for selecting STG type and devices.

* Note:

The STG/MSTP id is not used in case of spbm-bvlan for VSP 7000.

Procedure

1. In the Add/Select STG page, perform one of the following:
 - Choose **New Instance** in the **Select** field to add a new MSTP instance.
 - 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 to the Add VLAN page.

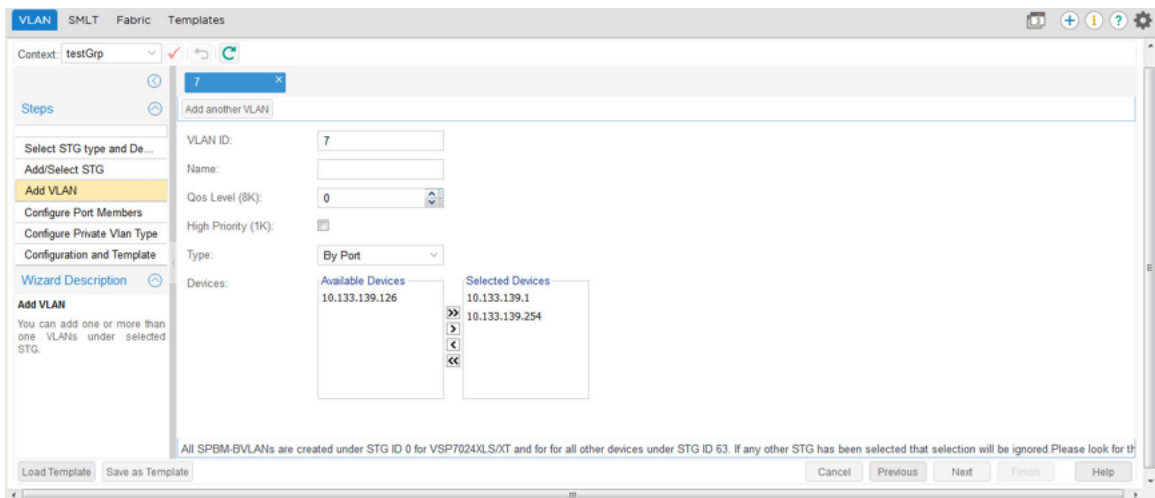
Adding a VLAN

Before you begin

1. Select **Wizard > VLAN**.
2. Perform the procedure for selecting STG type and devices.
3. Perform the procedure for adding or selecting an STG.

Procedure

1. In the **Add VLAN** page, enter information in all the fields to add a VLAN in the wizard.



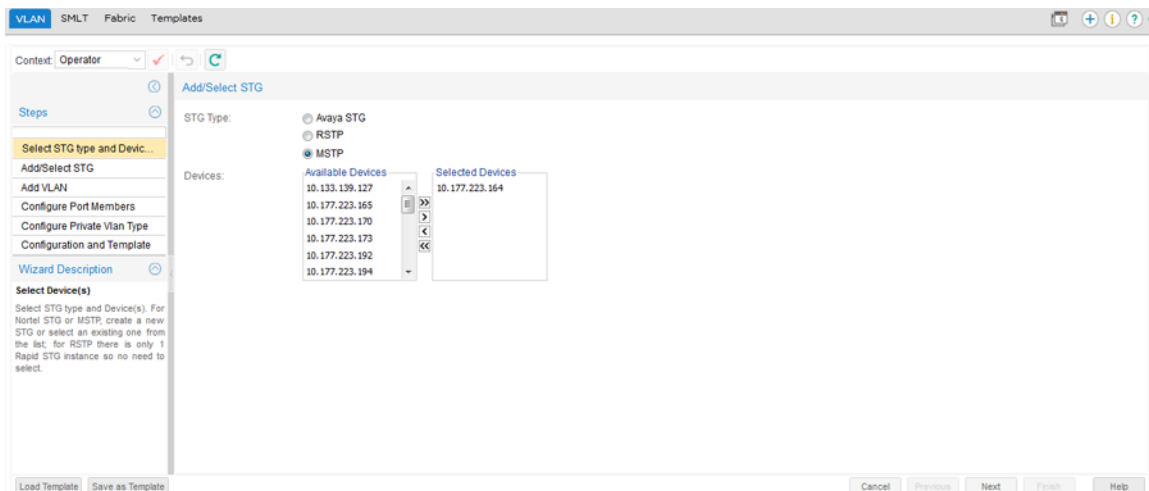
2. Choose the devices you wish to add from the **Available Devices** list, and then click the right-pointing arrow to move the devices to the **Selected Devices** list.
3. Click **Next** to move on Configure Port Members page.

Selecting MSTP or RSTP type and devices

Perform the following procedure to select MSTP or RSTP type and devices.

Procedure steps

1. Select **Wizard > VLAN**.
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

Before you begin

1. Select **Wizard > VLAN**.
2. Perform the procedure for selecting MSTP or RSTP type and devices.

* Note:

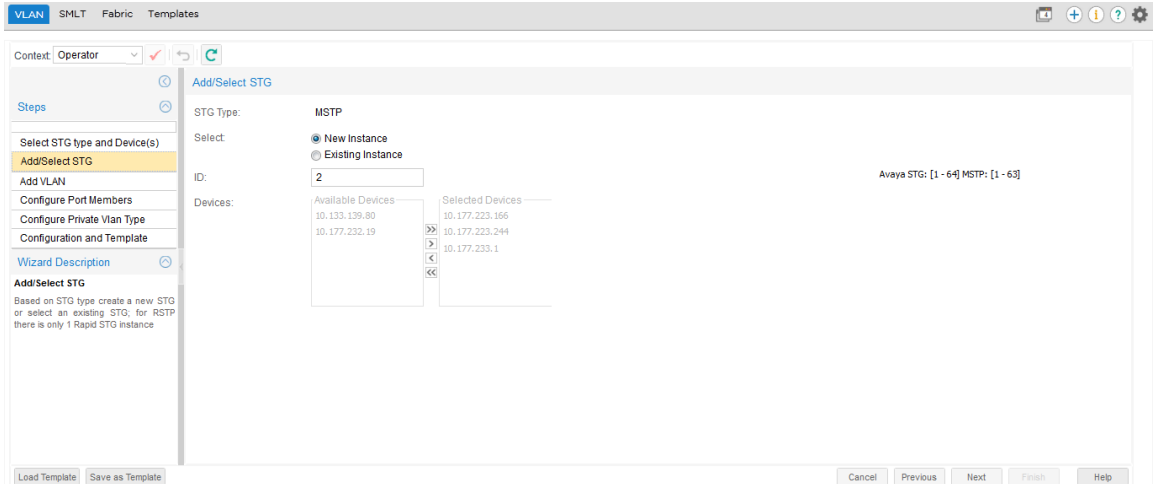
The STG/MSTP id is not used in case of spbm-bvlan for VSP 7000.

Procedure

1. Select **Wizard > VLAN**.
2. You must first enter information into the Select the STG type and Device(s), and click **Next**.
3. In the **Select** field, choose from one of the following two options:
 - To add a new MSTP instance, choose **New Instance**.

OR

 - To add an existing instance, choose **Existing instance**.



4. Select the devices.
5. Click **Next** to move on Add VLAN page.

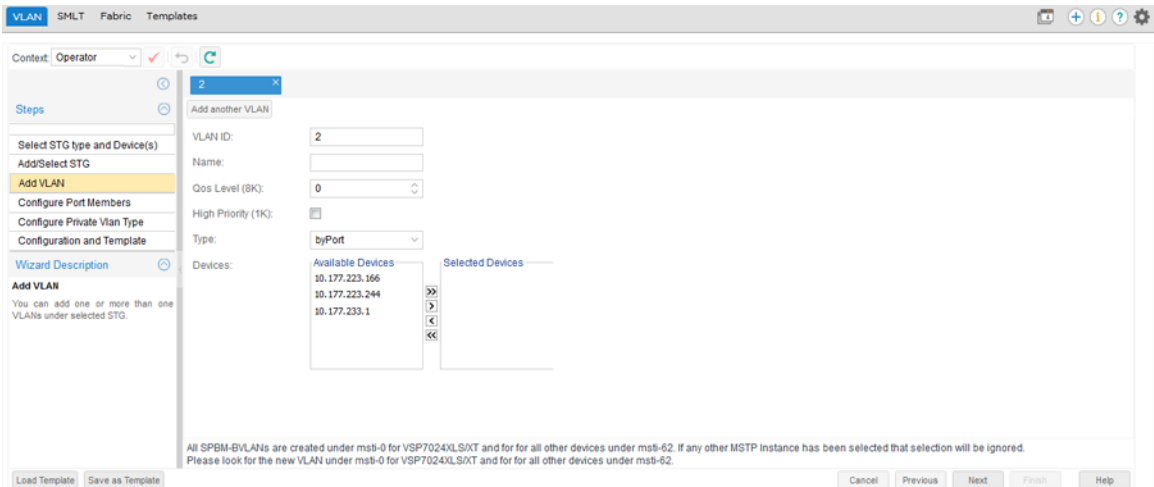
Adding a private VLAN

Before you begin

1. Select **Wizard > VLAN**.
2. Perform the procedure for selecting MSTP or RSTP type and devices.
3. Perform the procedure for adding or selecting an MSTP or RSTP.

Procedure

1. Select **Wizard > VLAN**.
2. In the Select STG type and Device(s) page, enter information and click **Next**.
3. In the Add/Select STG page, add or select an STG, and click **Next**.
4. In the **Add another VLAN** page, enter information in all the fields to add a VLAN in the wizard.



5. Select **By Private**.
6. Enter the secondary VLAN ID.
7. 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.
8. Click **Next** to move on Configure Port Members page.

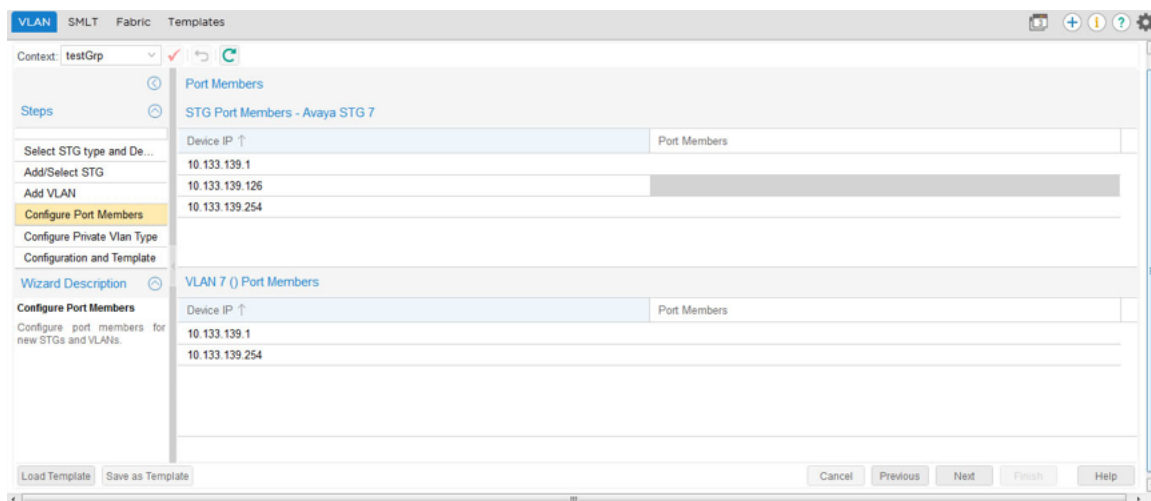
Configuring port members

Before you begin

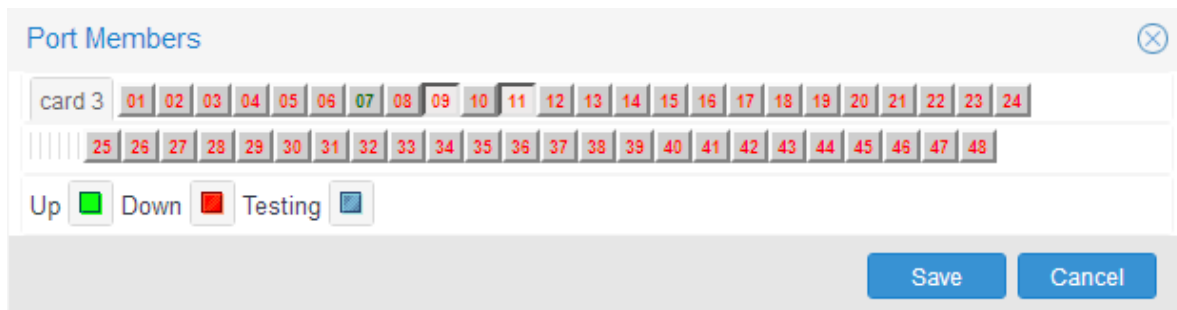
- Perform the procedure for selecting STG, MSTP or RSTP type and devices.
- Perform the procedure for adding or selecting an STG, MSTP or RSTP.
- Perform the procedure for adding a VLAN.

Procedure

1. In the Configure Port Members page, double-click in the **Port Members** cell to add ports to the device.



2. In the Port Members dialog box, select the ports you want to add by clicking on port numbers, and click **Save**.



3. In the Configure 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 procedure is required when the added VLAN type is private.

Saving VLAN configuration as template

Before you begin

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.

Configure port members.

About this task

Procedure

1. In the **Configuration and Template** page, select the **Save As Template** check box.
2. Enter the template name in the **Template Name** field.
3. Click **Finish**.

Loading a template in the VLAN wizard

Procedure

1. Select **Wizard > VLAN**.
2. In the VLAN Wizard dialog box, click **Load Template**.
3. Enter the name of the template file in the **Template Name** field, and click **Load**.

SMLT wizard

The SMLT wizard is a simplified and workflow driven wizard in the 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 CLI. 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.

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 InterSwitch Trunk configuration to define SMLT Topology Objects (Triangles).
- Creating SMLT/SLT—Helps you to create multiple trunks on the selected devices. The selections can be saved into a template, and reused if necessary.

SMLT configuration wizard has the following advantages over manual configuration:

- Efficient configuration
- Higher consistency of configuration
- Consistent and easy CLI commands and steps across devices
- Configures as a single workflow
- Ability to save and restore configuration
- Ability to apply the configuration to devices and view results

Launching SMLT Wizard

About this task

* Note:

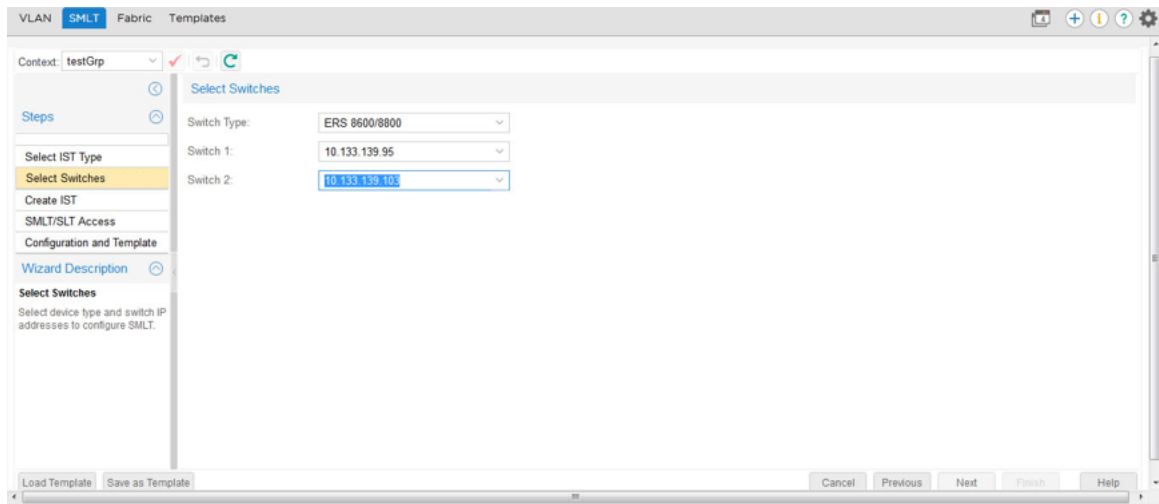
For VSP 9000 devices, there is no SMLT ID. To create a SMLT for VSP 9000 devices, you must enter a MLT ID. VSP 9000 supports the CLI.

Procedure

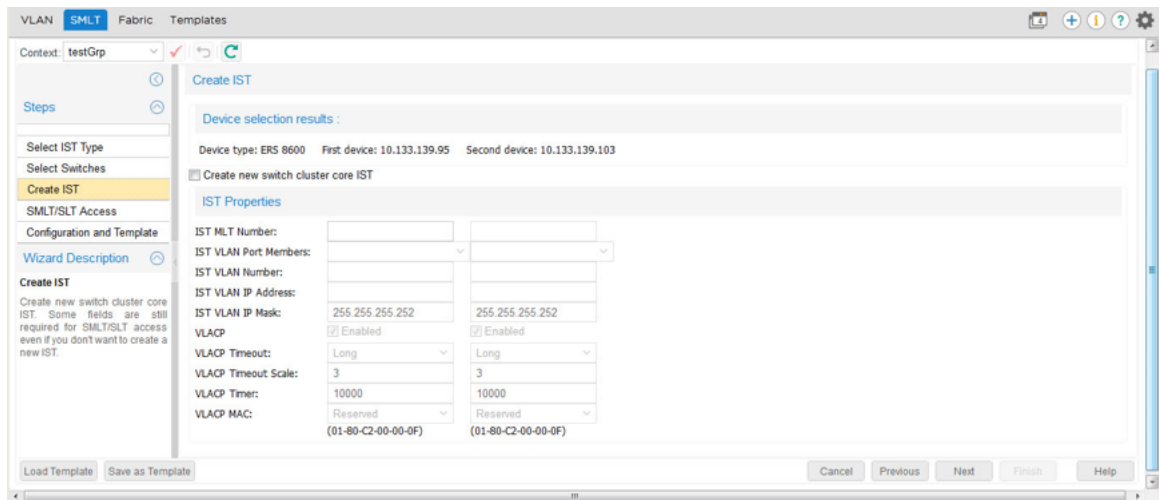
1. Select **Wizard > SMLT**.
2. Select **IST Type** or **VIST Type**, and then click **Next**.



3. Configure the following fields:
 - Switch Type: Enter a switch type from the list.
 - Switch 1: Enter a value from the list.
 - Switch 2: Enter a value from the list.



4. Click **Next**.
5. In the Create IST window, 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**.

8. In the SMLT/SLT access window, 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.

The screenshot shows the 'SMLT/SLT Access' configuration window. The 'Context' is 'Operator'. The 'Device type' is 'ERS 8600'. The 'First device' is '10.177.223.165' and the 'Second device' is '10.177.232.34'. The 'Create SMLT/SLT access' checkbox is checked. The 'Type' is 'SMLT'. The 'Add Access' button is highlighted. The 'Trunk Properties' section shows the following fields:

- SMLT Access Ports: [Dropdown]
- SMLT MLT Number: 4
- SMLT MLT Name: smlt-4
- SMLT ID: 4
- VLACP Enabled:
- VLACP Timeout: Short
- VLACP Timeout Scale: 5
- VLACP Timer: 500
- VLACP MAC: Default
- SLPP Enabled:
- SLPP Mode: Primary
- CP-Limit Modes: Aggressive

The 'VLAN Table' section shows a table with columns: Use, Id, Name, Sw1 VLA..., Sw2 VLA..., IP Mask, FDB..., SLPP, GwRedun..., VRRP IP, VRID, Sw1 VRR..., Sw2 VRR... The row for VLAN 19 is selected.

Use	Id	Name	Sw1 VLA...	Sw2 VLA...	IP Mask	FDB...	SLPP	GwRedun...	VRRP IP	VRID	Sw1 VRR...	Sw2 VRR...
<input checked="" type="checkbox"/>	19				255.255.2...	21601	<input checked="" type="checkbox"/>	RSMLT L2...				

9. In the New Access window, enter the ID of the new SMLT or SLT in the field of the New Access dialog box.

Important:

To disable the access of an SMLT you can click **Delete Access**

10. Click **OK**.

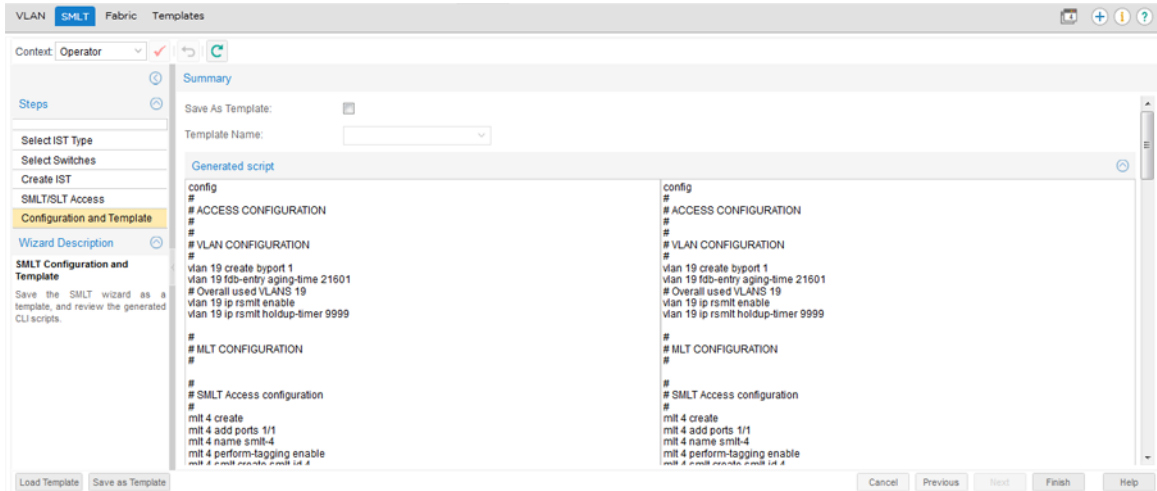
The SMLT Access or SLT Access forms are enabled. Depending on the SMLT and SLT, two forms are created.

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**.
17. 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.



18. In the SMLT Configuration and Template window, 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.
19. Provide a valid Template name or select the existing Template name if the selected template needs to be overwritten.
20. Click **Finish** to execute the commands on both devices.

Result

The wizard runs the command to show the SMLT/MLT configuration.

Create IST Trunk field descriptions

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.

Table continues...

Field	Description
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.

VLAN table field descriptions

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.

Launching SMLT with vIST wizard

Perform the following procedure to launch the SMLT wizard to create an SMLT using vIST.

Before you begin

- Enable SPBM and IS-IS globally.
- Configure SPBM and IS-IS.
- Configure a Layer 2 VSN by assigning an I-SID to the C-VLAN, which is used by the vIST.

Procedure

1. Select **Wizard > SMLT**.
2. Select **vIST Type**, and then click **Next**.
3. Create a VLAN and assign an ISID to the VLAN; this is used for vIST.
4. Select the IP address associated with each peer switch.
5. Click **Next**.
6. Select the **Create vIST** check box.
7. Enter the vIST VLAN ID number.
8. Enter the I-SID associated with the C-VLAN.
9. For each peer switch, enter the IP address associated with the vIST VLAN.
10. For each peer switch, enter the subnet mask associated with the vIST VLAN.
11. Click **Next**.
12. Select the **Create SMLT/SLT access** check box, choose the access type, and then click **Add Access** to provide access to a new SMLT.
13. Enter the ID of the new SMLT, and then click **OK**.

14. Enter the trunk properties to create an SMLT access. At a minimum, you must configure access ports.
15. Click **Add VLAN** in the VLAN Table to specify the properties of the VLANs to create or use for SMLT access.
16. Enter the VLAN ID. If you provide a VLAN ID that does not exist, the wizard creates the VLAN appropriately.
17. Enter the I-SID for the VLAN.
18. Select the **Use** check box beside the VLAN to use for each access.
19. Click **Next**.
The Summary page (Configuration and Template) appears. This page reviews the generated scripts and provides the option to save the SMLT wizard as a template and specify the template name.
20. Select the **Save as Template** check box to save the current SMLT wizard configuration as a template. After you select this check box, the **Template Name** text box becomes available.
21. Provide a valid template name or select the existing template name to overwrite the selected template.
22. Click **Finish** to issue the commands on both devices.

SMLT with vIST wizard field descriptions

The following tables describe the fields for the SMLT with vIST wizard.

Select IST Type

Name	Description
IST Type	Creates the SMLT using a traditional IST.
VIST Type	Creates the SMLT using a virtual IST.

Select Devices

Name	Description
Manual Area	Specifies the IS-IS manual-area (1–13 bytes in the format: <xx.xxx.xxx...xxx>
Switch 1	Specifies the IP address of the first peer switch.
Switch 2	Specifies the IP address of the second peer switch.

Create VIST

Name	Description
Create VIST	Creates a virtual IST channel between the peers.
Vlan Id	Configures a vIST VLAN ID number.

Table continues...

Name	Description
ISID	Specifies the I-SID associated with the C-VLAN.
Device IP	Specifies the IP addresses of the peer switches.
Vlan Ip	Specifies the IP addresses of the vIST VLAN on the peer switches.
Subnet Mask	Specifies the subnet masks for the vIST VLANs.

SMLT/SLT Access

Name	Description
Device type	Shows the type of device used for the peer switches.
First device	Shows the IP address of the first peer switch.
Second device	Shows the IP address of the second peer switch.
Create SMLT/SLT access	Creates the SMLT access and makes the trunk properties available for configuration.
Type	Specifies the access type.
SMLT Access Ports	Specifies the SMLT access port on each switch.
SMLT MLT Number	Specifies the SMLT MLT ID on each switch.
SMLT MLT Name	Specifies the SMLT MLT name on each switch.
VLACP Enabled	Enables or disables VLACP.
VLACP Timeout	Specifies the timeout control value. Specify long or short timeout.
VLACP Timeout Scale	Assigns the value used to calculate timeout time from the periodic time for all VLACP enabled ports. Timeout = PeriodicTime x TimeoutScale.
VLACP Timer	Specifies the number of milliseconds between periodic transmissions using short timeouts.
VLACP MAC	Specifies the multicast MAC address exclusively used for VLACPDUs.
SLPP Enabled	Enables or disables SLPP.
SLPP Mode	Specifies the SLPP mode, if enabled.
CP-Limit Modes	Specifies the CP-Limit mode.
Add VLAN	Adds a new VLAN entry to the table.
Delete VLAN	Removes the selected VLAN entry from the table.
Use	Identifies the VLAN to use for access.
Id	Specifies the VLAN ID.
Name	Specifies the VLAN name.
Sw1 VLAN IP	Specifies the VLAN IP address of the first switch.

Table continues...

Name	Description
Sw2 VLAN IP	Specifies the VLAN IP address of the second switch.
IP Mask	Specifies the subnet mask for the VLAN.
FDB Timer	Specifies the timeout period for dynamically learned MAC addresses on the VLAN.
SLPP	Enables or disables SLPP on the VLAN.
GwRedundancy	Specifies the gateway redundancy.
VRRP IP	Specifies the IP address of the virtual router interface.
VRID	Specifies a number that uniquely identifies a virtual router on a VRRP router. The virtual router acts as the default router for one or more assigned addresses.
Sw1 VRRP Prio	Specifies a priority value used by this VRRP router.
Sw2 VRRP Prio	Specifies a priority value used by this VRRP router.
IS-ID	Specifies the I-SID for the VLAN.

Configuration and Template

Name	Description
Save As Template	Save the wizard as a template.
Template Name	Specifies a name for the template.
Generated script	Shows the commands to complete the configuration.

Fabric wizard

The Fabric wizard navigation pane contains the following two sections:

- **Steps**—shows the current wizard step
- **Wizard Description**—shows the wizard description of current step

When you run the wizard, you can click **Save as Template** to save the wizard configuration as a template at any point. You can save as a new template or update an existing template.



Figure 44: Fabric wizard types

The following table outlines the supported device list for the Fabric wizard.

Supported device for Fabric wizard	Version	Wizard type supported
APLS	v4.3, v4.3.1	<ul style="list-style-type: none"> • SPB Infrastructure Wizard • L2 SPB Service Wizard • L3 SPB Service Wizard
ERS 4500	v5.7.2, v5.9	<ul style="list-style-type: none"> • SPB Infrastructure Wizard • L2 SPB Service Wizard
ERS 4800	v5.7.2	<ul style="list-style-type: none"> • SPB Infrastructure Wizard • L2 SPB Service Wizard
ERS 4900 and ERS 5900	v7.1, v7.2	<ul style="list-style-type: none"> • SPB Infrastructure Wizard • L2 SPB Service Wizard
ERS 8600 and ERS 8800	v7.1, v 7.1.3, v7.2.0, v7.2.10	<ul style="list-style-type: none"> • SPB Infrastructure Wizard • L2 SPB Service Wizard • L3 SPB Service Wizard
VOSS	v4.2.2, v4.2.3, v5.1, v5.1.1, v6.0	<ul style="list-style-type: none"> • SPB Infrastructure Wizard • L2 SPB Service Wizard • L3 SPB Service Wizard
VSP 4000	v3.0.1, v 3.1	<ul style="list-style-type: none"> • SPB Infrastructure Wizard • L2 SPB Service Wizard
VSP 7000	v10.1, v10.2, v10.3, v10.3.1 ¹	<ul style="list-style-type: none"> • SPB Infrastructure Wizard

Table continues...

Supported device for Fabric wizard	Version	Wizard type supported
		<ul style="list-style-type: none"> • L2 SPB Service Wizard <ul style="list-style-type: none"> - L2 SPB Service Wizard C Vlan UNI - L2 SPB Service Wizard Switched UNI - L2 SPB Service Wizard Transparent UNI • L3 SPB Service Wizard
VSP 7000	v10.4	<ul style="list-style-type: none"> • SPB Infrastructure Wizard • L2 SPB Service Wizard
VSP 8000	4.0	<ul style="list-style-type: none"> • SPB Infrastructure Wizard • L2 SPB Service Wizard
VSP 9000	v 3.2, v 3.3, v3.4, v4.0, v4.1	<ul style="list-style-type: none"> • SPB Infrastructure Wizard • L2 SPB Service Wizard • L3 SPB Service Wizard

1 — SPB Infrastructure and L2 SPB Service support only

Fabric wizard functionality

The Fabric wizard has the following wizard types:

- 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. Select **Wizard > Fabric**.

The Fabric Wizard dialog box appears.

2. In the Fabric Wizard dialog box, select **SPB Infrastructure Wizard**.

 **Note:**

For information about working offline, see [Offline mode](#) on page 481.

3. Click **Next**.

The Select Devices page appears.

4. In the Select Devices content pane, to move a device from the **Discovered Devices** list to the **Managed Devices** list, from the **Available Devices** list, double-click the device, or select the device, and click on the right pointing arrow.

Or

In the Select Devices content pane, to move all devices from the **Discovered Devices** list to the **Managed Devices** list, click the double right pointing arrow.

*** Note:**

- To clear a device, from the **Managed Devices** list, select the required item and click the left pointing arrow. To clear all devices, click the double left pointing arrows.
- 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**.

The system performs an IS-IS discovery, and the Operation Results page appears.

6. Click **Ok**.

The system performs an MLT discovery, and the Operation Results page appears.

7. Click **Ok**.

The Configure IS-IS page appears.

8. In the Configure IS-IS 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 IS-IS 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
Select Devices content pane	
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.
Configure ISIS content pane	
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.
Configure SPBM content pane	
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.

Table continues...

Field	Description
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> 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 Transparent UNI VLANs.

You can configure Switched UNI Vlans on the following devices as of the product release noted:

- APLS 4.3 and 4.3.1
- ERS 4500 5.7.2 and 5.9
- ERS 4800 5.7.2
- ERS 4900 7.1 and 7.2
- ERS 5900 7.1 and 7.2
- VOSS 4.2.2, 4.2.3, 5.1, 5.1.1, and 6.0
- VSP 4000 5.0
- VSP 7200 5.0
- VSP 8000 5.0
- VSP 7000 10.4
- VSP 9000 4.1

You can configure Transparent UNI on the following devices as of the product release noted:

- VSP 4000 3.1
- VSP 8000 4.2.1
- VSP 7200 4.2.1

Adding an L2 ISID with C-VLAN UNI type

Perform the following procedure to add an L2 ISID with CVLAN UNI type.

Procedure

1. Select **Wizard > Fabric**.
2. In the **Steps** navigation pane, click **Select Wizard Type**, and select the **L2 SPB Service Wizard** option.
3. Click **Next**.

The Select UNI Type window displays.

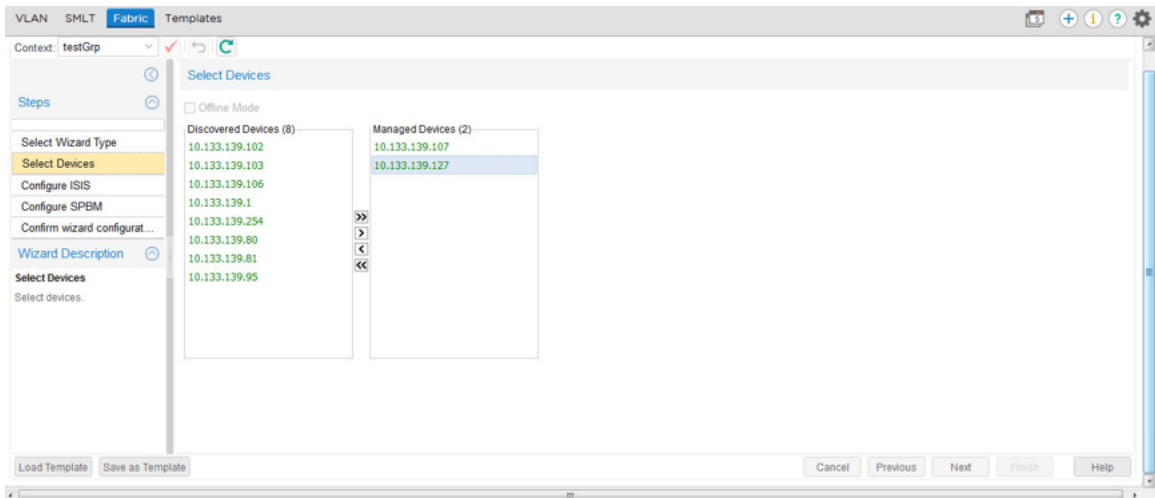
4. Click **C-VLAN UNI**, and click **Next**.



5. Move a device in the **Discovered Devices** field to the **Managed Devices** field:
 - To move a single device, select the device, and click > (right-pointing arrow).
 - To move all devices, click >> (double right-pointing arrows).

*** Note:**

To remove a device, in the **Managed Devices** field, select the device, and click < (left-pointing arrow). To remove all devices, click << (double left-pointing arrows).

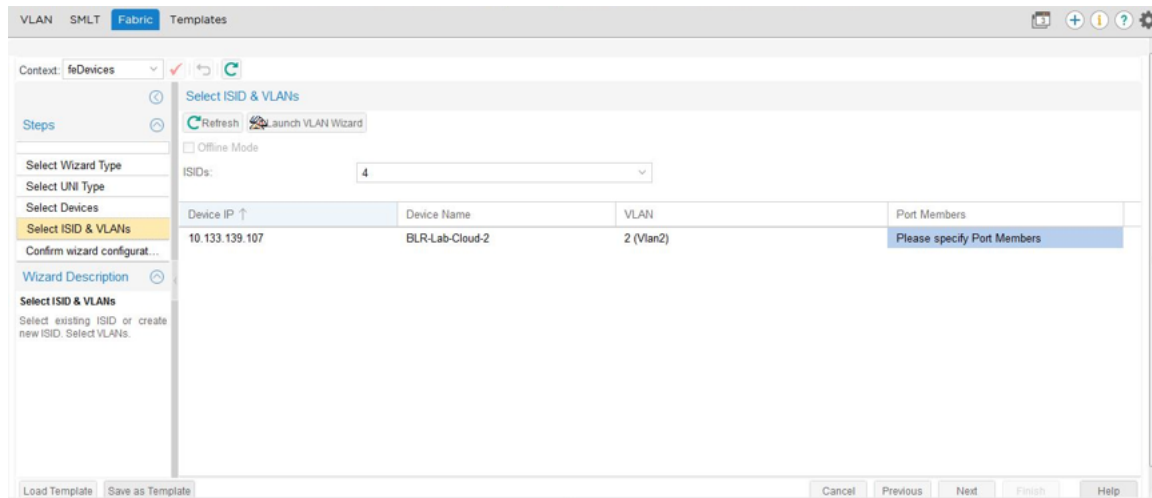


6. Click **Next**.

The system performs a Fabric discovery. the Operation Completed dialog box displays the results of the Fabric discovery.

- Click **OK**.

The Select ISID & VLANs page displays.



- In the **ISIDs** field, enter an ISID number.
- Select a VLAN from the list of devices. If there are no VLANs for a device, proceed to Step 11; otherwise, continue to Step 14.
- Click **Launch the VLAN Wizard** to add a new VLAN.
- Click the **Fabric Wizard** tab.
- Click **Refresh**, and select the VLAN.
- To view the information or make changes to the port currently mapped to the VLANs, in the **Port Members** column, double-click a cell for a specific device.
The Port Members window displays.
- Add or remove ports, then click **Save**.
- In the wizard frame, click **Next**.
- Click **Finish** or to save the wizard configuration as a template, perform the following steps:
 - Select the **Save as Template** check box.
 - Enter a Template name.
 - Click **Finish**.

Adding L2 ISID with Switched UNI type

Perform the following procedure to add an L2 ISID with Switched UNI type.

Procedure

- Select **Wizard > Fabric**.

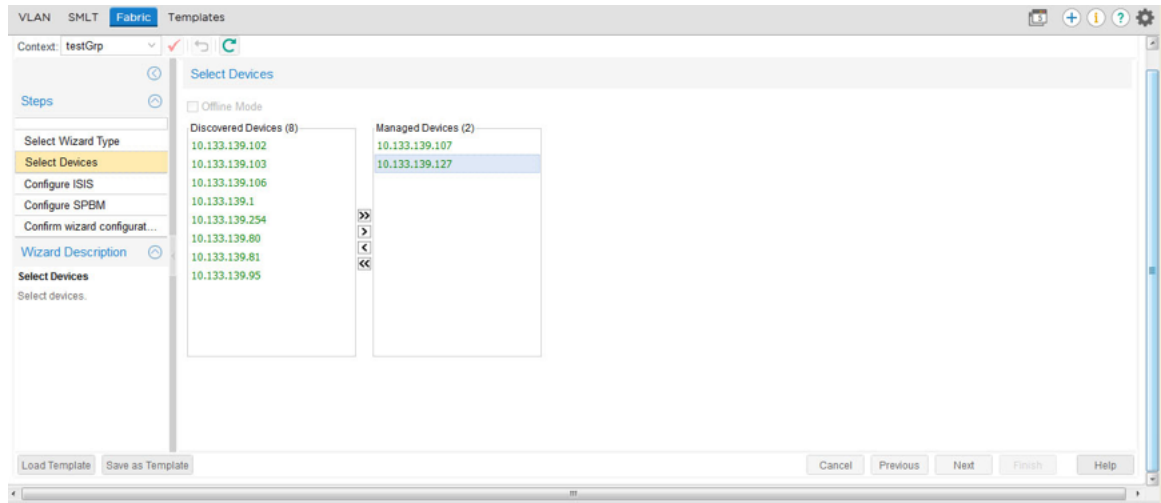
The Fabric Wizard dialog box opens.

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 **>**.
 - To move all devices from the Available Devices list to the Selected Devices list, click **>>**.

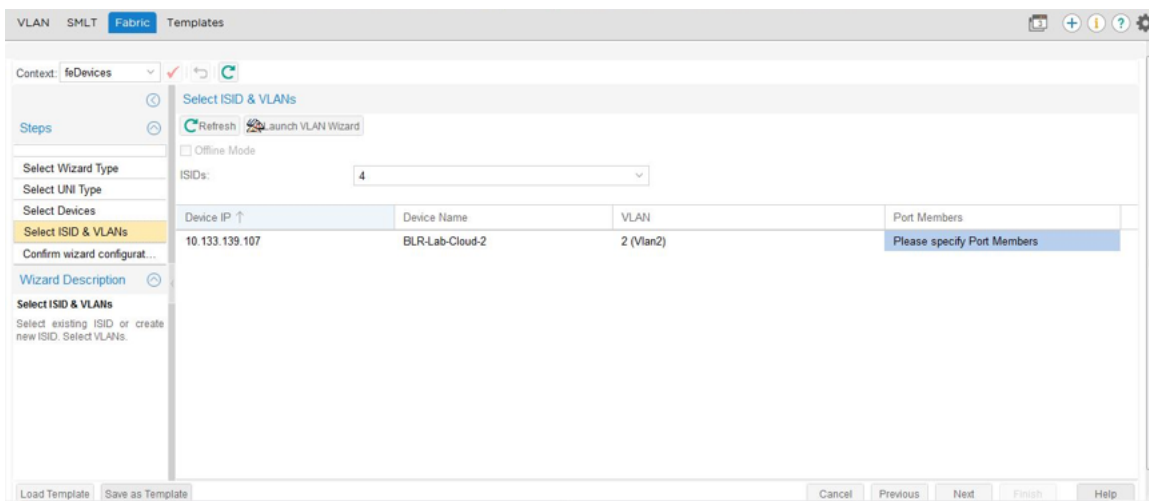
To unselect a device, from the Selected Devices table, select the required item and click **<**.
To unselect all devices, click **<<**.

7. Click **Next**.

The system 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

Perform the following procedure to add an L2 ISID with Transparent UNI type.

Procedure

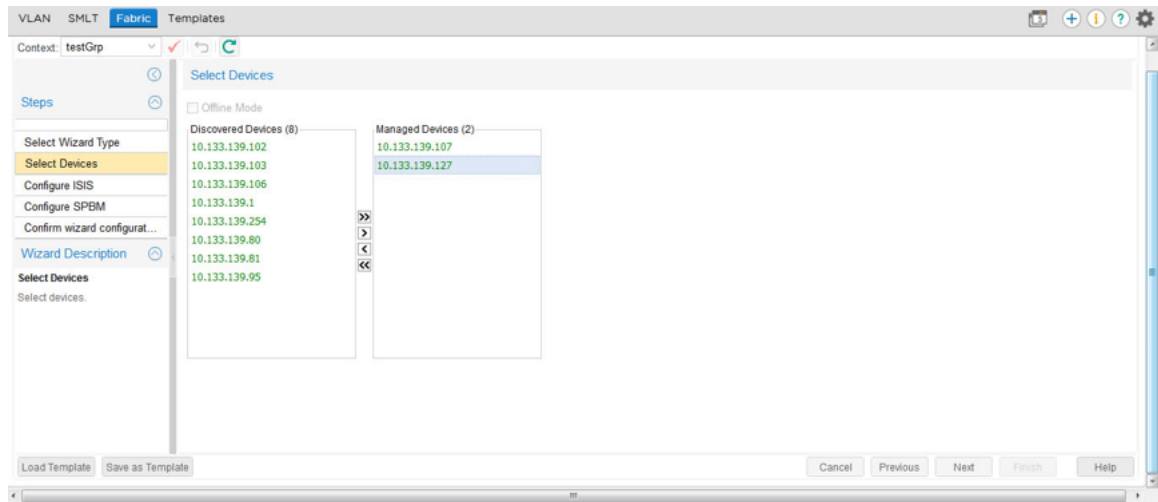
1. Select **Wizard > Fabric**.
The Fabric Wizard tab opens.
2. In the Select Wizard Type area in the Contents pane, select **L2 SPB Service Wizard**.

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 **>**.
- To move all devices from the Available Devices list to the Selected Devices list, click **>>**.

To unselect a device, from the Selected Devices table, select the required item and click **<**.
To unselect all devices, click **<<**.

7. Click **Next**.

The system 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 **Fabric 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**.

Adding L2 ISID with Flex UNI type

Use the following procedure to add an L2 ISID with Flex UNI type.

Procedure

1. Select **Wizard > Fabric**
2. In the Select Wizard Type area in the contents pane, select **L2 SPB Service Wizard**
3. Click **Next**.
4. Select **Flex UNI**.
5. Click **Next**.
6. From the Discovered Devices, select the required device or devices.
 - To move a device from the Discovered Devices list to the Managed Devices list, from the Discovered Devices list, select the corresponding row, and click **>**.
 - To move all devices from the Available Devices list to the Selected Devices list, click **>>**.To deselect a device, from the Selected Devices table, select the required item and click **<**.
To unselect all devices, click **<<**.
7. Click **Next**.
The system performs a VSN discovery and the Operation Completed box displays the results of the VSN discovery.
8. Click **Ok**.
9. On the Select ISID page, select an ISID number.
10. Click **Next**.
11. To confirm configuration, select **Save As Template**, and enter a template name.
- 12.

13. Click **Finish**.

Job aid

The following table describes the fields in the L2 SPB service wizard.

Field	Description
Select Devices content pane	
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.
Select ISID & VLANs content pane	
ISID	<p>Presents a combo box, that you can edit, with all ISID numbers that the system discovers from all compatible devices.</p> <p>Presents a table with all the devices that you selected in the Select Devices screen. The information includes the device IP/sysname, VLAN that you select, and port members for the VLAN you select. The VLAN table is visible only after you select the ISID number.</p>
VLAN column	Presents a drop-down combo box with all VLAN numbers that the system discovers on the device. If there is a VLAN assigned to a selected ISID on a device, then the system automatically selects the VLAN number and the selection is disabled.
Port Members column	Presents ports and MLTs that the system maps to the VLAN you select from the VLAN column. If you change the VLAN number, the system 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.
Confirm Configuration content pane	
Template Name	Presents a combo box with template names that you can edit. Enter a new template name or select from the available list.
CLI Script	Presents a screen that shows the CLI scripts running on the back end of the device.

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, the system 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, the system 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. Select **Wizard > Fabric**.

The Fabric 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 481.

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**.

The system 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**.

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**.

Adding a successful L3 VPN with the Fabric Wizard

Perform the following procedure to add a successful L3 VPN using the Fabric Wizard.

Procedure steps

1. Select **Wizard > Fabric**.

The Fabric Wizard window displays.

2. In the **Fabric 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 the device or select a device and click the right pointing arrow.

Or

To move all devices from the **Discovered Devices** list to the **Managed Devices** list, click the double right pointing arrows

*** Note:**

To clear a device, from the **Managed Devices** list, select the required item and click the left pointing arrow. To clear all devices, click the double left pointing arrows.

5. After you select your devices, click **Next**.

The system performs a VSN discovery, and the Operation Result box appears.

6. Click **Ok**.

The Select ISID & VRFs screen appears.

7. If you require a new VRF, click **Launch VRF Manager**.

For information about adding a new VRF, see [Adding VRF on a device or multiple devices](#) on page 166.

If configuration of any existing VRFs is changed or new VRFs are added, click on the **Fabric Wizard** tab, and click **Refresh**.

8. If you require a new VLAN, click **Launch VLAN Wizard**.

For information about adding a VLAN, see [Create and configure VLANs for an Avaya STG](#) on page 62.

If configuration of any existing VLANs is changed or new VLANs are added, click the **Fabric 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. In the **VLAN IP Address** and the **VLAN IP Mask** columns, enter 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 Fabric Connect view.

- 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.

Job aid

The following table describes the fields in the L3 SPB service wizard.

Field	Description
Select Devices content pane	
Discovered Devices	Devices that have a configured SPB infrastructure.

Table continues...

Field	Description
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.
Select ISID & VRFs	
ISID	Presents a combo box that you can edit, with all ISID numbers that the system discovers from all compatible devices. After you change the ISID, The system 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 the system 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 the system automatically selects the VRF number and disables the selection.
VLAN column	Presents a drop-down combo box with all VLAN ID numbers that the system 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 the system 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.

The following table describes the toolbar buttons in the L3 SPB service wizard.

Button	Description
Launch VLAN	Launches a pop-up window to create a VLAN for the required device.

Table continues...

Button	Description
	Refresh after the VLAN view updates.
Launch VRF	Launches a pop-up window to create a VRF for the required device. Refresh after the VRF view 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, the system 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 Fabric 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.
- The system does not discover information from the devices.
- You can enter any value into form fields; The system provides only basic validation because the device configuration is unknown.
- The system replaces the pull down combination boxes and lists with text fields you can edit.
- The system generates the CLI script but does not send it to the devices.
- The system 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 the system discovers from the devices.

Perform the following procedure to use the Offline Mode.

Procedure steps

1. Select **Wizard**, and select the appropriate wizard.
2. On the first page, select the **Offline Mode** check box.

Template support

All wizards support loading and saving configurations into template files.

If you use the template feature within the system 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.

Fabric Wizard

The Fabric 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 Fabric 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 Service 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 Fabric wizard does not load the configuration values connected to that IP address. However, the Fabric Wizard continues to discover the information from the network. The Fabric Wizard verifies the values loaded from the template against the values the Fabric Wizard discovers from the network. If you specify a value in the template that is invalid, then the Fabric Wizard resets the template, and you must specify the value again.

The Template Manager manages templates that you create in the Fabric Wizard. For more information about the Template Manager, see [Configuration of Templates](#) on page 482.

Configuration of Templates

The template contains a set of configuration attributes. Templates can be created by running the 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](#) on page 483.

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

Procedure

Select **Wizard > Templates**.

Result

The Templates window appears.




Templates window

Part	Description
Toolbar	Provides quick access to commonly used Template commands.
Contents pane	Displays details of the templates.

Templates toolbar

Icon	Name	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.
	Show	Displays the templates depending on the value selected. The available values are as follows: <ul style="list-style-type: none"> • All Templates • VLAN only • SMLT only

Table continues...

Icon	Name	Description
	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.

Templates contents pane

The Contents pane displays the details of the template based on the filter criteria.

- Template Name
- Type
- Last Modified By
- Last Modified Time

Double-click on a particular template to view the details.

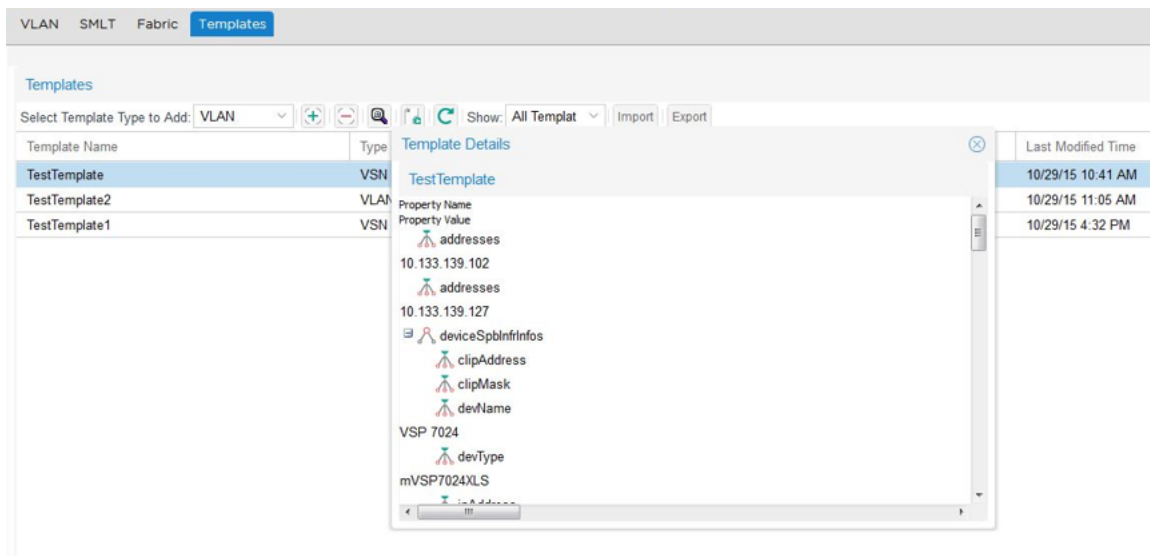


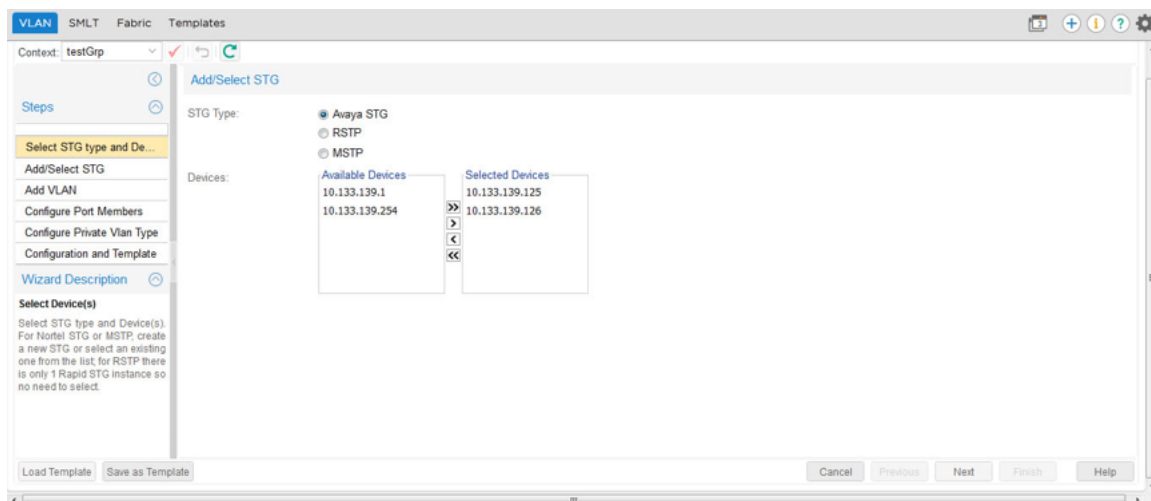
Figure 45: Template Details

Adding a VLAN template

Procedure

1. Select **Wizard > Templates**.
2. In the **Templates** window, select the VLAN template type from the **Select Template Type to Add** field.
3. Click **Add new template using wizard**.

The VLAN Wizard discovery occurs, and a Loading wizard data message displays. After the VLAN wizard discovery is complete, the VLAN Wizard window displays.



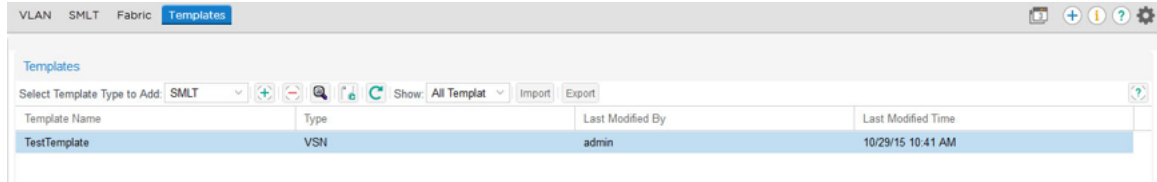
4. Select the **STG Type**.
5. From the **Available Devices** list, select a device and click the right-pointing arrow to move it to the **Selected Devices** list.
6. After you select the devices, click **Next**.
7. Enter the required values in the corresponding fields of Add/Select STG page.
8. Choose 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.
9. Click **Next** to move to the Add VLAN page.
10. 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.
11. Click **Next** to move on Configure Port Members page to view configuration details.
12. Click **Next** to move on Configure Private VLAN page to view configuration details.
This step is required when the added VLAN type is private.
13. Click **Next** to move on Configuration and Template page.
14. 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 450.
15. From the Template window, click **Refresh** to view the newly added template.

Adding an SMLT template

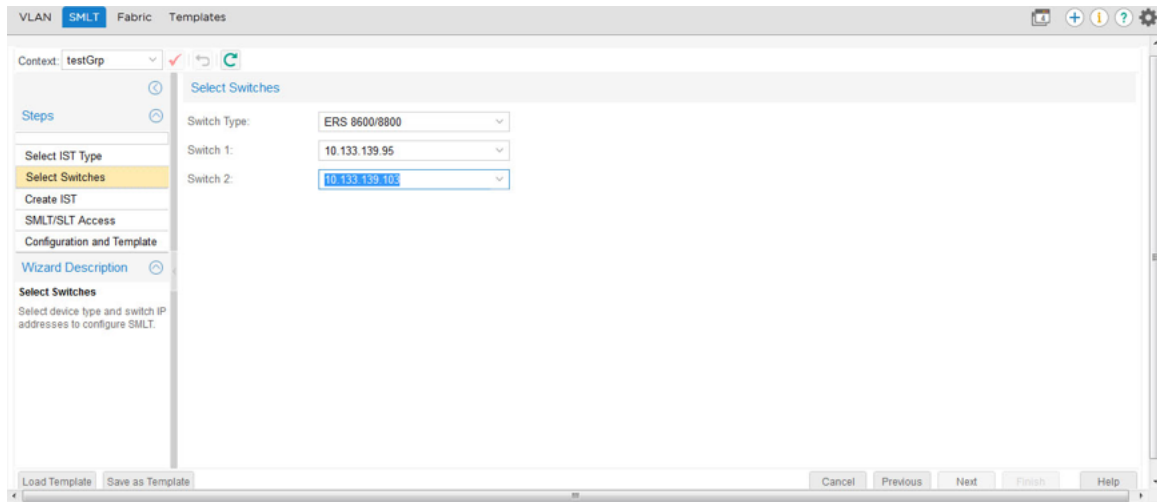
Procedure

1. Select **Wizard > Templates**.
2. In the **Select Template Type to Add** field, select **SMLT** from the list, and click **Add** from the toolbar.

Wizard



3. Click **Next**.
4. Enter the values in the fields as required, and click **Next**.



5. In the Create IST page, enter the values for creating the IST in the fields provided, and then click **Next**.
6. In the SMLT/SLT Access page, enter the required value in the corresponding fields, and then click **Next**.

Context: Operator

Device type: ERS 8600 First device: 10.177.223.165 Second device: 10.177.232.34

Create SMLT/SLT access:

Type: SMLT

Buttons: Add Access, Delete Access

SMLT 4

Trunk Properties

Trunk Properties		Trunk Properties	
SMLT Access Ports:		SMLT Access Ports:	
SMLT MLT Number:	4	SMLT MLT Number:	4
SMLT MLT Name:	smit-4	SMLT MLT Name:	smit-4
SMLT ID:	4	SMLT ID:	4
VLACP Enabled:	<input checked="" type="checkbox"/>	VLACP Enabled:	<input checked="" type="checkbox"/>
VLACP Timeout:	Short	VLACP Timeout:	Short
VLACP Timeout Scale:	5	VLACP Timeout Scale:	5
VLACP Timer:	500	VLACP Timer:	500
VLACP MAC:	Default	VLACP MAC:	Default
SLPP Enabled:	<input checked="" type="checkbox"/>	SLPP Enabled:	<input checked="" type="checkbox"/>
SLPP Mode:	Primary	SLPP Mode:	Secondary
CP-Limit Modes:	Aggressive	CP-Limit Modes:	Aggressive

VLAN Table

Buttons: Add VLAN, Delete VLAN

Use ...	Id	Name	Sw1 VLA...	Sw2 VLA...	IP Mask	FDB...	SLPP	GwRedun...	VRRP IP	VRID	Sw1 VRR...	Sw2 VRR...
<input checked="" type="checkbox"/>	19				255.255.2...	21601	<input checked="" type="checkbox"/>	RSMILT L2...				

Buttons: Load Template, Save as Template, Cancel, Previous, Next, Finish, Help

7. To save the configuration as a template, perform 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**.
8. Click **Refresh** to view the new template.

For more information about using the SMLT wizard, see [SMLT wizard](#) on page 456.

Adding a Fabric template

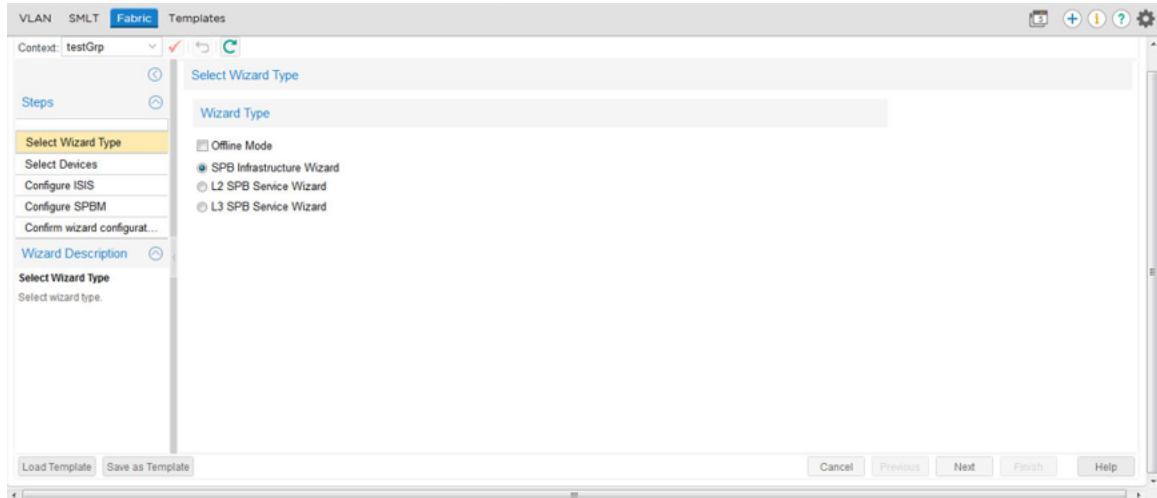
Perform the following procedure to add a Fabric template.

Procedure steps

1. Select **Wizard > Templates**.
2. In the **Templates** toolbar, in the **Select Template Type to Add** field, select **Fabric**.
3. In the **Templates** toolbar, click **Add new template using wizard**, which is the (+) sign.

The system launches the Fabric Wizard and displays the loading wizard data.

The Fabric Wizard window displays.



4. 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 466.

If you select the L2 SPB Service Wizard, see [Using the L2 SPB Service Wizard](#) on page 469.

If you select the L3 SPB Service Wizard, see [Using the L3 SPB Service Wizard](#) on page 477.

Deleting an existing template

Procedure

1. Select **Wizard > Templates**.
2. From the templates table, select the template you want to delete.
3. Click **Delete template** from the toolbar.

Result

The system deletes the selected template from the list.

Importing a template

Procedure

1. Select **Wizard > Templates**.
2. In the **Templates** window, click **Import**.
3. In the **Template file** field of the Select a template file to import window, perform one of the following options:
 - Enter the template file name in .xml format, and click **Import Template**.
 - Click **Browse** to navigate to the file, and click **Import Template**.

Exporting a template

Procedure

1. Select **Wizard > Templates**.
2. In the **Templates** window, select the template file you want to export, and then click **Export**.
3. You can choose one of the following options:
 - Click the **Open with** option, and select an option from the list to view the template file.
 - Click the **Save File** option, to save the file to a specific location.
4. Click **OK**.

Result

The selected template is exported from the system.

Running a template

Procedure

1. Select **Wizard > Templates**.
2. In the **Select Template Type to Add** field, choose a template from the list.
3. Click the **Run selected template** icon from the toolbar.

Result

The corresponding VLAN or SMLT wizard is launched with the template values.

Chapter 22: Tools

Tools

This chapter provides information about the tools supported under the **Tools** content pane, including the SmartDiff tool, MIB Browser, MIB Query, Port Scanner, Device Save Configuration, and Advanced Features.

*** Note:**

VSP 8000 does not support Device Config Save.

Starting SmartDiff Tool

Before you begin

About this task

With the SmartDiff tool you can compare two configuration files that have a .cfg extension.

Procedure

Select **Tools > Smart Diff**.

Result

The SmartDiff tool displays.

SmartDiff toolbar



Figure 46: SmartDiff toolbar

Icon	Description
1. Show differences	Shows differences between files.
2. Reset	Resets the input controls.
3. About	Provides information about SmartDiff.

Comparing configuration files

Procedure

1. Select **Tools > Smart Diff** .
2. In **First Config File** and **Second Config File** fields, enter the name of the configuration files you want to compare. Use the ... buttons to browse the files.

To reset the values in the **First Config File** and **Second Config File** fields, click **Reset the input controls**.

3. From the top-left toolbar, click **Show differences between files**. The File Diff Contents panel contains the output of compare operation.

The Status bar displays the comparison report including whether the files are identical or different, and the number of different lines. SmartDiff Tool highlights the content in three colors—white, blue, and yellow. The significance of these colors are as follows:

- Black text in a white background indicates the matched text in a line.
- Blue Text in a yellow background indicates any different text in the first line.
- White text in a blue background indicates any different text in the second line
- Black text in a grey background indicates the modified lines in the file.

To navigate from one modified section to the next, use the arrows in the toolbar.

MIB Browser

With the MIB Browser you can manage SNMP-enabled network devices and applications. You can browse and search MIBs, and perform all other SNMP-related functions using the MIB Browser. You can also view and operate the data available through an SNMP agent in a managed device.

The following figure shows the MIB Browser.

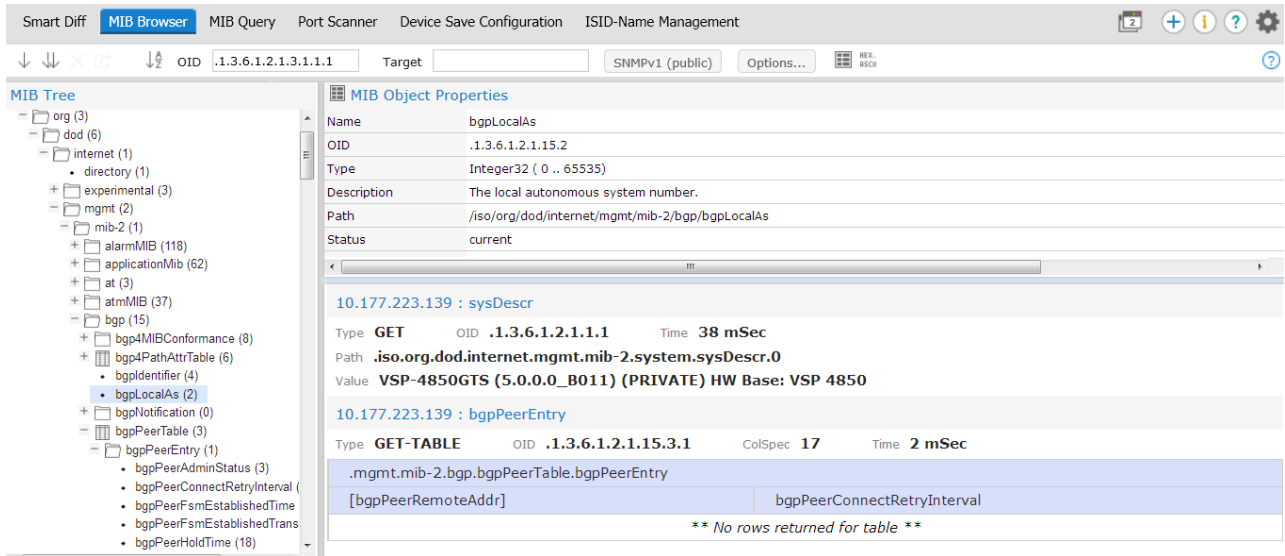


Figure 47: MIB Browser

The following table describes the parts of the MIB Browser.

Table 170: Parts of the MIB Browser

Part	Description
MIB Tree	Displays the currently loaded MIBs.
MIB Object Properties	Displays the details of the selected MIB name.
Toolbar	Provides quick access to commonly used SNMP commands.
Output Panel	Displays output of the operation performed using toolbar options.

The following table describes the tools available for the MIB Browser tab.

Table 171: MIB Browser tools









Icon	Tool	Description
	Get	Obtains the value of SNMP variables for a device.
	Get Next	Obtains the value of consecutive SNMP variables for a device.
	Clear results area	Clears the results of a Get or Get Next operation.
	Save last query results	Saves the results of a Get or Get Next operation as an XML file.
	Enable alphabetical mode	Sorts the MIB tree in alphabetical order.

Table continues...

Icon	Tool	Description
<input type="text" value="OID .1.3.6.1.2.1.1.1"/>	OID	Specifies the object identifier of a managed object in the MIB hierarchy.
<input type="text" value="Target"/>	Target	Specifies the IP address for the device.
<input type="button" value="SNMPv1 (public)"/>	Set SNMP Version	Sets the SNMP version. The available versions are as follows: <ul style="list-style-type: none"> • SNMP v1 • SNMP v2c • SNMP v3
<input type="button" value="Options..."/>	Options	Configures options for the device connection.
	Hide Properties	Shows or hides the MIB object properties.
	Trace on/off	Enables or disables tracing.
	Help	Opens Online Help.

Configuring SNMP version

Procedure

1. Select **Tools > MIB Browser**.
2. From the toolbar, click **SNMP** on the MIB Browser toolbar. The button can appear as SNMPv1, SNMPv2, or SNMPv3, depending on the configuration.



3. Choose the version that you want to set in the **Snmp Version** field.
4. Choose the Community that you want to set in the **Community** field.

Authentication... ✕

SNMP Version <input type="text" value="SNMPv1"/>	Username <input type="text"/>
Community <input type="text" value="public"/>	Auth Password <input type="text"/>
Auth Protocol <input type="text" value="NONE"/>	Privacy Password <input type="text"/>
Privacy Protocol <input type="text" value="NONE"/>	

5. If you select SNMPv3, complete the **Auth Protocol** and **Privacy Protocol** fields.
6. If you select SNMPv3, complete the **Username**, **Auth Password**, and **Privacy Password** fields.
7. Click **OK**.

SNMP-V3 Settings field descriptions

Field	Description
SNMP Version	Specifies the SNMP version to one of the following: <ul style="list-style-type: none"> • SNMPv1 • SNMPv2c • SNMPv3
Community	Specifies the community.
Auth Protocol	Specifies the authentication protocol, as one of the following: <ul style="list-style-type: none"> • NONE • MD5 • SHA <p>This option is only available if you select SNMPv3 as the SNMP version.</p>
Privacy Protocol	Specifies the privacy protocol as one of the following: <ul style="list-style-type: none"> • DES • 3DES • NONE • AES128 <p>This option is only available if you select SNMPv3 as the SNMP version.</p>
User Name	Specifies the SNMPv3 user name.
Auth Password	Specifies the password that is used for authentication purposes.
Privacy Password	Specifies the password that is used for privacy purposes.

Retrieving data of an MIB node

About this task

Perform the following procedure to retrieve the value of the leaf object from the managed objects.

Procedure

1. Select **Tools > MIB Browser**.

2. Select a node from the MIB tree.
3. Click **Get** on the MIB Browser toolbar on the top left.

Traversing the MIB tree

Procedure

1. Select **Tools > MIB Browser**.
2. Select a node from the MIB tree.
3. Click **Get Next** in the MIB Browser toolbar on the top left.

MIB Query

To access MIB query, select **Tools > MIB Query**.

You can view information about MIB queries by expanding the tree structure on the left side of the MIB Query page and selecting a query.

The MIB query information appears in the Results panel.

The following controls are available on the MIB Query page:

- Clear—Clears the query results.
- Execute—Starts the MIB query. Click the checkbox.
- Period—Displays the time period for the MIB query.
- Target—Displays an SNMP MIB based on an IP address.
- SNMP Version—Sets the SNMP authentication.
- Options—Adjusts the timeout value and retries.
- Switch to columns—Displays the results using columns.

From the queries panel, you can perform the following actions:

- Add—Adds a query.
- Delete—Deletes a query.
- Edit—Edits a query.

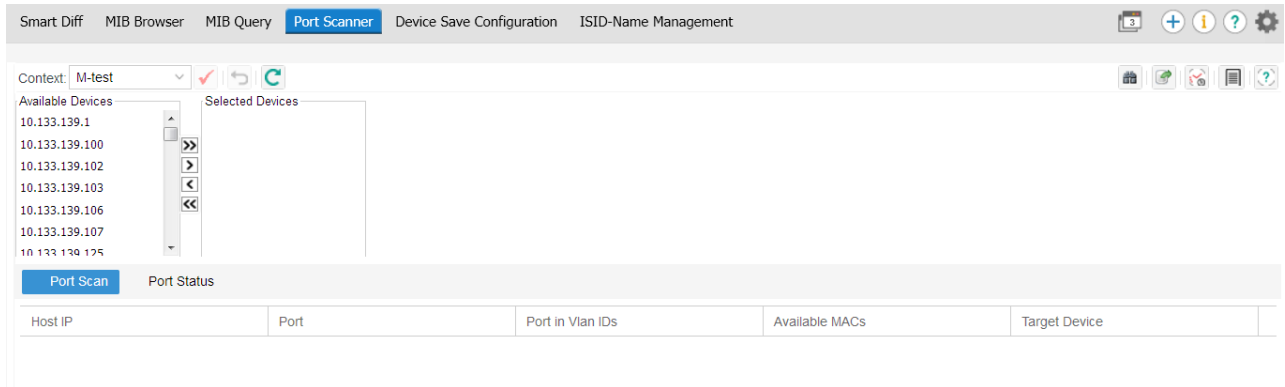
For more information about MIB Query, see *Network Monitoring using Extreme Fabric Orchestrator*, NN48100–500.

Accessing the Port Scanner

With the Port Scanner you can scan the target devices. Port Scanner enables parameters to configure periodic port scan, and store exported port scan data into files.

Procedure

Select **Tools > Port Scanner**.



Scanning Ports

Procedure

1. Select the **Tools > Port Scanner**.
2. In the **Available Device** field, select the devices you want to scan and use **>** or **>>** to move the devices to **Selected Devices** field.
3. Click **Scan Ports** from the toolbar on the top right.
4. Click **OK** to view results.

Result

The result appears in the content pane, in both the Port Scan tab and the Port Status tab.

Port Scanner tab field descriptions

Field	Description
Toolbar	Provides you with the following Port Scanner tools: <ul style="list-style-type: none"> • Scan Ports—scans the target devices. • Export—exports the result in text format. • Schedule Scan—schedules a scan. • View Scan Results—displays results of a port scan.
Available Devices	Contains a list of assigned devices.
Selected Devices	Contains devices selected from the Available Devices list.
>>	Use to move all the devices from the Available Devices list into the Selected Devices list.

Table continues...

Field	Description
>	Use to move the selected device from the Available Devices list into the Selected Devices list.
<	Use to move the selected device from the Selected Devices list to the Available Devices list.
<<	Use to move all the devices in the Selected Devices list to the Available Devices list.
Host IP	Specifies the IP addresses of the target devices.
Port	Specifies the device ports.
Port in Vlan ID	Specifies the VLAN ID of the ports present in the port attributes.
Available MACs	Specifies the MAC addresses of device ports.
Target Device	Specifies the IP address if the available MAC.

Port Status tab field descriptions

Field	Description
Host IP	Specifies the IP addresses of the target devices.
Port	Specifies the device ports.
Port Status	Specifies the status of the port.
Last Change	Specifies when the last port status change occurred.

Exporting a report of port scan

Procedure

1. Select **Tools > Port Scanner**.
2. In the **Available Device** field, select the devices you want to scan, and use **>** or **>>** to move the devices to the **Selected Devices** field.
3. Click the **Scan Ports** from the toolbar at the top right.
4. To export the report, from the toolbar at the top right, click **Export**.
5. Select **Text** or **Html**.
6. Select **port scan** or **port status**, or both **port scan** and **port status**.
7. Click **OK**.

Scheduling a scan

Perform the following procedure to schedule a scan of a device or devices.

Procedure

1. Select the **Tools > Port Scanner** to start the **Port Scanner** tool.

2. In the **Available Devices** field, select the devices you want to scan, and click the right-pointing arrow.
 - To select all devices, click the double right-pointing arrow.
 - To remove a device from the Selected Device list, select the device and click the left-pointing arrow.
 - To remove all devices from the Selected Device list, click the double left-pointing arrow.
3. Click **Schedule Scan** from the top-right toolbar.
4. Enter the Task Name.
5. Enter the Schedule Name.
6. Select a scheduled time frame of the scan.
7. Select the date and time of the scan.

If you select a schedule that does not require a date entry, the date field is unavailable.
8. Click **Set**.

Viewing scan results

Perform the following procedure to view scan results.

Before you begin

- You must schedule a scan before you can view the scan results.

Procedure

1. Select **Tools > Port Scanner** to start the **Port Scanner** tool.
2. In the **Available Devices** field, select the devices you want to scan, and click the right-pointing arrow.
 - To select all devices, click the double right-pointing arrow.
 - To remove a device from the Selected Device list, select the device and click the left-pointing arrow.
 - To remove all devices from the Selected Device list, click the double left-pointing arrow.
3. From the Port Scanner tool bar, click **Schedule Scan**.
4. Enter the Task Name.
5. Enter the Schedule Name.
6. Select a scheduled time frame of the scan.
7. Select the date and time of the scan.

If you select a schedule that does not require a date entry, the date field is unavailable.
8. Click **Set**.
9. From the Port Scanner tool bar, click **View Scan Results**.

10. To close the window, click **Ok**.

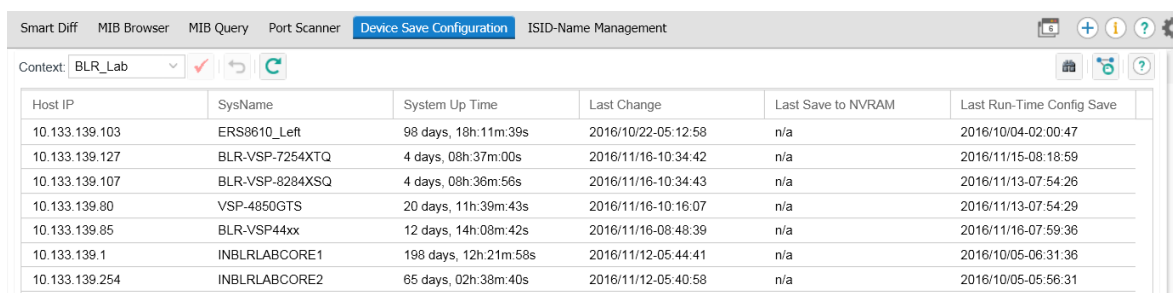
Device Save Configuration Tool

With the Device Save Configuration Tool, you can discover unsaved devices and save device configurations.

Perform the following procedure to start the Device Save Configuration Tool.

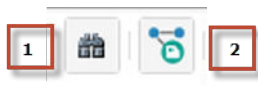
Procedure steps

1. Select the **Tools > Device Save Configuration** to start the **Device Save Configuration** tool.



Host IP	SysName	System Up Time	Last Change	Last Save to NVRAM	Last Run-Time Config Save
10.133.139.103	ERS8610_Left	98 days, 18h:11m:39s	2016/10/22-05:12:58	n/a	2016/10/04-02:00:47
10.133.139.127	BLR-VSP-7254XTQ	4 days, 08h:37m:00s	2016/11/16-10:34:42	n/a	2016/11/15-08:18:59
10.133.139.107	BLR-VSP-8284XSQ	4 days, 08h:36m:56s	2016/11/16-10:34:43	n/a	2016/11/13-07:54:26
10.133.139.80	VSP-4850GTS	20 days, 11h:39m:43s	2016/11/16-10:16:07	n/a	2016/11/13-07:54:29
10.133.139.85	BLR-VSP44xx	12 days, 14h:08m:42s	2016/11/16-08:48:39	n/a	2016/11/16-07:59:36
10.133.139.1	INBLRLABCORE1	198 days, 12h:21m:58s	2016/11/12-05:44:41	n/a	2016/10/05-06:31:36
10.133.139.254	INBLRLABCORE2	65 days, 02h:38m:40s	2016/11/12-05:40:58	n/a	2016/10/05-05:56:31

The following figure shows the Device Save Configuration Tool toolbar.



1. Discover Unsaved Devices
2. Save Device Configurations

ISID Name Management

With ISID Name Management you can assign names to service IDs and manage them network-wide so there are no duplications. This feature also provides the facility to create service groups which contain the service name and ID pairs. You can create, delete, modify, or retrieve the service group, name, or ID mappings.

Service Name	I-SID	Description	Added By User	Timestamp
Service Group: Multicast Video Services				
News Channel	130	Test1	admin	2016-10-21 11:14:44
Movies Channel	202	Test2	admin	2016-10-28 10:34:25
Service Group: Multicast Audio Services				
Classical Music Channel	1268	Test3	admin	2016-10-21 11:16:02
Film Songs Channel	1408	Test4	admin	2016-10-21 11:17:16
FA Service	10011	Test5	admin	2016-11-06 03:26:45

Figure 48: ISID Name Management

After you create the service name and id pairs, the system maps these service names in the following views:

- Fabric Connect — for Fabric-centric view, Device-centric view, and Fabric topology.

Adding a service group and name to an ISID

Procedure

1. Select **Tools > ISID Name Management**.
2. Click **Add**.
3. Select or enter a service group name.
4. Enter a service name.
5. Enter an ISID.

*** Note:**

Specify a value in the range 1 to 16777215.

6. **(Optional)** Enter a description of the ISID Name.
7. Click **Add**.
8. After you add the required ISID names, click **Close**.

Add ISID Name dialog box field descriptions

Field	Description
Service Group	Enter or select a service group name. You can enter 1 to 35 characters, including the following allowable characters: [a-z A-Z 0-9 space -].
Service Name	Enter a service name. You can enter 1 to 35 characters, including the following allowable characters: [a-z A-Z 0-9 space -].

Table continues...

Field	Description
ISID	Enter an ISID number from 1 to 16777215.
Description	Enter a description of the ISID Name that you are adding. This field is optional.

Managing service names and service groups

About this task

Use this procedure to view or edit the existing ISIDs mapped to the corresponding service names and service groups. You can edit the service name, ISID, and description.

Before you begin

- Ensure that you log on as an administrator.

Procedure

1. Select **Tools > ISID Name Management**.

The system displays the list of already mapped service names and service groups.

2. **(Optional)** To change the name of a service, double-click in the service name field, and enter a new name.
3. **(Optional)** To change the ISID associated with a service name, double-click in the ISID field, and enter a new ISID number.
4. **(Optional)** To change the descriptions associated with a service name, double-click in the Description field, and enter a new description.
5. Click **Save Changes**.
 - If you want to undo the changes that you made, click **Revert Changes**.

Manage ISID Names table field descriptions

Field	Description
Service Name	A unique name that you assign to an ISID. You can edit this field. Enter 1 to 35 characters that include the following allowable characters: [a-z A-Z 0-9 space -].
ISID	The ISID number. You can edit this field. Use a number from 1 to 16777215.
Description	The description of the service name associated with and ISID number that you enter when you add a service name. This field is optional. You can edit this field.
Added by User	The name of the user who entered the service name. This field is read-only.
Timestamp	The date and time the service name was created. This field is read-only.

Deleting a service group and name from an ISID

Procedure

1. Select **Tools > ISID-Name Management**.
2. Select a service name.
3. Click **Delete**.
4. To confirm deletion, click **Yes**.

Appendix A: Recommendations

Recommendations

The following sections describe how to resolve problems with configuration, and also describe the recommendations for those errors.

Rediscovery of devices

If the user performs a rediscovery, and some of the devices which were part of a created device group are not rediscovered, then those devices appear in red. These devices continue to appear in red until the user performs another discovery or removes the devices from the device group(s).

Internet browser settings

Certain security settings in Internet Explorer (IE) do not allow Java script execution. In this case, the login page does not display the login button.

Use the following settings for IE:

- To allow Java script execution, set the IE security settings to at least medium high or lower.

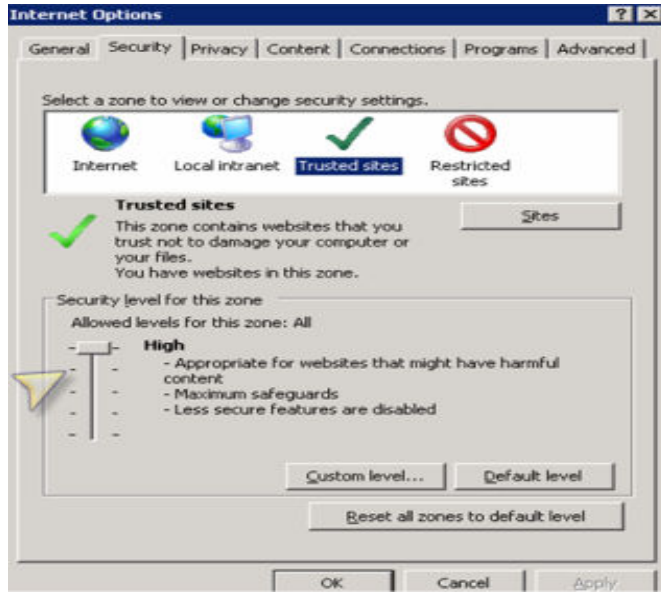


Figure 49: IE settings

- Additional settings for group policies that disable execution of scripts. Use the same functionality in Firefox, if a problem persists.