Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 7200 Series and 8000 Series

Release 5.1
NN47227-500
Issue 06.01
March 2016

© 2014-2016, Avaya, Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means a hosted service subscription that You acquire from either Avaya or an authorized Avaya 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 Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, 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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya 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 Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

Licence types

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

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage

Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya 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 Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. 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 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.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA 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 AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA 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.

Compliance with Laws

Customer acknowledges and agrees that it is responsible 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 Avaya 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.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

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 Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such

Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction 8
- Purpose 8
- Related resources 8
  - Subscribing to e-notifications 9
- Support 11
  - Searching a documentation collection 11

Chapter 2: New in this document 13
- Release 5.1 13

Chapter 3: VLAN fundamentals 14
- Port-based VLANs 14
- Private VLANs 15
- Policy-based VLANs 17
- SPBM B-VLAN 18
- VLAN tagging and port types 19
- VLAN router interfaces 21
- IP routing and VLANs 21
- VLAN implementation 22
- VLAN configuration rules 22
- VLAN feature support 23
- Network Load Balancing 23
  - Supported NLB topologies 24
- VLAN loop prevention 27
- IGMP Layer 2 Querier 28
- Switched UNI Layer 3 29

Chapter 4: VLAN configuration using ACLI 30
- Creating a VLAN 30
- Creating a private VLAN 32
- Performing a general VLAN action 35
- Configuring static MAC addresses for a VLAN 36
- Configuring the forwarding database timeout globally 37
- Adding or removing ports in a VLAN 38
- Configuring NLB support 39
- Configuring a tagged port to discard untagged frames 40
- Configuring SLPP 41
- Configuring SLPP packet-rx on a port 43
- Configuring SLPP packet-tx on a VLAN 45
- Viewing SLPP information 46
- Viewing SLPP information for a port 47
- Viewing VLAN information 48

Viewing private VLAN information... 49
Viewing brouter port information... 50
Viewing VLAN port member status... 51
Viewing VLAN forwarding database information... 52
Viewing NLB-mode information... 54
Displaying C-VLAN and Switched UNI I-SID information... 54
Variable definitions... 56
Job aid... 56
Chapter 5: VLAN configuration using EDM... 59
Configuring the VLAN feature on a port... 59
Viewing existing VLANs... 60
Creating a port-based VLAN... 61
Creating a private VLAN... 63
Configuring an IP address for a VLAN... 65
Changing VLAN port membership... 66
Creating a protocol-based VLAN... 67
Creating a SPBM B-VLAN... 68
Configuring advanced VLAN features... 68
Configuring NLB support using EDM... 70
Configuring a port to accept tagged or untagged frames... 71
Configuring untagging default VLAN on a tagged port... 72
Configuring SLPP globally... 72
Configuring the SLPP by VLAN... 73
Configuring the SLPP by port... 74
Configuring directed broadcast on a VLAN... 76
Configuring the forwarding database timeout globally... 77
Viewing VLAN forwarding database information... 77
Viewing the forwarding database for a specific VLAN... 78
Clearing learned MAC addresses by VLAN... 79
Clearing learned MAC addresses for all VLANs by port... 80
Configuring static forwarding... 80
Chapter 6: Spanning tree fundamentals... 82
Rapid Spanning Tree Protocol and Multiple Spanning Tree Protocol... 84
Chapter 7: Spanning Tree configuration using ACLI... 88
Configuring Spanning Tree... 88
Configuring Rapid Spanning Tree Protocol... 89
Configuring Rapid Spanning Tree Protocol for a port... 90
Configuring the Rapid Spanning Tree Protocol version... 91
Viewing the global RSTP configuration information... 92
Viewing RSTP statistics... 93
Viewing the RSTP status... 93
Viewing the RSTP configuration information... 94
Viewing the RSTP status for a port... 95

Viewing RSTP information for a selected port.... 95
Viewing the RSTP role.... 96
Viewing spanning tree configuration.... 97
Configuring Multiple Spanning Tree Protocol.... 98
Configuring MSTP MSTI options.... 100
Configuring Ethernet MSTP.... 101
Configuring Ethernet MSTP MSTI.... 102
Viewing MSTP configurations.... 104
Viewing MSTP status.... 104
Viewing MSTP port information.... 105
Viewing MSTP MSTI information.... 105
Viewing MSTP statistics.... 107
Chapter 8: Spanning Tree configuration using EDM.... 108
Configuring the Spanning Tree mode.... 108
Restarting the switch.... 109
Configuring RSTP global parameters.... 109
Configuring RSTP ports.... 111
Viewing RSTP port status.... 113
Configuring MSTP global parameters.... 113
Configuring CIST ports for MSTP.... 117
Configuring MSTI bridges for MSTP.... 120
Configuring MSTI ports for MSTP.... 121
Glossary.... 123

Chapter 1: Introduction

Purpose

This document provides information on features in VSP Operating System Software (VOSS). VOSS runs on the following product families:

- Avaya Virtual Services Platform 4000 Series
- Avaya Virtual Services Platform 7200 Series
- Avaya Virtual Services Platform 8000 Series

This document contains procedural and conceptual information to help you configure and manage Virtual Local Area Networks (VLAN), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP) on Avaya Virtual Services Platform 7200 Series and 8000 Series switches. This document also provides instructions to use Avaya Command Line Interface (ACLI) and Enterprise Device Manager (EDM).

For information on configuring VLAN and Spanning Tree on Avaya Virtual Services Platform 4000 Series, see *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 4000 Series*, NN46251-500.

Examples and network illustrations in this document may illustrate only one of the supported platforms. Unless otherwise noted, the concept illustrated applies to all supported platforms.

Related resources

Documentation

For installation and initial setup information of the Open Networking Adapter (ONA), refer to the Quick Install Guide that came with your ONA.

Note:

The ONA works only with the Avaya Virtual Services Platform 4000 Series. For more information about configuring features, refer to the VOSS documentation. See *Documentation Reference for VSP Operating System Software*, NN47227-100 for a list of all the VSP 4000 documents.

Training

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

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
    - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
    - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
    - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
    - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Subscribing to e-notifications

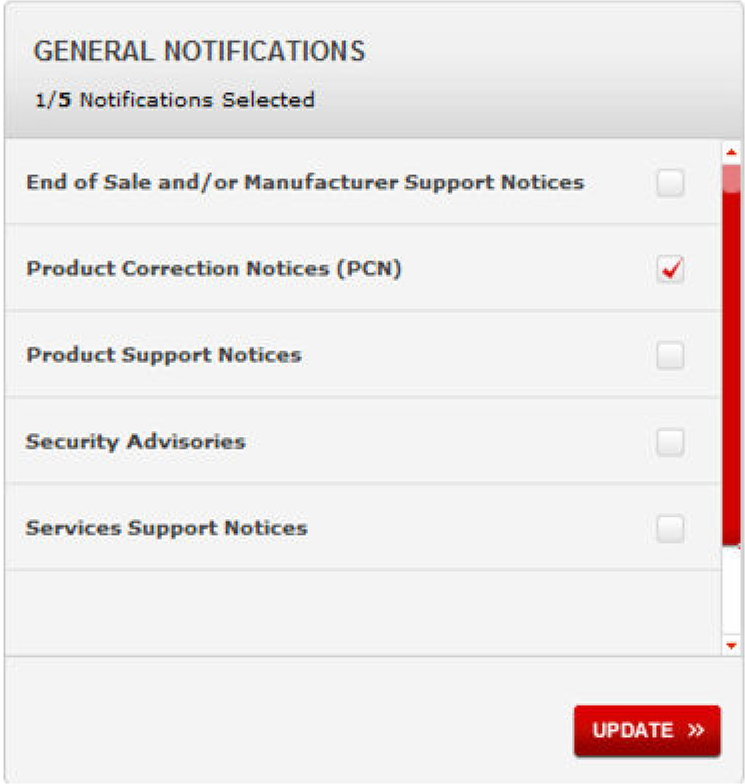
Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

Procedure

1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.

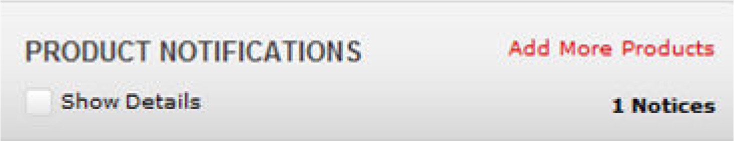


GENERAL NOTIFICATIONS

1/5 Notifications Selected

- End of Sale and/or Manufacturer Support Notices ☐
- Product Correction Notices (PCN) ☑
- Product Support Notices ☐
- Security Advisories ☐
- Services Support Notices ☐

6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.

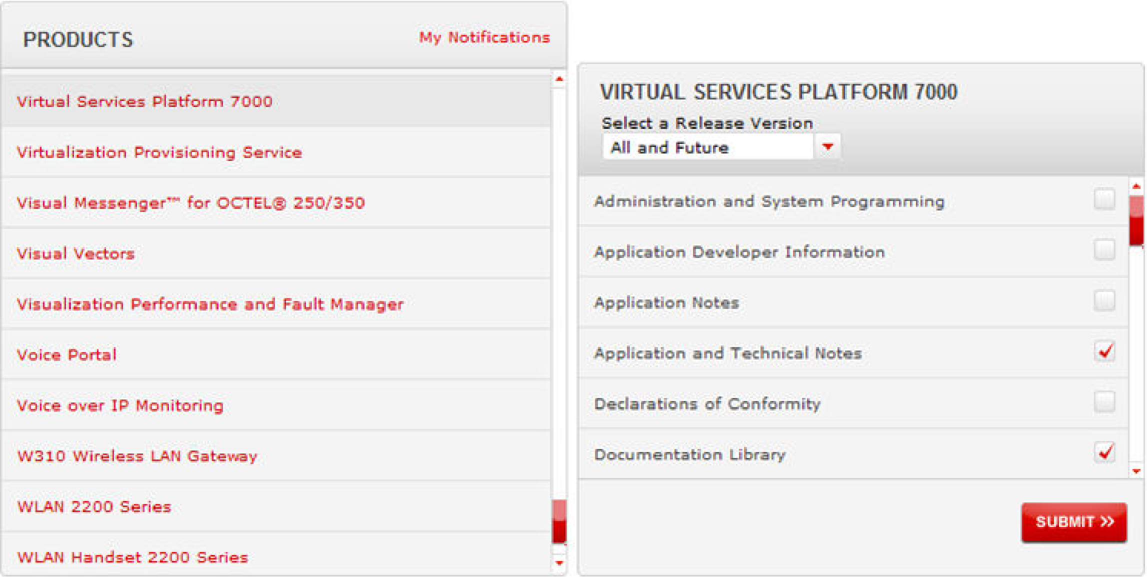


PRODUCT NOTIFICATIONS

☐ Show Details

1 Notices

8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.


PRODUCTS
My Notifications
Virtual Services Platform 7000
Virtualization Provisioning Service
Visual Messenger™ for OCTEL® 250/350
Visual Vectors
Visualization Performance and Fault Manager
Voice Portal
Voice over IP Monitoring
W310 Wireless LAN Gateway
WLAN 2200 Series
WLAN Handset 2200 Series
VIRTUAL SERVICES PLATFORM 7000
SUBMIT »

Select a Release Version: All and Future

☐ Administration and System Programming
☐ Application Developer Information
☐ Application Notes
☑ Application and Technical Notes
☐ Declarations of Conformity
☑ Documentation Library

11. Click **Submit**.

Support

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

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.

3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
    - Whole Words Only
    - Case-Sensitive
    - Include Bookmarks
    - Include Comments
6. Click **Search**.

    The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Chapter 2: New in this document

The following sections details what is new in *Configuring VLANs, Spanning Tree, and NLB on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-500.

Release 5.1

Supported NLB topology

This release supports a topology where the NLB Server and the NLB Client workstations connect to the same aggregation switch and then connect to the VOSS device using the same port.

Important:

The L3 routing between an NLB-enabled VLAN and another VLAN on the same port is supported on the VSP 7200, VSP 8200, and VSP 8400 platforms. It is not supported on VSP 4000 platform.

For more information, see Supported NLB topologies on page 24.

Chapter 3: VLAN fundamentals

This section describes the virtual local area network (VLAN) features supported on the switch.

For more information about the user interface, see *Using ACLI and EDM on VSP Operating System Software*, NN47227-103.

A VLAN is a switched network that is logically segmented by functions, project teams, or applications without regard to the physical location of users. By using a VLAN, you can divide the Local Area Network into smaller groups without interfering with the physical network.

The practical applications of VLAN include the following:

- You can create VLANs, or workgroups, for common interest groups.
- You can create VLANs, or workgroups, for specific types of network traffic.
- You can add, move, or delete members from these workgroups without making physical changes to the network.

By dividing the network into separate VLANs, you can create separate broadcast domains. This arrangement conserves bandwidth, especially in networks supporting broadcast and multicast applications that flood the network with traffic. A VLAN workgroup can include members from a number of dispersed physical segments on the network, improving traffic flow between them.

The switch performs the Layer 2 switching functions necessary to transmit information within VLANs, as well as the Layer 3 routing functions necessary for VLANs to communicate with one another. You can define a VLAN for a single switch or spanning multiple switches. A port can be a member of multiple VLANs. A VLAN is associated with a spanning tree group.

A VLAN packet is classified before it is forwarded. If the packet matches a classification rule, the port membership is checked. If the port is not an allowed member (potential, static, or active), the system drops the packet.

Port-based VLANs

A port-based VLAN is a VLAN in which you explicitly configure the ports to be in the VLAN. When you create a port-based VLAN on a device, you assign a VLAN identification number (VLAN ID) and specify the ports that belong to the VLAN. These port members are always active port members. The VLAN ID is used to coordinate VLANs across multiple switches. Any type of frame can be classified to a port-based VLAN.

The example in the following figure shows two port-based VLANs: one for the marketing department, and one for the sales department. Ports are assigned to each port-based VLAN. A change in the sales area can move the sales representative at port 1/1 to the marketing department without moving cables. With a port-based VLAN, you only need to indicate in the Avaya Command Line Interface (ACLI) that port 1/1 in the sales VLAN now is a member of the marketing VLAN.

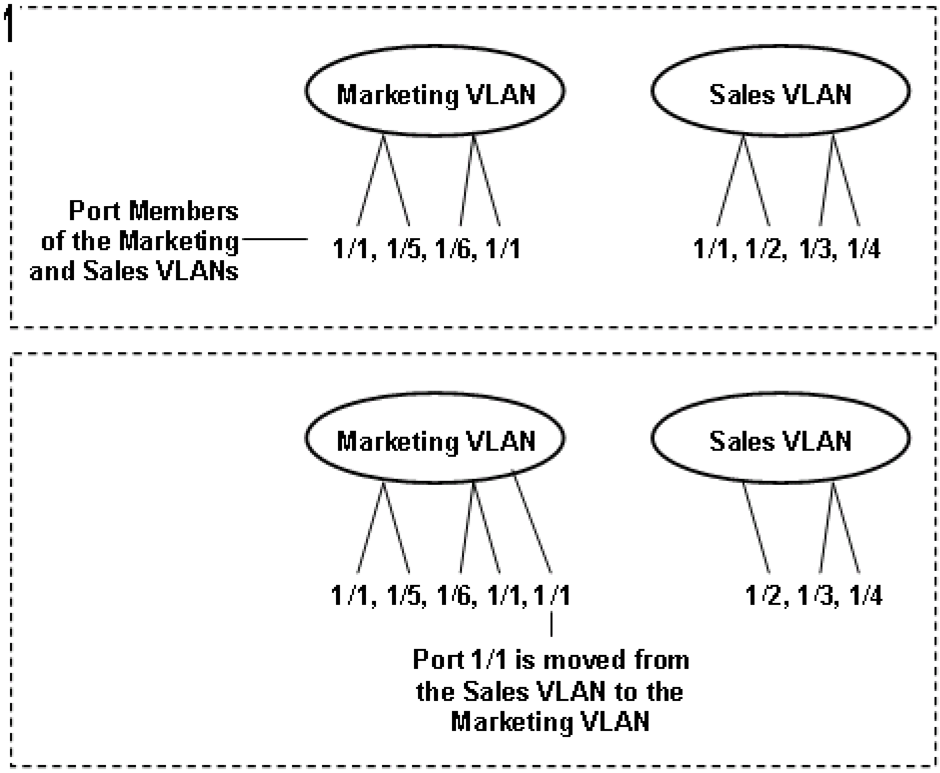

Marketing VLAN
Sales VLAN
Port Members of the Marketing and Sales VLANs
1/1, 1/5, 1/6, 1/1
1/1, 1/2, 1/3, 1/4
Marketing VLAN
Sales VLAN
1/1, 1/5, 1/6, 1/1, 1/1
1/2, 1/3, 1/4
Port 1/1 is moved from the Sales VLAN to the Marketing VLAN

Figure 1: Port-based VLAN

Private VLANs

Private VLANs provide isolation between ports within a Layer-2 service.

The primary and secondary VLAN make the private VLAN. Standard VLAN configuration takes place on the primary VLAN. The secondary VLAN is virtual and inherits configuration from the primary VLAN.

Ports in the private VLAN are configured as isolated, promiscuous, or trunk. The default value is None.

Port types

Table 1: Port types for private VLANs

Port type	Description
Promiscuous	Promiscuous ports communicate with all other ports within the private VLAN. Uses the primary VLAN.

Table continues…

Port type	Description
(tagged or untagged ports)	
Isolated (tagged or untagged ports)	Isolated ports communicate with the promiscuous ports, but not with any other isolated port. Uses the secondary VLAN.
Trunk (tagged ports)	Trunk ports carry traffic between other port members within the private VLANs. Accepts either primary or secondary VLAN.

Trunk ports must have VLAN encapsulation enabled. A port may be a single port or may belong to an MLT.

The following figure shows a basic private VLAN topology with private VLAN configured on five switches. All ports connecting to other switches are trunk type ports and all other ports are either promiscuous or isolated ports. On the secondary VLAN, spokes can communicate with hubs, hubs can communicate with all spokes in the same private VLAN using the primary VLAN, but spokes cannot communicate with other spokes.

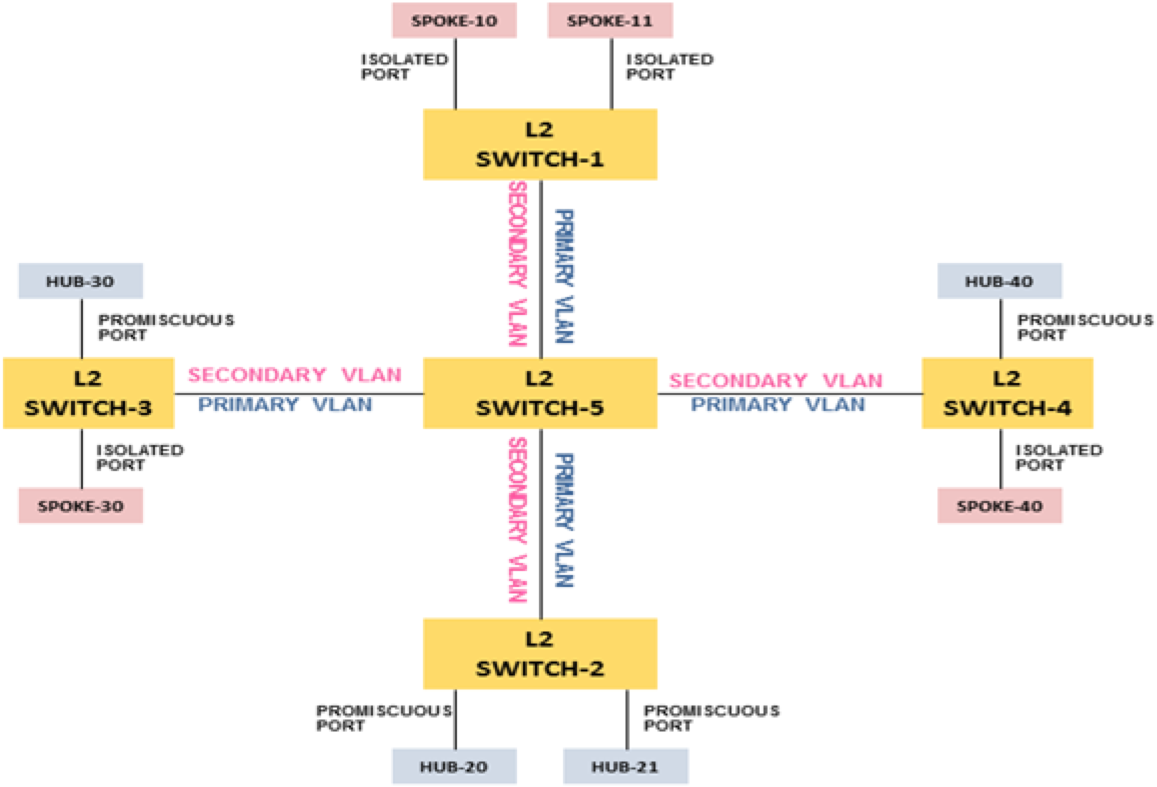

SPOKE-10
SPOKE-11
ISOLATED PORT
ISOLATED PORT
L2 SWITCH-1
SECONDARY VLAN
PRIMARY VLAN
HUB-30
PROMISCUOUS PORT
HUB-40
PROMISCUOUS PORT
L2 SWITCH-3
SECONDARY VLAN
PRIMARY VLAN
L2 SWITCH-5
SECONDARY VLAN
PRIMARY VLAN
L2 SWITCH-4
ISOLATED PORT
SPOKE-30
ISOLATED PORT
SPOKE-40
SECONDARY VLAN
PRIMARY VLAN
L2 SWITCH-2
PROMISCUOUS PORT
PROMISCUOUS PORT
HUB-20
HUB-21

Figure 2: Private VLAN topology

E-Tree

The E-Tree allows private VLANs to traverse the Shortest Path Bridging MAC (SPBM) network.

For more information about E-Tree and SPBM configuration, see

Configuring Avaya Fabric Connect on VSP Operating System Software, NN47227-510.

Private VLAN configuration rules

The following are private VLAN rules for the Switch:

- Use private VLANs for Layer 2 services only
- Forwarding is based on MAC address based lookups
- IP routing and creation of IP interfaces are not supported on private VLANs
- Do not use the untag-port default vlan parameter on private VLAN interfaces that are operating as trunk ports, because it impacts the private VLAN functionality.

Policy-based VLANs

Received frames are classified into a policy-based VLAN based on certain fields of the frame that matches the associated VLAN policy.

Port membership types

In a policy-based VLAN, a port can be designated as a potential member, a static member, or one not allowed to be a member of the VLAN.

If a port is designated as a potential member of the VLAN, and the incoming traffic matches the policy, the system dynamically adds the port to the active port list of the VLAN, making the port an active member of the VLAN. After the system adds a port to the active list, it can remove the port from the active list due to time-out. Potential member ports that join the VLAN are removed (timed out) from the active port list of the VLAN after the timeout (aging time) period expires.

All members of the Spanning Tree Group associated with a protocol-based VLAN are automatically considered potential members of the VLAN. In addition, all tagged ports (trunk ports) become static ports. If you do not want all the tagged ports to be static members of a protocol-based VLAN, put the port in the disallowed list.

Static port members are always members of the VLAN. Static port members are not aged out due to inactivity and they are not removed from the active list. If a server or router connects to a port, designate that port as a static member of a VLAN. If a server connects to a port that is only a potential member and the server sends very little traffic, a client fails to reach the server if the server port is timed out of the VLAN. Avaya recommends that you make these ports static members of the VLAN.

A disallowed port can never become a member of the VLAN until you add it as a port-member. After you remove a port from the VLAN, the system adds the port to the disallowed list.

On any single spanning-tree instance, an access (untagged) port can belong to one port-based VLAN and many policy-based VLANs. A trunk (tagged) port can belong to many port-based and policy-based VLANs.

The following table describes port membership types for policy-based VLANs.

Table 2: Port membership types for policy-based VLANs

Membership type	Description
Potential	Potential members of a VLAN become active members upon receiving data matching the policy defined for the VLAN (a packet tagged with that VLAN, or an untagged packet matching the policy).
Static (always a member)	Static members are always active members of the VLAN after you configure them as belonging to that VLAN.
Not allowed to join (never a member)	Ports of this type cannot join the VLAN.

The following table lists supported policy-based VLANs.

Table 3: Supported policy-based VLAN types

VLAN type	Support
Protocol-based	supported

Protocol-based VLANs

Protocol-based VLANs are an effective way to segment your network into broadcast domains according to the network protocols in use.

A port member of a port-based VLAN can belong to multiple protocol-based VLANs. Port tagging is not required for a port to be a member of multiple protocol-based VLANs.

The switch supports IPv6 protocol-based VLAN only.

SPBM B-VLAN

Each SPBM network instance is associated with at least one backbone VLAN (B-VLAN) in the core SPBM network.

This VLAN is used for both control plane traffic and dataplane traffic.

Note:

Avaya recommends to always configure two B-VLANs in the core to allow load distribution over both B-VLANs.

SPBM alters the behavior of the VLAN. When a B-VLAN is associated with an SPBM network the following VLAN attributes and behaviors are modified for the B-VLAN:

- Flooding is disabled
- Broadcasting is disabled
- Source address learning is disabled
- Unknown MAC discard is enabled

Ports cannot be added to a B-VLAN manually, IS-IS takes care of adding ports to the B-VLAN.

Essentially the B-MAC addresses are programmed into the B-VLAN Forwarding Information Bases (FIBs) by IS-IS instead of the traditional VLANs flooding and learning approach.

Modification of the VLAN behavior is necessary to ensure proper control over the SPBM traffic.

VLAN tagging and port types

The switch supports the IEEE 802.1Q specification for tagging frames and coordinating VLANs across multiple switches.

Figure 3: VLAN tag insertion on page 19 shows how an additional four octet (tag) header is inserted in a frame after the source address and before the frame type. The tag contains the VLAN ID associated with the frame.

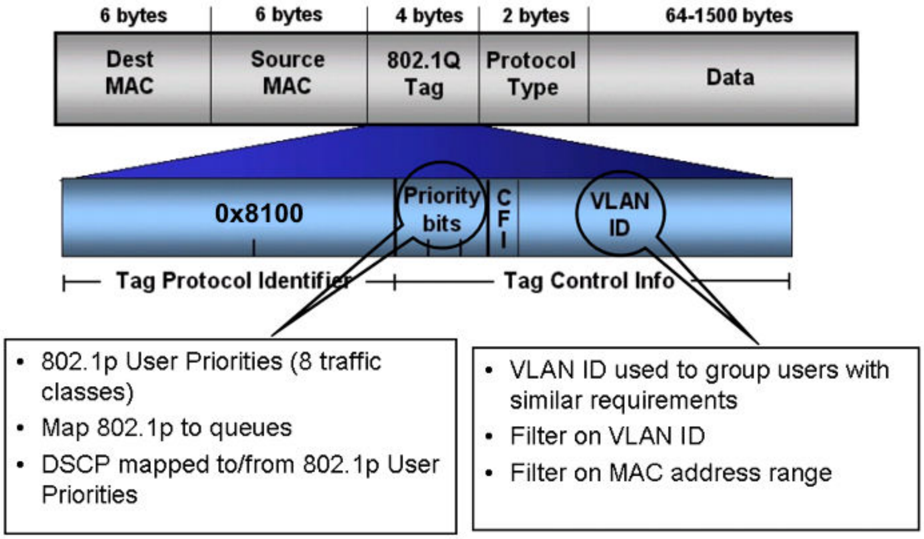

6 bytes
6 bytes
4 bytes
2 bytes
64-1500 bytes
Dest MAC
Source MAC
802.1Q Tag
Protocol Type
Data
0x8100
Priority bits
C F I
VLAN ID
Tag Protocol Identifier
Tag Control Info
802.1p User Priorities (8 traffic classes)
Map 802.1p to queues
DSCP mapped to/from 802.1p User Priorities
VLAN ID used to group users with similar requirements
Filter on VLAN ID
Filter on MAC address range

Figure 3: VLAN tag insertion

802.1Q tagged ports

Tagging a frame adds four octets to a frame, possibly making it bigger than the traditional maximum frame size. If a device does not support IEEE 802.1Q tagging, it can have problems interpreting tagged frames that it receives.

Whether or not tagged frames are sent depends on what you configure at the port level. Tagging is configured as true or false for the port and is applied to all VLANs on that port.

A port with tagging enabled applies the VLAN ID tag to all packets sent on the port. Tagged ports are typically used to multiplex traffic belonging to multiple VLANs to other IEEE 802.1Q-compliant devices.

If you disable tagging on a port, it does not send tagged frames. A nontagged port connects a switch to devices that do not support IEEE 802.1Q tagging. If a tagged frame is forwarded to a port with tagging configured to false, the switch removes the tag from the frame before sending it to the port.

Treatment of tagged and untagged frames

The switch associates a frame with a VLAN based on the data content of the frame and the configuration of the receiving port. The treatment of the frame depends on whether the frame is tagged or untagged.

If a tagged frame is received on a port, if the port is a static or potential member of the VLAN ID specified in the tag, the switch directs it to that VLAN. If the port is not a member of the VLAN that is identified by the tag in the packet, the Virtual Services Platform discards the packet. If a port is untagged, you can configure it to discard tagged frames received on the port. In this case the tagged frame is discarded.

For untagged frames, VLAN membership is implied from the content of the frame itself. You can configure a tagged port to accept or discard untagged frames received on the port.

The default VLAN of a port is the VLAN to which untagged frames are classified if they do not match the criteria of any policy-based VLAN of which the port is a member. The default VLAN of the port can be any port-based VLAN a port belongs to, or the unassigned VLAN (1). Frames classified to the unassigned VLAN are discarded.

The frame is forwarded based on the VLAN on which the frame is received, and on the forwarding options available for that VLAN. The switch tries to associate untagged frames with a VLAN in the following order:

- Does the frame belong to a protocol-based VLAN?
- What is the default VLAN for the receiving port?
- Is the default VLAN for the port not the unassigned VLAN?

If the frame meets none of these criteria, it is discarded.

Untagging default VLAN on a tagged port feature

This feature provides the ability to connect two devices such as an IP phone and a PC to a single port of the switch. Most IP phones ship with an embedded three port switch, and traffic coming from the phone is generally tagged (VLAN ID configured statically or remotely). However, the traffic originating from a PC is usually untagged traffic and must be separated from the IP phone traffic. This separation ensures that broadcast traffic from the PC does not impact voice quality.

After an IP phone is attached to an untagged port, it can fail to register with a remote Internet Telephony Gateway (or equivalent device) dependent on the netmask of the destination IP address (Call Server subnet).

For more information about the Network with IP phone and PC, see the following figure.

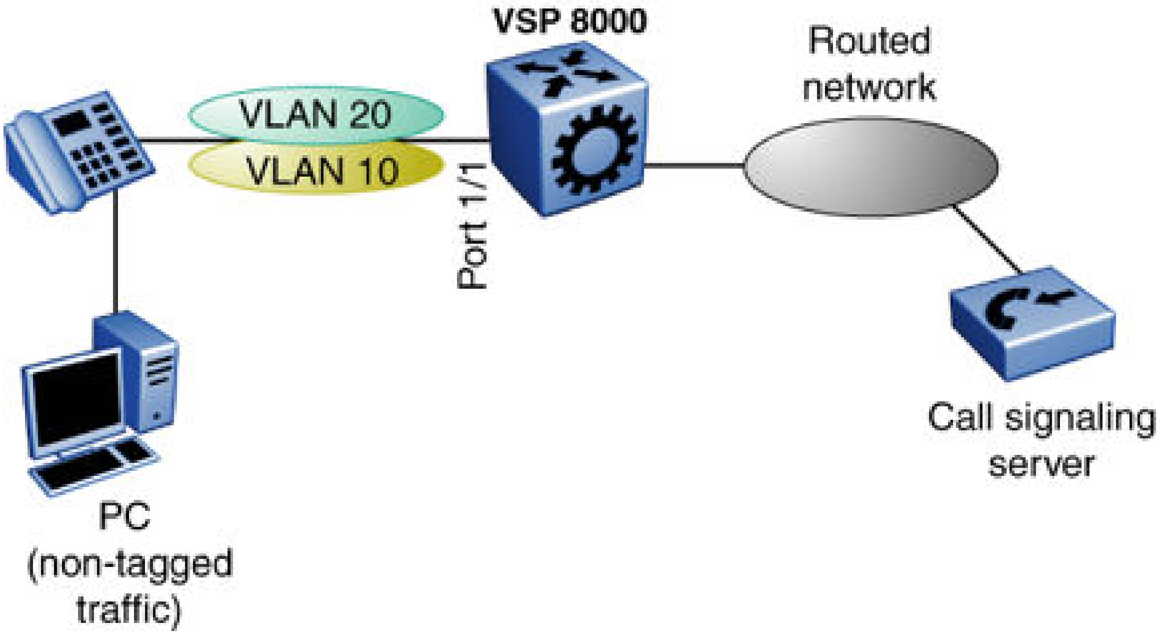


Figure 4: Network with IP phone and PC

IP phones and PCs coexist on the same port due to the use of an embedded IP Phone Layer 2 switch. In this scenario if you configure the port as untagged, the egress traffic on this port is untagged and no separation exists between the traffic to the IP phone and the PC. To avoid this condition, the port that connects to the IP phone must be tagged. If the port is tagged, the traffic for the PC is tagged with the default VLAN ID for the port. This configuration creates a problem because the PC does not expect tagged packets. Untag the default VLAN on a tagged port (in this example, port 1/1 that connects to the IP phone) to ensure that the traffic to the PC is sent untagged.

VLAN router interfaces

When you configure routing on a VLAN, you assign an IP address to the VLAN, which acts as a virtual router interface address for the VLAN. This IP address is not associated with a physical port. You can reach the VLAN IP address through any of the VLAN port members. Frames are routed to another VLAN IP address within the device. A port can belong to multiple VLANs; some, all, or none can perform routing.

IP routing and VLANs

The switch supports IP routing on the following types of VLANs:

- Port-based VLANs
- IP protocol-based VLANs

VLAN implementation

This section describes how to implement VLANs and describes default VLANs, the unassigned (NULL) VLAN, and brouter ports. This section also summarizes the defaults and rules regarding VLAN creation on the switch.

- Default VLAN on page 22
- NULL VLAN on page 22
- Brouter ports on page 22

Default VLAN

Devices are factory-configured so that all ports are in a port-based VLAN called the default VLAN. Because all ports are in the default VLAN, the device behaves like a Layer 2 device. The VLAN ID of this default VLAN is always 1, and it is always a port-based VLAN. You cannot delete the default VLAN.

NULL VLAN

Internally, the switch creates a special port-based VLAN called NULL VLAN or unassigned VLAN. This is a place holder VLAN for ports that are not members of any port-based VLAN. When a port is removed from all port-based VLANs, it is added to the NULL VLAN as a port member. Ports can belong to policy-based VLANs as well as to the NULL VLAN. If a frame does not meet the policy criteria and no underlying port-based VLAN exists, the port belongs to the NULL VLAN and the frame is dropped.

Because it is an internal construct, the NULL VLAN cannot be deleted.

Brouter ports

A brouter port is actually a one-port VLAN with an IP interface. The difference between a brouter port and a standard IP protocol-based VLAN configured to perform routing is that the routing interface of the brouter port is not subject to the spanning tree state of the port. A brouter port can be in the blocking state for nonroutable traffic and still route IP traffic. Because a brouter port is a single-port VLAN, it uses one VLAN ID. Each brouter port decreases the number of available VLANs by one.

VLAN configuration rules

The following are VLAN rules for the switch:

- The switch supports configurable VLANs from 1 to 4059. VLAN ID 0 is invalid and VLAN 1 is automatically created. VLAN IDs on the switch range from 2 to 4084, but VLAN IDs 4060 to 4094 are reserved for system internal use.
- A tagged port can belong to multiple VLANs in multiple Spanning Tree Groups.
- Under the default configuration, the default Spanning Tree Group is number 1 if the chassis configuration permits multiple STGs.
- An untagged port can belong to only one port-based VLAN.
- You can configure only one protocol-based VLAN for a given protocol.

- The VLAN membership of a frame is determined by the following order of precedence, if applicable:
    1. IEEE 802.1Q tagged VLAN ID
    2. protocol-based VLAN
    3. port-based VLAN default VLAN of the receiving port

VLAN feature support

The following table summarizes supported features.

For the latest scalability information, see *Release Notes for VSP Operating System Software*, NN47227-401.

Table 4: VLAN support

Feature	Description
Number of VLANs	4059
Port-based VLANs	Supported
Policy-based VLANs • Protocol-based • SPBM-based	Supported
IEEE 802.1Q tagging	Supported
IP routing and VLANs	Supported
Special VLANs • Default VLAN • Null VLAN • Brouter ports	Supported

Network Load Balancing

Microsoft Network Load Balancing (NLB) is a clustering technology available with the Microsoft Windows 2000, Microsoft Windows 2003, Microsoft Windows 2008, and Microsoft Windows 2012 Server family of operating systems. You can use NLB to share the workload among multiple clustering servers. NLB uses a distributed algorithm to load balance TCP/IP network traffic across a number of hosts, enhancing the scalability and availability of mission critical, IP based services, such as Web, VPN, streaming media, and firewalls. Network Load Balancing also provides high availability by detecting host failures and automatically redistributing traffic to remaining operational hosts.

The switch interoperates with NLB clusters operating in Unicast mode.

You must configure NLB to use the same mode as the switch.

For interoperability with NLB, the switch provides configuration options at VLAN level.

NLB clustering in unicast mode

When the cluster is running in NLB unicast mode, all servers in the cluster share a common virtual MAC address, which is 02-bf-x-x-x-x (where x-x-x-x is the cluster IP address). All traffic destined to this MAC address is sent to all the servers in the cluster. The virtual MAC address is specified in the Sender MAC Address field of the Address Resolution Protocol (ARP) reply from the cluster to the switch. ARP responses from the switch are sent to the virtual MAC address (rather than to the hardware MAC address).

You can configure the switch for NLB unicast mode support. After you enable the NLB unicast option, the switch floods traffic destined to the cluster IP address to all ports on the VLAN. Unicast mode supports connectivity to a secondary virtual IP address. For information about software scaling capabilities in unicast mode, see *Release Notes for VSP Operating System Software*, NN47227-401.

Supported NLB topologies

The switch supports Network Load Balancing (NLB) in the following topologies.

Supported NLB topology–example 1

The switch supports NLB when the NLB Cluster connections use a different physical port on the switch than the NLB clients.

The following figure illustrates this configuration where the NLB Server and the NLB Client workstations connect to different aggregation switches, which connect to the switch using different VLANs and different ports.

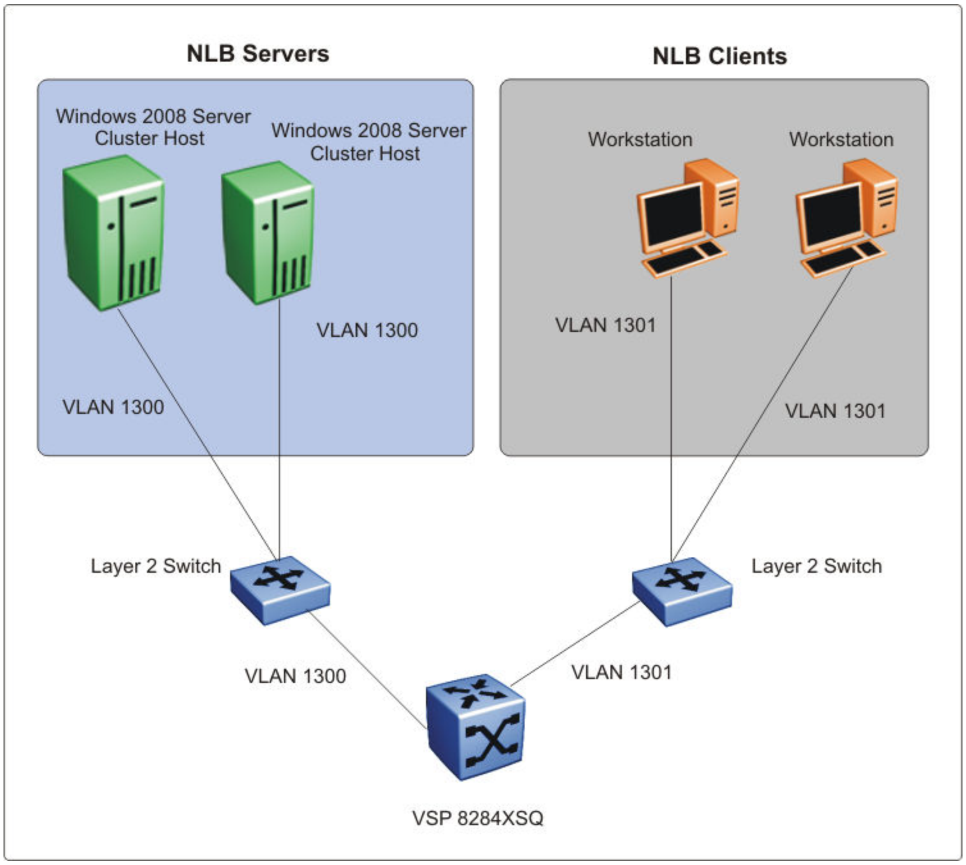

NLB Servers
NLB Clients
Windows 2008 Server Cluster Host
Windows 2008 Server Cluster Host
Workstation
Workstation
VLAN 1300
VLAN 1300
VLAN 1301
VLAN 1301
Layer 2 Switch
Layer 2 Switch
VLAN 1300
VLAN 1301
VSP 8284XSQ

Figure 5: Supported NLB topology–example 1

Supported NLB topology–example 2

The switch also supports the following topology where the NLB Server and the NLB Client workstations connect to the same aggregation switch and then connect to the switch using the same port.

Important:

The switch supports L3 routing between an NLB-enabled VLAN and another VLAN on the same port.

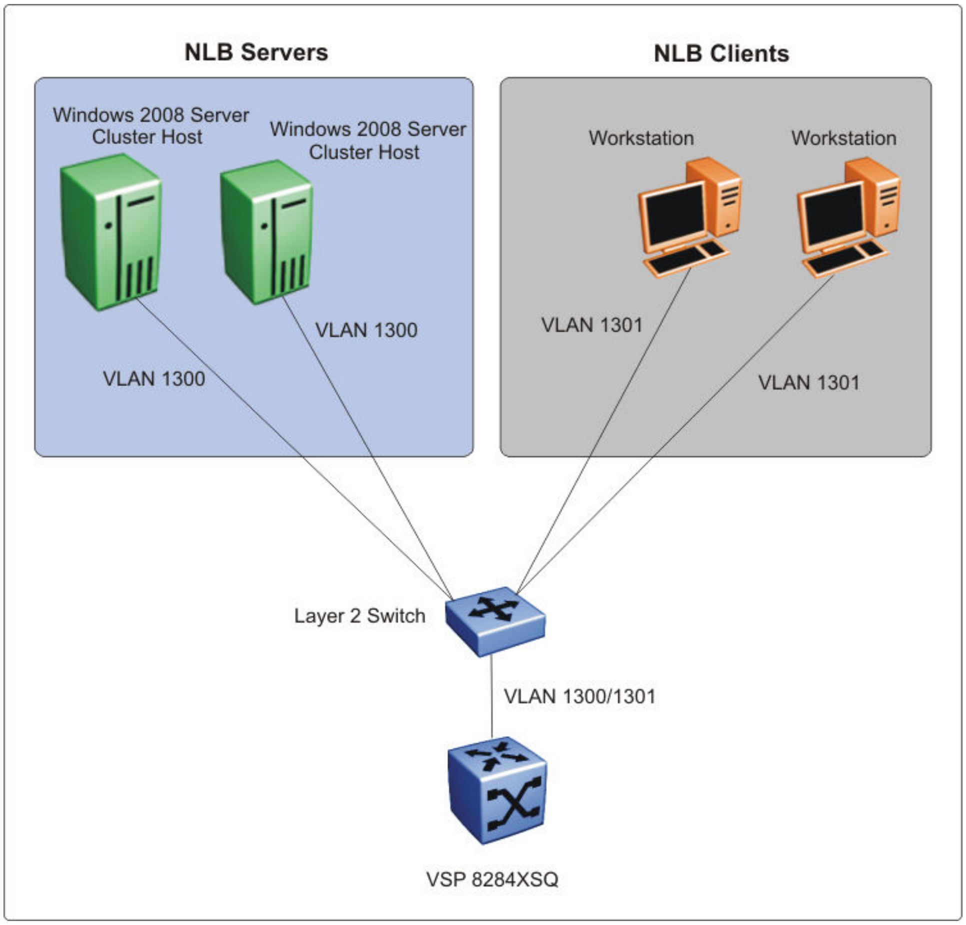

NLB Servers
NLB Clients
Windows 2008 Server Cluster Host
Windows 2008 Server Cluster Host
Workstation
Workstation
VLAN 1300
VLAN 1300
VLAN 1301
VLAN 1301
Layer 2 Switch
VLAN 1300/1301
VSP 8284XSQ

Figure 6: Supported NLB topology–example 2

Other supported NLB topologies

The switch supports NLB in the following other topologies:

- NLB cluster hosts and clients are connected to Layer 2 Ethernet switches that are SMLT connected to the SMLT cluster.
- NLB cluster hosts are directly connected and distributed between the switches and the clients are connected to Layer 2 Ethernet switch that is SMLT connected to the SMLT cluster.
- NLB cluster hosts and clients are directly connected and distributed between the switches in the SMLT cluster.
- NLB cluster hosts and clients are connected to Layer 2 Ethernet switches that are SMLT connected to the SMLT cluster core.

Note:

For more information on the above topologies, see *Technical Configuration Guide for Microsoft Network Load Balancing*, NN48500-593.

VLAN loop prevention

Loop prevention

Under certain conditions, such as incorrect configurations or cabling, loops can form. This is true mainly for layer 2 bridged domains, such as VLANs.

Simple Loop Prevention Protocol (SLPP) provides active protection against Layer 2 network loops on a per-VLAN basis. SLPP uses a lightweight hello packet mechanism to detect network loops. Sending hello packets on a per VLAN basis allows SLPP to detect VLAN based network loops for untagged as well as tagged IEEE 802.1Q VLAN link configurations. After SLPP detects a loop, the port is shutdown.

Note:

> If SLPP is used in a vIST environment, it must be enabled on both the vIST peers. Because, when an SLPP packet of a vIST peer is looped through UNI ports to the other device, that device will shut down its UNI port due to receiving SLPP packets from its peer. A device's own SLPP packets will go over a vIST connection but will not be forwarded by its vIST peer back onto its UNI ports.

Configure the SLPP functionality with the following criteria:

- SLPP TX Process – You decide on which VLANs a switch can send SLPP hello packets. The packets are then replicated out all ports which are members of the SLPP-enabled VLAN. Avaya recommends that you enable SLPP on all VLANs.
- SLPP RX Process – You decide on which ports the switch can act when receiving an SLPP packet that is sent by the same switch or by its SMLT peer. You must enable this process only on Access SMLT ports. You can enable this process only when the design permits on SMLT CORE ports in the case of a square/full mesh core design.
- SLPP Action – The action operationally disables the ports receiving the SLPP packet. You can also tune the network failure behavior. You can choose how many SLPP packets a port needs to receives before a switch takes an action. You need to stagger these values to avoid edge switch isolation – see the recommendations at the end of this section.

Loops can be introduced into the network in many ways. One way is through the loss of an MLT/link aggregation configuration caused by user error or malfunctioning equipment. This scenario does not always introduce a broadcast storm, but because all MAC addresses are learned through the looping ports, does significantly impact Layer 2 MAC learning. Spanning Tree cannot in all cases detect such a configuration issue, whereas SLPP reacts and disables the malfunctioning links and limits network impact to a minimum.

The desire is to prevent a loop from causing network problems, while also attempting not to isolate totally the edge where the loop was detected. Total edge closet isolation is the last resort to protect the rest of the network from the loop. With this in mind, some administrators adopt the concept of an SLPP primary switch and SLPP secondary switch. These are strictly design terms and are not configuration parameters. The Rx thresholds are staggered between the primary and secondary switch. Therefore, the primary switch disables an uplink immediately upon a loop occurring. If this resolves the loop issue, then the edge closet still has connectivity back through the SLPP secondary switch. If the loop is not resolved, then the SLPP secondary switch disables the uplink and isolates the closet to protect the rest of the network from the loop.

As the number of VLANs running SLPP scale off of a specific uplink port, the Rx-threshold value may need to be increased to prevent complete isolation of the offending edge. The primary goal of

SLPP is to protect the core at all costs. In certain loop conditions, what can occur is the secondary switch also detects the loop and SLPP Rx-threshold of the secondary switch is reached before the primary can stop the loop by taking its port down. Therefore, both switches eventually take their ports down and the edge is isolated. The larger the number of VLANs associated with the port, the more likely this can occur, especially for loop conditions that affect all VLANs.

You cannot configure the EtherType for SLPP. The switch uses an EtherType of 0x8102 .

IGMP Layer 2 Querier

In a Layer 2 multicast network, you can enable Layer 2 querier on one of the switches in the VLAN. IGMP Layer 2 querier provides the IGMP querier function so that the switch can provide the recurring queries that maintain IGMP groups when you do not use multicast routing for multicast traffic.

Overview

In a multicast network, if you only need to use Layer 2 switching for the multicast traffic, you do not need multicast routing. However, you must have an IGMP querier on the network for multicast traffic to flow from sources to receivers. A multicast router provides the IGMP querier function. You can also use the IGMP Layer 2 Querier feature to provide a querier on a Layer 2 network without a multicast router.

The Layer 2 querier function originates queries for multicast receivers, and processes the responses accordingly. On the connected Layer 2 VLANs, IGMP snoop continues to provide services as normal. IGMP snoop responds to queries and identifies receivers for the multicast traffic.

You must enable Layer 2 querier and configure an IP address for the querier before it can originate IGMP query messages. If a multicast router exists on the network, the switch automatically disables the Layer 2 querier.

In a Layer 2 multicast network, enable Layer 2 querier on only one of the switches in the VLAN. A Layer 2 multicast domain supports only one Layer 2 querier. No querier election exists.

IGMP Snooping

IGMP Snooping enables Layer 2 switches in the network to examine IGMP control protocol packets exchanged between downstream hosts and upstream routers.

When Layer 2 switches examine the IGMP control protocol packets, they:

- Generate the Layer 2 MAC forwarding tables used for further switching sessions
- Regulate the multicast traffic to prevent it from flooding the Layer 2 segment of the network

IGMP Layer 2 Querier and IGMP interaction

IGMP Layer 2 Querier uses IGMP to learn which groups have members on each of the attached physical networks, and it maintains a list of multicast group memberships for each attached network and a timer for each membership. In this case, multicast group memberships means the presence of at least one member of a multicast group on a given attached network, not a list of all of the members.

IGMP Layer 2 Querier can assume one of two roles for each of the attached networks:

- Querier
- Non-Querier

After you enable IGMP Layer 2 Querier, the system assumes it is a multicast router, so it sends the General Query, Group Specific/Group, and Source Specific Query when Leave/BLOCK messages are received. IGMP queries are required to maintain an IGMP group.

Note:

Group Specific When Leave does not apply to IGMPv1.

For more information about how to configure IGMP Layer 2 Querier, see

Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 7200 Series and 8000 Series, NN47227-504.

Switched UNI Layer 3

Platform VLAN is created using the command **`vlan create <vlan-id> type port-mstprsp <msti-instance>`**. Layer 3 services are enabled on the platform VLAN and is associated with the Switched UNI (S-UNI) Service Instance Identifier (I-SID). All S-UNI ports are added to the platform VLAN.

You must associate the S-UNI I-SID to the platform VLAN. Once the platform VLAN is associated with the I-SID, it becomes a CVLAN.

MAC and ARP learning is done on the platform VLAN.

Note:

You cannot add S-UNI ports or MLT to the S-UNI platform VLANs directly. The ports should be added to the I-SID and the I-SID has to be assigned to the platform VLAN.

Note:

Only port based VLAN can be associated with S-UNI I-SID.

Chapter 4: VLAN configuration using ACLI

This chapter describes how to configure and manage a virtual local area network (VLAN) by using Avaya Command Line Interface (ACLI).

Configure and manage a VLAN to create VLANs, including private VLANs, add or remove ports in the VLAN, configure priority, change a VLAN name, or perform other operations.

Creating a VLAN

Create a VLAN using ACLI by port, protocol, or SPBM. Optionally, you can choose to assign the VLAN a name and color.

Assign an IP address to the VLAN. You can also assign a MAC-offset value that allows you to manually change the default MAC address.

About this task

Create a VLAN and assign an IP address in ACLI.

If you configure the SLA Mon™agent address under an IP interface or VLAN, you must remove the SLA Mon address before you can remove the IP address or VLAN.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create a VLAN using ACLI:

   ```
   vlan create <2-4059>
   ```

3. Specify a name for the VLAN:

   ```
   vlan create <2-4059> name WORD<0-64>
   ```

4. Create a VLAN by port:

   ```
   vlan create <2-4059> type port-mstprstp <0-63>
   ```

5. Associate CVLAN I-SID to the platform VLAN.

   ```
   vlan i-sid <1-4059> <1-16777215>
   ```

6. Create a VLAN using a user-defined protocol and specify the frame encapsulation header type:

   ```
   vlan create <2-4059> type protocol-mstprstp <0-63> ipv6
   ```

7. Assign a color to the VLAN:

   ```
   vlan create <2-4059> type port-mstprstp <0-63> [color <0-32>]
   ```

8. Log on to the VLAN Interface Configuration mode for the VLAN ID in ACLI:

   ```
   interface VLAN <1-4059>
   ```

9. Assign an IP address to a VLAN:

   ```
   ip address <A.B.C.D/X>|<A.B.C.D> <A.B.C.D>
   ```

10. Specify the MAC-offset value:

    ```
    ip address <A.B.C.D/X>|<A.B.C.D> <A.B.C.D> [<0-511>]
    ```

Example

```
Switch:1> enable
Switch:1# configure terminal
Switch:1(config)# vlan create 2 type port-mstprstp 6 color 4
Switch:1(config)#vlan i-sid 2 100
Switch:1(config)# interface vlan 2
Switch:1(config-if)# ip address 46.140.54.40/24
```

Variable Definitions

Use the data in the following table to use the `vlan create` command.

Variable	Value
<2-4059>	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. The system reserves VLAN IDs 4060 to 4094 for internal use.
name *WORD<0-64>*	Specifies the VLAN name. The name attribute is optional.
type port-mstprstp *<0-63> [color <0-32>]*	Creates a VLAN by port: • *<0-63>* is the STP instance ID from 0 to 63. • *color <0-32>* is the color of the VLAN in the range of 0 to 32.

Table continues…

Variable	Value
	Note: MSTI instance 62 is reserved for SPBM if SPBM is enabled on the switch.
type pvlan-mstprstp *<0-63> [color <0-32>]*	Creates a private VLAN by port: • *<0-63>* is the STP instance ID from 0 to 63. • *color <0-32>* is the color of the VLAN in the range of 0 to 32.
type protocol-mstprstp *<0–63>* ipv6	Creates a VLAN by protocol: • *<0–63>* is the STP instance ID. • color <0-32> is the color of the VLAN in the range of 0 to 32.
type spbm-bvlan	Creates a SPBM B-VLAN.

Use the data in the following table to use the `ip address` command.

Variable	Value
<A.B.C.D/X>|*<A.B.C.D> <A.B.C.D>*	Specifies the IP address and subnet mask in the format A.B.C.D/X or A.B.C.D A.B.C.D.
[<0-511>]	Specifies the MAC-offset value. The value is in the range of 0–511.

Use the data in the following table to use the `vlan i-sid` command.

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
<0-16777215>	Specifies the i-sid number. The value is in the range of <0-16777215>.

Creating a private VLAN

About this task

You can Create a private VLAN and set the port type. The primary and secondary VLAN IDs are associated with the same MTSI, the secondary VLAN inherits the primary VLAN configuration. You cannot create another VLAN with the same VLAN ID as the secondary VLAN. The secondary VLAN cannot be any other type of VLAN other than a secondary VLAN.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Create a private VLAN using ACLI:

   ```
   vlan create <2-4059> type pvlan-mstprstp <0-63> secondary <2-4059>
   ```

3. Specify a name for the VLAN:

   ```
   vlan create <2-4059> name
   ```

4. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   configure terminal
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform 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.

5. Set the port type:

   ```
   private-vlan <isolated|promiscuous|trunk}
   ```

   Note:

   If the port is a member of an MLT, the port inherits the private VLAN port type of the MLT. For more information about creating MLTs and LACPs, see,

   Configuring Link Aggregation, MLT, SMLT, and vIST on VSP Operating System Software, NN47227-503.

6. Enter VLAN Interface Configuration mode:

   ```
   enable
   configure terminal
   interface vlan <1-4059>
   ```

7. Add ports to the primary VLAN:

   ```
   vlan members add <1-4059> {slot/port[-slot/port][,...]}
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#vlan create 2 type pvlan-mstprstp 6 secondary 5
Switch:1(config)#interface gigabitethernet 1/36
Switch:1(config-if)#private-vlan isolated
```

```
Switch:1(config-if)# exit
Switch:1(config)# interface vlan 2
Switch:1(config-if)# vlan members add 2 1/36
```

Variable Definitions

Use the data in the following table to use the `vlan create` command.

Table 5: Variable definitions

Variable	Value
<2-4059>	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. The system reserves VLAN IDs 4060 to 4094 for internal use.
name *WORD<0-64>*	Specifies the VLAN name. The name attribute is optional.
type pvlan-mstprstp *<0-63>*	Creates a private VLAN by port. The variable *<0-63>* is the STP instance ID from 0 to 63. **Note:** MSTI instance 62 is reserved for SPBM if SPBM is enabled on the switch.
secondary*<2-4059>*	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. The system reserves VLAN IDs 4060 to 4094 for internal use.

Use the data in the following table to use the `private vlan port type` command.

Table 6: Variable definitions

Variable	Value
<isolated|promiscuous|trunk}	Specifies the port type. If not specified, the port type defaults to None. • Isolated: An Isolated port can belong only to one private VLAN • Promiscuous: A Promiscuous port can belong to many private VLANs • Trunk: A Trunk port can belong to many private VLANs, is tagged, and can also belong to non-private VLANs
`no private-vlan`	Port defaults to type None.
`default private-vlan`	Port defaults to type None.

Note:

If there are other non-private VLANs using the defined port, the following message is displayed:

```
All non private VLANs using this interface will be removed once this
port becomes a member of a private VLAN. Ports with private-vlan type
of isolated or promiscuous may only contain private VLANs. Do you wish
to continue (y/n) ?
```

Use the data in the following table to use the `interface vlan` and `vlan members add` commands.

Table 7: Variable definitions

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

Performing a general VLAN action

Perform a general VLAN action to initiate a specific function on a VLAN, such as clearing learned MAC addresses or ARP entries from the forwarding database by performing this procedure.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Perform a general VLAN action:

   ```
   vlan action <1-4059> {none|flushMacFdb|flushArp|flushIp|
   flushDynMemb|triggerRipUpdate|all}
   ```

Example

Perform a general VLAN action:

```
Switch(config)#vlan action 1 none

Switch(config)#vlan action 1 flushMacFdb

Switch(config)#vlan action 1 flushIp

Switch(config)#vlan action 1 flushDynMemb
```

Variable definitions

Use the data in the following table to use the `vlan action` command.

Table 8: Variable definitions

Variable	Value
none	Configures action to none. This action performs no updates.
flushMacFdb	Configures action to flushMacFdb. This action removes the learned MAC addresses from the forwarding database for the selected VLAN.
flushArp	Configures action to flushArp. This action removes the ARP entries from the address table for the selected VLAN.
flushIp	Configures action to flushIp. This action removes the learned IP addresses from the forwarding table for the selected VLAN.
flushDynMemb	Configures action to flushDynMemb. This action removes port members not configured as static from the list of active port members of a policy-based VLAN, and removes MAC addresses learned on those ports for this VLAN.
flushDynMemb	Configures action to flushDynMemb. This action removes port members not configured as static from the list of active port members of a policy-based VLAN, and removes MAC addresses learned on those ports for this VLAN.
triggerRipUpdate	Configures action to triggerRipUpdate.
all	Configures action to all and performs all preceding actions.

Configuring static MAC addresses for a VLAN

Configure the static MAC address parameters.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure a static MAC address of a VLAN:

```
vlan mac-address-static <1-4059> <0x00:0x00:0x00:0x00:0x00:0x00>
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}
```

Example

Configure a static MAC address of a VLAN:

```
Switch(config)#vlan mac-address-static 1 0x00:0x00:0x00:0x00:0x00:0x01
1/1
```

Variable definitions

Use the data in the following table to use the `vlan mac-address-static` command.

Table 9: Variable definitions

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
<0x00:0x00:0x00:0x00:0x00:0x00>	Indicates the MAC address.
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform 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.

Configuring the forwarding database timeout globally

Use the following procedure to configure the aging time globally for the forwarding database.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter the following command:

   ```
   mac-address-table aging-time <10-1000000>
   ```

Variable definitions

Use the data in the following table to use the `mac-address-table` command.

Table 10: Variable definitions

Variable	Value
aging-time	Specifies the timeout period for dynamically learned mac addresses on the vlan. The default valus is 300.
<10–1000000>	Specifies the range for the aging time.

Adding or removing ports in a VLAN

Add or remove the ports in a VLAN to configure the ports in the VLAN.

Procedure

1. Enter Interface Configuration mode:

   `enable`

   `configure terminal`

   `interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}` or `interface vlan <1-4059>`

   Note:

   If your platform 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.

2. Add ports in a VLAN:

   ```
   vlan members add <1-4059> {slot/port[/sub-port][-slot/port[/sub-port]][,...]} [{portmember|static|notallowed}]
   ```

3. Remove ports in a VLAN:

   ```
   vlan members remove <1-4059> {slot/port[/sub-port][-slot/port[/sub-port]][,...]} [{portmember|static|notallowed}]
   ```

Example

Add ports in a VLAN:

```
Switch(config-if)#vlan members add 1 1/2 static
```

Remove ports in a VLAN:

```
Switch(config-if)#vlan members remove 1 1/2 notallowed
```

Variable definitions

Use the data in the following table to use the `vlan members add` and `vlan members remove` commands.

Table 11: Variable definitions

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform 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.
portmember	Configures the port type as port member.

Configuring NLB support

Use Microsoft Network Load Balancing (NLB) to share the workload among multiple clustering servers. For information about software scaling capabilities, see *Release Notes for VSP Operating System Software*, NN47227-401.

Before you begin

Configure an IP address on the VLAN enabled with NLB.

About this task

Use the following procedure to configure NLB support on an IP interface to enable or disable NLB support.

The default value is NLB support disabled.

Note:

SPBM supports Network Load Balancing (NLB) unicast.

Procedure

1. Enter VLAN Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

`interface vlan <1-4059>`

2. Enable NLB support on an interface:

   `nlb-mode unicast`

3. Exit to Global Configuration mode:

   `exit`

Example

Configure unicast mode for VLAN 2.

```
Switch:1(config)#interface vlan 2
Switch:1(config-if)#nlb-mode unicast
Switch:1(config-if)#exit
```

Configuring a tagged port to discard untagged frames

Configure a tagged port to discard all untagged packets so that the frame is not classified into the default VLAN for the port.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   `enable`

   `configure terminal`

   `interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}`

   ✱ **Note:**

   If your platform 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.

2. Configure a tagged port to discard untagged frames:

   `untagged-frames-discard [port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}]`

3. Discard a tagged frame on an untagged port:

   `tagged-frames-discard [port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}] enable`

4. Untag the default VLAN on a tagged port:

   `untag-port-default-vlan [port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}] enable`

Example

Configure a tagged port to discard untagged frames:

```
Switch(config-if)#untagged-frames-discard port 1/1
```

Discard a tagged frame on an untagged port:

```
Switch(config-if)#tagged-frames-discard port 1/1 enable
```

Untag the default VLAN on a tagged port:

```
Switch(config-if)#untag-port-default-vlan port 1/2 enable
```

Variable definitions

Use the data in the following table to use optional parameters with the `untagged-frames-discard` command.

Table 12: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform 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.

Configuring SLPP

Enable the Simple Loop Prevention Protocol (SLPP) globally and for a VLAN to detect a loop and automatically stop it. The VLAN configuration controls the boundary of SLPP-PDU transmission.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable SLPP:

   ```
   slpp enable
   ```

3. Configure the transmission interval:

   ```
   slpp tx-interval <500-5000>
   ```

4. Add a VLAN to the transmission list:

   ```
   slpp vid <1-4059>
   ```

Example

Enable SLPP:

```
Switch(config)#slpp enable
```

Configure the transmission interval to 5000 milliseconds:

```
Switch(config)#slpp tx-interval 5000
```

Add a VLAN, with the VLAN ID 2, to the transmission list:

```
Switch(config)#slpp vid 1
```

Variable definitions

Use the data in the following table to use the `slpp` command.

Table 13: Variable definitions

Variable	Value
enable	Enables or disables the SLPP operation. You must enable the SLPP operation to enable the SLPP packet transmit and receive process. If you disable the SLPP operation, the system sends no SLPP packets and discards received SLPP packets. To set this option to the default value, use the default operator with the command. The default is disabled.
500–5000	Configures the SLPP packet transmit interval, expressed in milliseconds in a range from 500–5000. The default value is 500. To set this option to the default value, use the default operator with the command.
<1-4059>	Adds a VLAN, by VLAN ID, to a SLPP transmission list. Use the no operator to remove this configuration.

Job aid

The following table provides the Avaya recommended SLPP values.

Table 14: SLPP recommended values

Enable SLPP	Setting
Access SMLT	Yes
Core SMLT	No
Primary switch	
Packet Rx threshold	5
Transmission interval	500 milliseconds (ms) (default)
Secondary switch	
Packet Rx threshold	50
Transmission interval	500 ms (default)

Configuring SLPP packet-rx on a port

Enable SLPP by port to detect a loop and automatically stop it.

Important:

To provide protection against broadcast and multicast storms, Avaya recommends that you enable Rate Limiting for broadcast traffic and multicast traffic.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform 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.

2. Configure SLPP on a port:

   ```
   slpp port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   packet-rx [packet-rx-threshold <1-500>]
   ```

Example

```
Switch(config-if)# slpp port 1/1 packet-rx-threshold 5
```

Variable definitions

Use the data in the following table to use the `slpp port` command.

Table 15: Variable definitions

Variable	Value
<1-500>	Specifies the SLPP reception threshold on the ports, expressed as an integer. The packet reception threshold specifies how many SLPP packets the port receives before it is administratively disabled. To set this option to the default value, use the default operator with the command. The default value is 1. ❗ **Important:** Avaya recommends that you configure the rx-threshold above 50 slpp packets only on lightly loaded switches. If you configure the rx-threshold to a value greater than 50 on a heavily loaded switch and a loop occurs, the system can experience high CPU utilization.
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform 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.

Job aid

The following table provides the Avaya recommended SLPP values.

Table 16: SLPP recommended values

Enable SLPP	Setting
Access SMLT	Yes
Core SMLT	No
Primary switch	
Packet Rx threshold	5
Transmission interval	500 milliseconds (ms) (default)
Secondary switch	
Packet Rx threshold	50
Transmission interval	500 ms (default)

Configuring SLPP packet-tx on a VLAN

Enable SLPP by VLAN to detect a loop and automatically stop it. This configuration controls the boundary of SLPP-PDU transmission.

Important:

To provide protection against broadcast and multicast storms, Avaya recommends that you enable Rate Limiting for broadcast traffic and multicast traffic.

Procedure

1. Enter Interface Configuration mode:

   `enable`

   `configure terminal`

   `interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}` or `interface vlan <1-4059>`

   Note:

   If your platform 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.

2. Enable SLPP:

   `slpp enable`

3. Configure the transmission interval:

   `slpp tx-interval <500-5000>`

4. Add a VLAN to the transmission list:

   `slpp vid <1-4059>`

Example

Log on to the VLAN Interface Configuration mode:

```
Switch(config)# interface vlan 2
```

Enable SLPP:

```
Switch(config-if)# slpp enable
```

Configure the transmission interval to 500 milliseconds:

```
Switch(config-if)# slpp tx-interval 500
```

Add a VLAN, with the VLAN ID of 2, to the transmission list:

```
Switch(config-if)# slpp vid 2
```

Variable definitions

Use the data in the following table to use the `slpp` command.

Table 17: Variable definitions

Variable	Value
enable	Activates or disables the SLPP operation. You must enable the SLPP operation to enable the SLPP packet transmit and receive process. If you disable the SLPP operation, the system sends no SLPP packets and discards received SLPP packets. To set this option to the default value, use the default operator with the command. The default is disabled.
500–5000	Configures the SLPP packet transmit interval, expressed in milliseconds in a range from 500–5000. The default value is 500. To set this option to the default value, use the default operator with the command.
<1-4059>	Adds a VLAN, by VLAN ID, to a SLPP transmission list. Use the no operator to remove this configuration.

Viewing SLPP information

Use SLPP information to view loop information.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. View SLPP information:

   `show slpp`

Example

```
Switch# show slpp
```

```
================================================================================
                                   SLPP Info
================================================================================
                   operation :  enabled
                 tx-interval :  500
                        vlan : 2
```

Viewing SLPP information for a port

Show SLPP information for a port so that you can view the loop information for a port.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View SLPP information for a port:

   ```
   show slpp interface GigabitEthernet [{slot/port[/sub-port][-slot/
   port[/sub-port]][,...]}]
   ```

3. Clear SLPP packet RX counters:

   ```
   clear slpp stats port [{slot/port[/sub-port][-slot/port[/sub-port]]
   [,...]}]
   ```

Example

```
Switch# show slpp interface GigabitEthernet 1/7
```

```
================================================================================
                                    Port Interface
   ================================================================================
   PORT        PKT-RX      PKT-RX     INCOMING   SLPP PDU
   NUM                     THRESHOLD  VLAN ID    ORIGINATOR
   --------------------------------------------------------------------------------
   1/7         enabled     5

   PORT        PKT-RX      TIME LEFT
   NUM         COUNT       TO CLEAR RX COUNT
   --------------------------------------------------------------------------------
   1/7         29          21600
```

Variable definitions

Use the data in the following table to use the `show slpp interface GigabitEthernet` command.

Table 18: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform 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.

Viewing VLAN information

View the VLAN information to display the basic configuration for all VLANs or a specified VLAN.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View VLAN information:

   ```
   show vlan basic <1-4059>
   ```

3. View advanced parameters:

   ```
   show vlan advance <1-4059>
   ```

Example

View VLAN information for VLAN 2:

```
Switch:1> show vlan basic 2
```

```
=====================================================================================
                                   Vlan Basic
=====================================================================================
VLAN                              INST
ID    NAME             TYPE         ID  PROTOCOLID SUBNETADDR      SUBNETMASK   VRFID

-------------------------------------------------------------------------------------
2     VLAN-2          byPort       0   none       N/A             N/A           0
```

View VLAN information:

```
Switch:1> show vlan basic
```

```
=====================================================================================
                                   Vlan Basic
=====================================================================================
VLAN                              INST
ID    NAME             TYPE         ID  PROTOCOLID SUBNETADDR      SUBNETMASK   VRFID

-------------------------------------------------------------------------------------
1     Default          byPort       0   none       N/A             N/A          0

2     abc              byPort       0   none       N/A             N/A          0

3     VLAN-VRRP        byPort       0   none       N/A             N/A          0

4     VLAN-6           byPort       0   none       N/A             N/A          1

5     VLAN-7           byPort       0   none       N/A             N/A          1

6     VLAN-8           byPort       0   none       N/A             N/A          1

19    VLAN-9           byPort       0   none       N/A             N/A          0

10    VLAN-10          byPort       0   none       N/A             N/A          0

11    VLAN-11          byPort       0   none       N/A             N/A          0

12    VLAN-12          byPort       0   none       N/A             N/A          0

13    VLAN-13          spbm-bvlan   62  none       N/A             N/A          0
```

```
14    VLAN-14          spbm-bvlan   62   none        N/A             N/A           0
15    VLAN-15          byPort       1    none        N/A             N/A           0
--More-- (q = quit)
```

View advanced parameters:

```
Switch:1> show vlan advance
```

```
=================================================================================
                                  Vlan Advance
=================================================================================
VLAN             IF     AGING MAC                  USER
ID    NAME       INDEX TIME  ADDRESS               DEFINEPID ENCAP  DSAP/SSAP
---------------------------------------------------------------------------------
2     Default 2050  0     00:24:7f:9f:6a:03  0x0000
```

Variable definitions

Use the data in the following table to use optional parameters with the `show vlan basic` and `show vlan advance` commands.

Table 19: Variable definitions

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

Viewing private VLAN information

You can view the private VLAN information to display the primary and secondary VLANs and I-SIDs, and also view the private VLAN port types.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View private VLAN information:

   ```
   show vlan private—vlan <1-4059>
   ```

3. View private vlan port information:

   ```
   show interfaces gigabitethernet private-vlan
   ```

Example

View VLAN information for private VLAN :

```
Switch:1(config)# show vlan private-vlan
```

```
===============================================================================
                                  PRIVATE VLAN
===============================================================================
Primary               Primary               Secondary             Secondary
VLAN                  ISID                  VLAN                  ISID
-------------------------------------------------------------------------------
3                     75                     5                     75
10                    22                     15                    22

All 2 out of 2 Total Num of Private Vlans displayed
```

View port information for private VLAN:

```
Switch:1(config)# show interfaces gigabitethernet private-vlan
```

```
===============================================================================
                                Port Private Vlans
===============================================================================
PORT                                      VID
NUM    TAGGING   PVLAN    PVLAN TYPE     TYPE       VID
-------------------------------------------------------------------------------
1/1    enable    enable   isolated       secondary  5
1/2    enable    enable   promiscuous    primary    3
1/3    enable    enable   trunk          both       3/5
```

Viewing brouter port information

View the brouter port information to display the brouter port VLAN information for all VLANs on the device or for the specified VLAN.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View brouter port information:

   ```
   show vlan brouter-port
   ```

Example

View brouter port information:

```
Switch:1> show vlan brouter-port
```

```
            Vlan Id          Port        VrfId
        ========         =====       ======
           2202          1/11        0

All 1 out of 1 Total Num of Vlan Brouter Port Entries displayed
```

Viewing VLAN port member status

View the VLAN port member status to display the port member status for all VLANs on the device or for the specified VLAN.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View VLAN port member status:

   ```
   show vlan members [<1-4059>][null-vlan][port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}]
   ```

Example

View VLAN port member status:

```
Switch:1> show vlan members port 1/2
```

```
===============================================================================
                                   Vlan Port
===============================================================================
VLAN PORT               ACTIVE             STATIC             NOT_ALLOW
ID   MEMBER             MEMBER             MEMBER             MEMBER
-------------------------------------------------------------------------------
2    1/2,1/5-1/8,1/11,  1/2,1/5-1/8,1/11,

     1/14,1/26,1/38     1/14,1/26,1/38


3    1/2,1/5-1/8,1/14,  1/2,1/5-1/8,1/14,

     1/26,1/38          1/26,1/38


4    1/1-1/2,1/5-1/8,   1/1-1/2,1/5-1/8,

     1/13-1/14,1/25-    1/13-1/14,1/25-

     1/26,1/37-1/38     1/26,1/37-1/38


100  1/2,1/14,1/23-     1/2,1/14,1/23-

     1/24,1/26-1/28,    1/24,1/26-1/28,

     1/38               1/38


300  1/2,1/5-1/8,1/14,  1/2,1/5-1/8,1/14,

     1/26,1/38          1/26,1/38
```

Variable definitions

Use the data in the following table to use optional parameters with the `show vlan members` command.

Table 20: Variable definitions

Variable	Value
null-vlan	Displays port members of the NULL VLAN. This is a place holder VLAN for ports that are not members of any port-based VLAN. When a port is removed from all port-based VLANs, it is added to the NULL VLAN as a port member. The NULL VLAN is an internal construct and cannot be deleted.
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform 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. If you do not specify a port, the command shows information for all the ports.
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. **Important:** Entering a VLAN ID is optional. If you enter a VLAN ID the command shows information for the specified VLAN or port. Without the VLAN ID the command shows information for all the configured VLANs.

Viewing VLAN forwarding database information

Use this procedure to display the MAC addresses that are learned or statically configured for a VLAN. In order to learn you have to be connected to another switch or host and receive some traffic.

Procedure

1. Log on to the switch to enter User EXEC mode.

2. View VLAN forwarding database information:

```
show vlan mac-address-entry [<1-4059>]
```

Example

View VLAN forwarding database information:

```
Switch:1> show vlan mac-address-entry
```

```
================================================================================
                                    Vlan Fdb
================================================================================
VLAN            MAC                                 SMLT
ID   STATUS     ADDRESS            INTERFACE  REMOTE TUNNEL
--------------------------------------------------------------------------------
1    learned    f8:15:47:e1:80:0c  Port-1/2   false  -
2    learned    32:20:d3:81:00:77  Port-1/9   false  -
4    learned    b4:a9:5a:2b:78:31  Port-2/1   false  -

3 out of 3 entries in all fdb(s) displayed.
```

View where entries are learned. The TUNNEL column indicates where in the SPBM network an entry is learned.

```
Switch:1> show vlan mac-address-entry spbm-tunnel-as-mac
```

```
================================================================================
                                    Vlan Fdb
================================================================================
VLAN            MAC                                 SMLT
ID   STATUS     ADDRESS            INTERFACE  REMOTE TUNNEL
--------------------------------------------------------------------------------
1    learned    f8:15:47:e1:80:0c  Port-1/2   false  -
2    learned    32:20:d3:81:00:77  Port-1/9   false  -
4    learned    b4:a9:5a:2b:78:31  Port-2/1   false  -

3 out of 3 entries in all fdb(s) displayed.
```

Variable definitions

Use the data in the following table to use optional parameters with the `show vlan mac-address-entry` command.

Table 21: Variable definitions

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
mac <0x00:0x00:0x00:0x00:0x00:0x00>	Specifies the MAC address.
port {slot/port[-slot/port][,...]}	Specifies the port or port list.

Table continues…

Variable	Value
spbm-tunnel-as-mac	Displays where entries are learned. The TUNNEL column indicates where in the SPBM network an entry is learned.

Viewing NLB-mode information

View Network Load Balancing-mode (NLB-mode) information.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. View NLB port information:`show interface vlan nlb-mode` *`<1-4059>`*

Example

View NLB-mode information.

```
Switch:1#show interface vlan nlb-mode
==========================================================================
                             Vlan Nlb
==========================================================================
VLAN_ID NLB_ADMIN_MODE NLB_OPER_MODE PORT_LIST MLT_GROUPS
--------------------------------------------------------------------------
2   unicast disable
Total Entries: 1
```

Displaying C-VLAN and Switched UNI I-SID information

Use the following procedure to display C-VLAN I-SID information.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. Display the C-VLAN to I-SID associations:

   `show vlan i-sid <1-4094>`

3. Display I-SID information and Switched UNI to I-SID associations:

   `show i-sid <1-16777215>`

4. Display the IS-IS SPBM multicast-FIB calculation results by I-SID:

   `show isis spbm i-sid {all|config|discover} [vlan <1-4094>] [id <1-16777215>] [nick-name <x.xx.xx>]`

5. Display all elan I-SID.
    - `show i-sid elan`
6. Display I-SID configured on MLT.
    - `show mlt i-sid`
7. Display I-SID configured on port.
    - `show interfaces gigabitethernet i-sid`

Example

```
Switch#show vlan i-sid
================================================================================
                                   Vlan I-SID
================================================================================
VLAN_ID    I-SID
--------------------------------------------------------------------------------
1
2
5          5
10
20
```

```
Switch#show isis spbm i-sid all
=================================================================================
                                 SPBM ISID INFO
=================================================================================
ISID   SOURCE NAME    VLAN   SYSID                TYPE         HOST_NAME
---------------------------------------------------------------------------------
200    1.11.16        1000   0014.c7e1.33df       config       ERS-4000
300    1.11.16        1000   0014.c7e1.33df       config       ERS-4000
400    1.11.16        1000   0014.c7e1.33df       config       ERS-4000
200    1.11.16        2000   0014.c7e1.33df       config       ERS-4000
300    1.11.16        2000   0014.c7e1.33df       config       ERS-4000
400    1.11.16        2000   0014.c7e1.33df       config       ERS-4000
200    1.12.45        1000   0016.ca23.73df       discover     VSP-9001
300    1.12.45        1000   0016.ca23.73df       discover     VSP-9001

---------------------------------------------------------------------------------
 Total number of SPBM ISID entries configed: 6
---------------------------------------------------------------------------------
 Total number of SPBM ISID entries discovered: 2
---------------------------------------------------------------------------------
 Total number of SPBM ISID entries: 8
---------------------------------------------------------------------------------
```

```
switch#show i-sid

==================================================================================
                                    Isid Info
==================================================================================
ISID        ISID                    PORT               MLT                ORIGIN
ID          TYPE       VLANID       INTERFACES         INTERFACES
----------------------------------------------------------------------------------
999         ELAN       99           -                  c110:100           CONFIG
                       99           1/21               -

c: customer vid    u: untagged-traffic
```

```
All 1 out of 1 Total Num of i-sids displayed
```

```
switch#show mlt i-sid
================================================================================
                                 MLT Isid Info
================================================================================
              ISID                   ISID
MLTID IFINDEX ID       VLANID C-VID  TYPE     ORIGIN           BPDU
--------------------------------------------------------------------------------
10    6153    100      N/A    20     ELAN     CONFIG
--------------------------------------------------------------------------------

1 out of 1 Total Num of i-sid endpoints displayed
```

```
switch#show interfaces gigabitEthernet i-sid
================================================================================
                                 PORT Isid Info
================================================================================
                ISID                   ISID
PORTNUM IFINDEX ID       VLANID C-VID  TYPE     ORIGIN          BPDU
--------------------------------------------------------------------------------
1/1     192     100      N/A    10     ELAN     CONFIG
1/2     193     100      N/A    10     ELAN     CONFIG
--------------------------------------------------------------------------------

2 out of 3 Total Num of i-sid endpoints displayed
```

Variable definitions

Use the data in the following table to use the **`show vlan i-sid`** commands.

Variable	Value
<1-4059>	Displays I-SID information for the specified C-VLAN. You can specify the VLAN ID.

Use the data in the following table to use the **`show i-sid`** commands

Variable	Value
<1–16777215>	Displays I-SID information. You can specify the I-SID ID.

Use the data in the following table to use the **`show isis`** commands.

Variable	Value
spbm i-sid {all|config|discover}	• all: displays all I-SID entries • config: displays configured I-SID entries • discover: displays discovered I-SID entries

Job aid

The following sections describe the fields in the outputs for the C-VLAN I-SID show commands.

show vlan i-sid

The following table describes the fields in the output for the **`show vlan i-sid`** command.

Parameter	Description
VLAN_ID	Indicates the VLAN IDs.
I-SID	Indicates the I-SIDs associated with the specified C-VLANs.

show i-sid

The following table describes the fields in the output for the **`show i-sid`** command.

Parameter	Description
I-SID	Indicates the I-SID IDs.
I-SID TYPE	Indicated the I-SID type. • T-UNI: Transparent UNI service. • ELAN: any to any service (switched service). • CVLAN: CVLAN based service.
VLANID	Indicates the VLAN IDs.
PORT INTERFACES	Indicated the port interface.
MLT INTERFACES	Indicates the MLT interface.
ORIGIN	Indicates if the I-SID is discovered by fabric attach or manually added.

show isis spbm i-sid

The following describes the fields in the output for the **`show isis spbm i-sid`** command.

Parameter	Description
ISID {all | discover | config}	Indicates the IS-IS SPBM I-SID identifier. • all: display all SPBM I-SID • discover: display discovered SPBM I-SID • config: display configured SPBM I-SID
SOURCE NAME	Indicates the nickname of the node where this I-SID was configured or discovered. **Note:** SOURCE NAME is equivalent to nickname.
VLAN	Indicates the B-VLAN where this I-SID was configured or discovered.
SYSID	Indicates the system identifier.

Table continues…

Parameter	Description
TYPE	Indicates the SPBM I-SID type as either configured or discovered.
HOST_NAME	Indicates the host name of the multicast FIB entry.

Chapter 5: VLAN configuration using EDM

This chapter describes how to configure and manage Virtual Local Area Networks (VLAN) using Enterprise Device Manager (EDM).

Configuring the VLAN feature on a port

Configure the VLAN feature on a port.

Procedure

1. In the Device Physical View tab, select a port or multiple ports.
2. In the Navigation tree, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **VLAN** tab.
5. To perform tagging, select **PerformTagging**.
6. To discard tagged frames, select **DiscardTaggedFrames**.
7. To discard untagged frames, select **DiscardUntaggedFrames**.
8. To use the Untag Default VLAN feature, select **UntagDefaultVlan**.

   Important:

   Avaya recommends that you enable tagging on the port before you configure UntagDefaultVlans.
9. Enter a default VLAN ID.
10. To enable spoof detect, select **SpoofDetect**.
11. In the Classification area, select the types of VLAN to enable.
12. In the **Classification** area, select the Private VLAN port type. See Creating a private VLAN on page 63 for more information.
13. Click **Apply**.
14. Click **Close**.

VLAN field descriptions

Use the data in the following table to use the **VLAN** tab.

Name	Description
PerformTagging	If checked, this port is a tagged (Trunk) Port. It can belong to multiple port-based VLANs and a VLAN tag is inserted in every frame it transmits. If it is not checked, the port is an untagged (Access) port. The default is disabled.
VlanIdList	Identifies which VLANs this port is assigned.
DiscardTaggedFrames	If selected, and the port is untagged (an access port), tagged frames received on the port are discarded by the forwarding process. If clear, tagged frames are processed normally. The default is disabled.
DiscardUntaggedFrames	If selected and the port is tagged (a trunk port),untagged frames received on the port are discarded by the forwarding process. If clear, untagged frames are processed normally. The default is disabled.
UntagDefaultVLAN	If selected, even if the port is tagged (a trunk port), frames forwarded to the default VLAN for the port are not tagged. The default is disabled.
DefaultVlanId	Specifies the VLAN ID assigned to untagged frames received on this trunk port that match no policy-based VLAN to whch the port belongs.
Protocol	Enables protocol-based VLAN on the port. This feature is always enabled.
PrivateVlanPortType	Specifies the port type. If not specified, the port type defaults to None. • Isolated: Only private VLANs are permitted on isolated ports. • Promiscuous: Only private VLANs are permitted on promiscuous ports. • Trunk: The port is tagged.

Viewing existing VLANs

Display existing VLANs to view all defined VLANs, their configurations, and the current status.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. View the configured VLANs in the **Basic** tab.
4. View the configured private VLANs in the **Private VLAN** tab.

Creating a port-based VLAN

Create a port-based VLAN to add a new VLAN. To create a different type of VLAN, see one of the following procedures:

- Creating a protocol-based VLAN on page 67
- Creating an SPBM B-VLAN on page 68

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. In the **Basic** tab, click **Insert**.
4. In the **Id** box, enter an unused VLAN ID, or use the ID provided.
5. In the **Name** box, type the VLAN name, or use the name provided.
6. In the **Color Identifier** box, click the down arrow and choose a color from the list, or use the color provided.
7. In the **MstpInstance** box, click the down arrow and choose an msti instance from the list.
8. In the **Type** box, select **byPort**.
9. In the **PortMembers** box, click the **(...)** button.
10. Click on the ports to add as member ports.

    The ports that are selected are recessed, while the nonselected ports are not recessed. Port numbers that appear dimmed cannot be selected as VLAN port members.
11. Click **OK**.
12. Cick **Insert**.

Basic field descriptions

Use the data in the following table to use the **Basic** tab.

Name	Description
Id	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. The system reserves VLAN IDs 4060 to 4094 for internal use.
Name	Specifies the name of the VLAN.
IfIndex	Specifies the logical interface index assigned to the VLAN.
Color Identifier	Specifies a proprietary color scheme to associate a color with the VLAN. Color does not affect how frames are forwarded.
Type	Specifies the type of VLAN: • byPort • byProtocolId • spbm-bvlan
MstpInstance	Identifies the MSTP instance.
VrfId	Indicates the Virtual Router to which the VLAN belongs.
VrfName	Indicates the name of the Virtual Router to which the VLAN belongs.
PortMembers	Specifies the slot/port of each VLAN member.
ActiveMembers	Specifies the slot/port of each VLAN member.
StaticMembers	Specifies the slot/port of each static member of a policy-based VLAN.
NotAllowToJoin	Specifies the slot/ports that are never allowed to become a member of the policy-based VLAN.
ProtocolId	Specifies the network protocol for protocol-based VLANs. If the VLAN type is port-based, none is displayed in the Basic tab ProtocolId field.

Note:

If you or another user changes the name of an existing VLAN using the VLAN **Basic** tab (or using ACLI), the new name does not initially appear in EDM. To display the updated name, do one of the following:

- Refresh your browser to reload EDM.
- Logout of EDM and login again to restart EDM.
- Click **Refresh** in the VLAN **Basic** tab toolbar. (If the old VLAN name appears in any other tabs, click the **Refresh** toolbar button in those tabs as well.)

Creating a private VLAN

Before you begin

- To create a private VLAN, you must set the VLAN type to private and set the private VLAN port type
- The ports you add to a private VLAN must have a port type of isolated, promiscuous, or trunk

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. In the **Basic** tab, click **Insert**.
4. In the **Id** box, enter an unused VLAN ID, or use the ID provided.
5. In the **Name** box, type the VLAN name, or use the name provided.
6. In the **Color Identifier** box, click the down arrow and choose a color from the list, or use the color provided.
7. In the **MstpInstance** box, click the down arrow and choose an msti instance from the list.
8. In the **Type** box, select **private**.
9. In the **PortMembers** box, click the **(...)** button.
10. Click on the ports to add as member ports.

    The ports that are selected are recessed, while the non-selected ports are not recessed. Port numbers that appear dimmed cannot be selected as VLAN port members.
11. Click **OK**.
12. In the **Secondary Vlan** box, enter an unused VLAN ID.
13. Click **Insert**.
14. Collapse the **VLANs** tab.

    The VLAN is added to the **Basic** tab.

    To set the port type for the private VLAN:
15. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
16. Click **VLANs**.
17. In the Classification area, select the **PrivateVlanPortType**.
18. Click **Apply**.
19. Click **Close**.

Basic field descriptions

Use the data in the following table to use the **Basic** tab.

Name	Description
Id	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
Name	Specifies the name of the VLAN.
IfIndex	Specifies the logical interface index assigned to the VLAN.
Color Identifier	Specifies a proprietary color scheme to associate a color with the VLAN. Color does not affect how frames are forwarded.
MstpInstance	Identifies the MSTP instance.
Type	Specifies the type of VLAN: • byPort • byProtocolId • spbm-bvlan • private
VrfId	Indicates the Virtual Router to which the VLAN belongs.
VrfName	Indicates the name of the Virtual Router to which the VLAN belongs.
PortMembers	Specifies the slot/port of each VLAN member.
Secondary Vlan	Specifies the VLAN ID for the Secondary Vlan.
ActiveMembers	Specifies the slot/port of each VLAN member.
StaticMembers	Specifies the slot/port of each static member of a policy-based VLAN.
NotAllowToJoin	Specifies the slot/ports that are never allowed to become a member of the policy-based VLAN.
ProtocolId	Specifies the network protocol for protocol-based VLANs. If the VLAN type is port-based, none is displayed in the Basic tab ProtocolId field.

✱ **Note:**

If you change the name of an existing VLAN using the VLAN **Basic** tab, or using ACLI, the new name does not initially appear in EDM. To display the updated name, perform one of the following actions:

- Refresh your browser to reload EDM
- Restart EDM (logout and login)
- Click **Refresh** in the VLAN **Basic** tab toolbar. If the old VLAN name appears in any other tabs, click the **Refresh** toolbar button in those tabs as well

Use the data in the following table to use the **VLAN** tab.

Name	Description
PrivateVlanPortType	Specifies the port type. If not specified, the port type defaults to None. • Isolated: An Isolated port can belong only to one private VLAN • Promiscuous: A Promiscuous port can belong to many private VLANs. • Trunk: A Trunk port can belong to many private VLANs, is tagged, and can also belong to non-private VLANs.

Configuring an IP address for a VLAN

Assign an IP address to a VLAN to enable routing on the VLAN.

About this task

If you configure the SLA Mon agent address under an IP interface or VLAN, you must remove the SLA Mon address before you can remove the IP address or VLAN.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. In the **Basic** tab, select the VLAN for which you are configuring an IP address.
4. Click **IP**.
5. Click **Insert**.
6. Configure the required parameters.
7. Click **Insert**.

IP Address field descriptions

Use the data in the following table to use the **IP Address** tab.

Name	Description
Interface	Shows the interface to which this entry applies.
Ip Address	Specifies the IP address to associate with the VLAN.
Net Mask	Specifies the subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits configured to 1 and all the hosts bits configured to 0.
BcastAddrFormat	Shows the IP broadcast address format on this interface.
ReasmMaxSize	Shows the size of the largest IP datagram which this entity can reassemble from incoming IP fragmented datagrams received on this interface.
VlanId	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
BrouterPort	Indicates whether this entry corresponds to a brouter port, as oppose to a routable VLAN.
MacOffset	Routable VLANS are assigned MAC addresses arbitrarily or by offset. Their MAC addresses are: • 24 bits: Avaya ID • 12 bits: Chassis ID • 12 bits: 0xA00-0xFFF If you enter the MAC offset, the lowest 12 bits are 0xA00 plus the offset. If not, they are arbitrary.
VrfId	Associates the VLAN or brouter port with a VRF. VRF ID 0 is reserved for the administrative VRF.

Changing VLAN port membership

Modify VLAN port members to control access to the VLAN.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.

3. Double-click the **PortMembers** number for the VLAN for which you want to modify port membership.
4. Click the port members you wish to add or remove.
5. Click **Ok**.
6. Click **Apply**.

   The VLAN port membership is changed.

Creating a protocol-based VLAN

Use a protocol-based VLAN so that the VLAN only carries certain traffic types.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. In the **Basic** tab, click **Insert**.
4. In the **Id** box, type the unique VLAN ID or use the ID provided.
5. In the **Name** box, type the VLAN name or use the name provided.
6. In the **Color Identifier** box, select the color or use the color provided.

   This color is used to visually distinguish the VLANs in a network.
7. In the **MstpInstance** box, click the down arrow and choose an MSTI instance from the list.
8. In the **Type** box, select **byProtocolId**.

   This activates additional fields needed to configure protocol-based VLANs.
9. To specify the VLAN port membership, click the button **(...)** for one of the following fields:

   Port Members

   OR

   StaticMembers

   OR

   NotAllowToJoin
10. Click each port button to choose the desired membership color.

    Yellow: Potential members—dynamic (potential members are treated as always members)

    OR

    Green: Always members—static

    OR

Red: Never members—not allowed to join

Important:

In a protocol-based VLAN, a potential member becomes an active member of the VLAN after a frame of the specified protocol is received.

11. Click **Insert**.

Creating a SPBM B-VLAN

Create a Shortest Path Bridging MAC (SPBM) Backbone VLAN (B-VLAN). Each SPBM network instance is associated with at least one backbone VLAN (B-VLAN) in the core SPBM network. This VLAN is used for both control plane traffic and dataplane traffic.

Note:

Avaya recommends that you always configure two B-VLANs in an SPBM dual-homing environment.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. In the **Basic** tab, click **Insert**.
4. In the **Id** box, enter an unused VLAN ID, or use the ID provided.
5. In the **Name** box, type the VLAN name, or use the name provided.
6. In the **Color Identifier** box, click the down arrow and choose a color from the list, or use the color provided.
7. In the **Type** box, select **spbm-bvlan**.
8. Cick **Insert**.
9. Collapse the **VLANs** tab.

   The VLAN is added to the **Basic** tab.

Configuring advanced VLAN features

Use advanced VLAN features to configure the VLAN name, aging time, VLAN operation action, and QoS level. The VLAN Operation Action parameter can be useful for troubleshooting.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. In the VLANs tab, click the **Advanced** tab.
4. Configure the parameters as required by double-clicking fields to make changes.

   You cannot make changes to fields that appear dim.
5. Click **Apply**.

Advanced field descriptions

Use the data in the following table to use the **Advanced** tab.

Name	Description
Id	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
Name	Specifies the name of the VLAN.
IfIndex	Specifies the logical interface index assigned to the VLAN.
Type	Specifies the type of VLAN: • byPort • byProtocolId • spbm-bvlan • private
I-sid	Specifies the I-SID number assigned to a customer VLAN (C-VLAN). The range is 0 – 16777215. The default value is 0, which indicates that no I-SID is assigned.
ProtocolId	Specifies the network protocol for protocol-based VLANs. If the VLAN type is not protocol-based, None is displayed in the Basic tab ProtocolId field.
AgingTime	Specifies the timeout period for dynamic VLAN membership. A potential VLAN port is made ACTIVE after it receives a packet that matches the VLAN; if no such packet is received for AgingTime seconds, the port is no longer active. The default is 600.

Table continues…

Name	Description
MacAddress	Specifies the MAC address assigned to the virtual router interface for this VLAN. This field is relevant only after the VLAN is configured for routing. This MAC address is used as the Source MAC in routed frames and ARP replies.
Vlan Operation Action	Performs an operation on the VLAN. The values are: • none • flushMacFdb: Configures action to flushMacFdb. This action removes the learned MAC addresses from the forwarding database for the selected VLAN. • flushArp: Configures action to flushArp. This action removes the ARP entries from the address table for the selected VLAN. • flushIp: Configures action to flushIp. This action removes the learned IP addresses from the forwarding table for the selected VLAN. • flushDynMemb: Configures action to flushDynMemb. This action removes port members not configured as static from the list of active port members of a policy-based VLAN and removes MAC addresses learned on those ports. • all: Configures action to all. This action performs all the supported actions; it does does not perform the Snoop-related actions. The default is none.
Result	Specifies the result code after you perform an action.
SpbMcast	Enables or disables Multicast over Fabric Connect. The default is disabled.
RmonEnable	Enables or disables Remote Monitoring (RMON) on the interface. The default is disabled.
IpsecEnable	Enables or disables IP security (IPsec) on the interface. The default is disabled.

Configuring NLB support using EDM

Use Microsoft Network Load Balancer (NLB) to share the workload among multiple clustering servers. For more information about software scaling capabilities, see *Release Notes for VSP Operating System Software*, NN47227-401.

Before you begin

The VLAN exists and has an associated IP address.

About this task

Procedure

1. In the navigation pane, expand the following folders: **Configuration** --> **VLAN**.
2. Click **VLANs**.
3. Click the **Advanced** tab.
4. In the row for the VLAN, double-click the value in the **NlbMode** column.
5. Select the appropriate value.
6. Click **Apply**.

Configuring a port to accept tagged or untagged frames

Configure a port to accept tagged or untagged frames.

Procedure

1. In the Device Physical View tab, select a port.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **VLAN** tab.
5. To configure tagging on the port, select the **PerformTagging** check box.

   This setting applies to all VLANs associated with the port.

   Important:

   If the check box is selected, tagging is enabled. All frames sent from this port are tagged.

   If the check box is cleared, tagging is disabled. The port does not send tagged frames. The switch removes the tag before sending the frame out of the port.
6. To discard tagged frames on a port for which tagging is disabled, select **DiscardTaggedFrames**.
7. To discard untagged frames on a port for which tagging is enabled, select **DiscardUntaggedFrames**.
8. To designate a default VLAN to associate with a packet that does not match a policy-based VLAN, enter a VLAN ID in the **DefaultVLANId** box or use the default VLAN 1.
9. Click **Apply**.

10. Click **Close**.

Configuring untagging default VLAN on a tagged port

Configure an untagged default VLAN on a tagged port to separate untagged packets originating from a PC from the tagged packets originating from an IP phone.

Procedure

1. In the Device Physical View tab, select a port.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **VLAN** tab.
5. Select **UntagDefaultVlan**.
6. In the **DefaultVlanId**, enter a default VLAN ID.
7. Click **Apply**.
8. Click **Close**.

Configuring SLPP globally

Enable the Simple Loop Prevention Protocol (SLPP) to detect a loop and automatically stop it.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **SLPP**.
3. Click the **Global** tab.
4. Select **GlobalEnable**.
5. In the **TransmissionInterval** box, type a value for the time interval for loop detection.
6. Click **Apply**.

Global field descriptions

Use the data in the following table to use the **Global** tab.

Name	Description
GlobalEnable	Activates or disables SLPP globally. The default is disabled.
TransmissionInterval	Configures the interval for which loop detection occurs. The interval is expressed in milliseconds in a range from 500–5000. The default value is 500.

Job aid

The following table provides the Avaya recommended SLPP values.

Table 22: SLPP recommended values

Enable SLPP	Setting
Access SMLT	Yes
Core SMLT	No
Primary switch	
Packet Rx threshold	5
Transmission interval	500 milliseconds (ms) (default)
Secondary switch	
Packet Rx threshold	50
Transmission interval	500 ms (default)

Configuring the SLPP by VLAN

Activate SLPP on a VLAN to enable forwarding of the SLPP packet over the VLAN. This configuration controls the boundary of SLPP-PDU transmission.

Before you begin

- Enable SLPP globally before you configure it on a VLAN.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **SLPP**.
3. Click the **VLANS** tab.
4. Click **Insert**.
5. Click the **VlanId** ellipses (...).
6. Select the desired VLAN ID.

7. Click **Ok**.
8. Select **SlppEnable**.
9. Click **Insert**.

Insert VLANs field descriptions

Use the data in the following table to use the **Insert VLANS** dialog box.

Name	Description
VlanId	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
SlppEnable	Activates SLPP on the selected VLAN. The SLPP packet transmission and reception process is active only if you enable the SLPP operation. If you disable the SLPP operation, the following occurs: • the system sends no SLPP packets • the system discards received SLPP packets The default is enabled.

Configuring the SLPP by port

Use SLPP on a port to avoid traffic loops on the port.

Important:

To provide protection against broadcast and multicast storms, Avaya recommends that you enable Rate Limiting for broadcast traffic and multicast traffic.

Before you begin

- Enable SLPP globally before you configure it on a port.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **SLPP**.
3. Click the **Ports** tab.

4. Double-click the **PktRxThreshold** box for the desired port to edit the threshold value for packet reception.
5. Double-click the **SlppEnable** box for the desired port.
6. Select **true** to enable SLPP.
7. Click **Apply**.

Ports field descriptions

Use the data in the following table to use the **Ports** tab.

Name	Description
IfIndex	Specifies the interface index number for a port.
PktRxThreshold	Specifies the threshold for packet reception. Configure the SLPP packet receive threshold to a value (1- 500) that represents the number of received SLPP-PDUs to shut down the port. This variable is a port-level parameter, therefore if the port is tagged, SLPP-PDUs from the various VLANs increment this single threshold counter. The default is 1.
SlppEnable	Activates SLPP on the selected interface. The default is disabled.
IncomingVlanId	Shows the VLAN ID of the classified packet on a port disabled by SLPP.
SrcNodeType	Specifies the source node type of the received SLPP packet.
PktRxCount	Shows the total number of SLPP packets the port received.
TimeToClrPktRxCount	Specifies the timer to clear the SLPP receive counter. After you enable SLPP and the port receives SLPP PDUs, the timer starts. After the timer exceeds the configured value, the system resets the count to zero. The default is 21,600 seconds.
RemainingTimeToClrPktRxCount	Shows the time remaining before the SLPP receive counter is reset to zero.

Job aid

The following table provides the Avaya recommended SLPP values.

Table 23: SLPP recommended values

Enable SLPP	Setting
Access SMLT	Yes
Core SMLT	No
Primary switch	
Packet Rx threshold	5
Transmission interval	500 milliseconds (ms) (default)
Secondary switch	
Packet Rx threshold	50
Transmission interval	500 ms (default)

Configuring directed broadcast on a VLAN

Configure directed broadcast on a VLAN to enable or disable directed broadcast traffic forwarding for an IP interface.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. Select the **Basic** tab.
4. Select a VLAN.
5. Click **IP**.
6. Click the **Direct Broadcast** tab.
7. Select **DirectBroadcastEnable**.

   Important:

   Configure multiple VLANs or IPs in the same subnet but in different systems simultaneously.
8. Click **Apply**.

Direct Broadcast field descriptions

Use the data in the following table to use the **Direct Broadcast** tab.

Name	Description
DirectBroadcastEnable	Specifies that an Isolated Routing Port (IRP) can forward directed broadcast traffic. A directed

Name	Description
	broadcast is a frame sent to the subnet broadcast address on a remote IP subnet. By disabling or suppressing directed broadcast on an interface, all frames sent to the subnet broadcast address for a local router interface are dropped. Disabling this function protects a host from possible denial of service (DoS) attacks. With the feature enabled, the Control Processor (CP) does not receive a copy of the directed broadcast. As a result, the system does not respond to a subnet broadcast ping sent from a remote subnet. The default is disabled.

Configuring the forwarding database timeout globally

Configure the forwarding database global timeout to age out dynamically learned forwarding information.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**
2. Click **VLANs**.
3. Click the **FdbAging** tab.
4. Type an interval, in seconds, for aging out dynamically learned forwarding information, or keep the default.
5. Click **Apply**.

FDB Aging field descriptions

Use the data in the following table to use the **FDB Aging** tab.

Name	Description
FdbAging	Specifies the timeout period for dynamically learned mac addresses on the vlan. The default valus is 300.

Viewing VLAN forwarding database information

Perform this procedure to view forwarding database entries for all VLANs on the device.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. In the VLANs tab, click the **Forwarding** tab.

Forwarding field descriptions

Use the data in the following table to use the **Forwarding** tab.

Name	Description
VlanId	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
Address	Specifies a unicast MAC address for which the VLAN has forwarding or filtering information.
Status	Specifies the status of the VLAN. The values are: • other • invalid • learned • self • mgmt
Port	Specifies either a value of zero (0) or the port number of the port on which a frame having the specified MAC address was seen. A value of **cpp** indicates a self-assigned MAC address.
BMac	Shows the backbone MAC address if the entry is learned from a Shortest Path Bridging MAC (SPBM) network.

Viewing the forwarding database for a specific VLAN

Use the forwarding database for VLANs to determine how the system forwards a received frame.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**
2. Click **VLANs**.

3. Select a VLAN.
4. Click **Bridge**.
5. Click the **Forwarding** tab and the VLAN forwarding database information is displayed.

Forwarding field descriptions

Use the data in the following table to use the **Forwarding** tab.

Name	Description
VlanId	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
Address	Specifies a unicast MAC address for which the bridge has forwarding or filtering information.
Status	Specifies the status. Values include: • self—one of the bridge addresses • learned—a learned entry that is being used • mgmt—a static entry
Port	Specifies either a value of zero (0) or the port number of the port on which a frame having the specified MAC address was seen. A value of **cpp** indicates a self-assigned MAC address.

Clearing learned MAC addresses by VLAN

Use the clear learned MAC addresses feature to flush the bridge forwarding database.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. Click the **Advanced** tab.
4. Double-click in the **VLAN Operation Action** field.
5. Choose **FlushMacFdb** from the list.
6. Click **Apply**.

Clearing learned MAC addresses for all VLANs by port

Use the following procedure to clear all the forwarding database (FDB) for VLANs associated with this port.

Procedure

1. In the Device Physical View tab, select a port.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. In the Interface tab **Action** box, select **FlushMacFdb**.
5. Click **Apply**.

   All learned MAC addresses are cleared from the forwarding database (FDB) for VLANs associated with this port.
6. Click **Close**.

Configuring static forwarding

Configure static forwarding to specify the group of ports that are allowed to forward frames.

Important:

Entries are valid for unicast and for group/broadcast addresses.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. Select the **Basic** tab.
4. Select a VLAN.
5. Click **Bridge**.
6. In the Bridge, VLAN tab, click the **Static** tab.
7. Click **Insert**.
8. In the **MacAddress** box, enter a forwarding destination MAC address.
9. In the **Port** box, click the ellipsis button **(...)**.
10. Select the port on which the frame is received.
11. Click **Ok**.
12. Click **Insert**.

Static field descriptions

Use the data in the following table to use the **Static** tab.

Name	Description
MacAddress	Specifies the destination MAC address in a frame to which the forwarding information for this entry applies. This object can take the value of a unicast address.
Port	Specifies the port number of the port on which the frame is received.
VlanId	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
Status	Specifies the status of the VLAN.

Chapter 6: Spanning tree fundamentals

This section describes the spanning tree features supported on the switch.

The switch supports Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).

Spanning tree

Spanning Tree protocols detect and eliminate logical loops in a bridged or switched network. If multiple paths exist, the spanning tree algorithm configures the network so that a bridge or device uses the root bridge path based on hop counts. Although link speed is taken into account, the path is based on the root bridge rather than on an optimized path. If that path fails, the protocol automatically reconfigures the network and makes another path active, thereby sustaining network operations. The switch supports RSTP and MSTP but can downgrade a port automatically if it receives an STP Bridge Protocol Data Unit (BPDU) from a switch that runs STP.

Note:

Spanning tree is disabled on all Switched UNI (S-UNI) ports. The ports will move into forwarding state as soon as the physical port or VLACP or LACP comes up on the port. If the platform VLAN is associated to the S-UNI Service Instance Identifier (I-SID), then the S-UNI ports added to the platform VLAN will become the member of MSTP instances associated with the platform VLAN. To enable SLPP on the S-UNI ports, the platform VLAN must be associated with the S-UNI I-SID.

Spanning Tree Groups

Spanning Tree Groups (STGs) represent logical topologies. A topology is created based on bridge configuration values such as root bridge priority. In the case of multiple STGs, you can map a VLAN to the most appropriate logical topology in the physical network.

The switch supports spanning-tree modes RSTP and MSTP. The default spanning-tree mode is MSTP. The default STG is 0. In RSTP mode, all VLANs run in the default STG. In MSTP mode, you can create additional STGs by using the VLAN create command. The switch supports up to 64 STGs.

Although STP and MSTP are variations of the same spanning tree protocol, they communicate information differently. A switch in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with Avaya STP. MSTP spanning tree groups are not the same as Avaya STP spanning tree groups. Using a switch in MSTP mode with a chassis in STP mode can create a loop in the network.

The root bridge for Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) is determined by comparing attributes of each bridge in the network.

The protocol considers bridge priority first. If more than one bridge has the same priority, then the protocol must consider the bridge ID. The bridge with the lowest ID becomes the root bridge. For

MSTP, this bridge is called the Common and Internal Spanning Tree (CIST) Root because it is the root of the entire physical network.

In MSTP mode, you can create additional Spanning Tree instances, by using the VLAN command. These instances, known as Multiple Spanning Tree Instances (MSTIs), can assign different priorities to switches. The MSTIs have different link costs or port priorities and as a result create separate logical topologies.

MSTP also allows the creation of MSTP regions. A region is a collection of switches sharing the same view of physical and logical topologies. For switches to belong to the same region, the following attributes must match:

- MSTP configuration ID selector
- MSTP configuration name
- MSTP configuration revision number
- VLAN instance mapping

Links connecting sections are called boundary ports. In a region, the boundary switch that contains the boundary port providing the shortest external path cost to the CIST Root is the CIST Regional Root.

STGs and VLANs

When you map VLANs to STGs, be aware that all links on the bridge belong to all STGs. Because each Spanning Tree group can differ in its decision to make a link forwarding or blocking, you must ensure that the ports you add to a VLAN are in the expected state.

Untagged ports can only belong to one VLAN and therefore can only belong to one STG. Tagged ports can belong to multiple VLANs and therefore to multiple STGs.

BPDU handling on S-UNI port/MLT

The switch handles Bridge Protocol Data Units (BPDUs) according to whether or not you configure a platform VLAN.

- When you configure a platform VLAN:
  - BPDUs are forwarded to the CPU by default.
  - BPDUs are not flooded in the S-UNI I-SID associated with the platform VLAN.

  Note:

  If the platform VLAN is configured for the S-UNI port, you cannot enable BDPU forwarding.
- When you DO NOT configure a platform VLAN:
  - BPDUs received on untagged-traffic ports are dropped by default.
  - To flood BPDUs in its I-SID, enable BPDU forwarding under S-UNI I-SID using the command **`untagged-traffic port <port no> bpdu enable`**.

Rapid Spanning Tree Protocol and Multiple Spanning Tree Protocol

The Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. It also maintains backward compatibility with IEEE 802.1d (the spanning tree implementation prior to RSTP). In certain configurations, the recovery time of RSTP can be reduced to less than 1 second. RSTP also reduces the amount of flooding in the network by enhancing the way Topology Change Notification (TCN) packets are generated.

With Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s), you can configure multiple instances or Spanning Tree groups on the same device. Each instance or Spanning Tree group can include one or more VLANs.

By using RSTP and MSTP, the switch achieves the following:

- reduces convergence time after a topology change (from 30 seconds to less than 1 or 2 seconds)
- eliminates unnecessary flushing of the MAC database and the flooding of traffic to the network
- creates backward compatibility with classic 802.1d switches
- creates support for 64 instances of spanning tree in MSTP mode

The following sections relate to RSTP and MSTP:

- RSTP interoperability with STP on page 84
- Differences in port roles for STP and RSTP on page 85
- Port roles: root forwarding role on page 85
- Port roles: designated forwarding role on page 85
- Port roles: alternate blocking role on page 86
- Edge port on page 86
- Path cost values on page 86
- RSTP negotiation process on page 86

RSTP interoperability with STP

RSTP provides a parameter called ForceVersion to provide backward compatibility with standard STP. A user can configure a port in either STP-compatible mode or RSTP mode:

- An STP-compatible port transmits and receives only STP Bridge Protocol Data Units (BPDUs). An RSTP BPDU that the port receives in this mode is discarded.
- An RSTP-compatible port transmits and receives only RSTP BPDUs. If an RSTP port receives an STP BPDU, it becomes an STP port. User intervention is required to change this port back to RSTP mode. This process is called Port Protocol Migration.

Note:

You must configure protocol migration to true on all spanning-tree enabled interfaces when you change the spanning tree version from STP-compatible to MSTP for those interfaces to work in the proper mode.

Differences in port roles for STP and RSTP

RSTP is an enhanced version of STP. These two protocols have almost the same parameters.

The following table lists the differences in port roles for STP and RSTP. STP supports two port roles, while RSTP supports four port roles.

Table 24: Differences in port roles for STP and RSTP

Port Role	STP	RSTP	Description
Root	Yes	Yes	This port receives a better BPDU than its own and has the best path to reach the Root. The root port is in Forwarding state. The root port and designated ports can be in the Discarding state before they go to root forwarding.
Designated	Yes	Yes	This port has the best BPDU on the segment. The designated port is in the Forwarding state.
Alternate	No	Yes	This port receives a better BPDU than its own BPDU, and a root port exists within the same device. The alternate port is in the Discarding state.
Backup	No	Yes	This port receives a better BPDU than its own BPDU, and this BPDU is from another port within the same device. The backup port is in the Discarding state.

Port roles: root forwarding role

MSTP and RSTP root forwarding roles are as follows:

- The port that receives the best path BPDU on a device is the root port, and is referred to as a Root Forwarding (RF) port. This is the port that is the closest to the root bridge in terms of path cost.
- The spanning tree algorithm elects a single root bridge in a bridged network. With MSTP, a root bridge is selected for the Common and Internal Spanning Tree (CIST). A root bridge is selected for the region, and a root bridge is selected for each spanning tree instance.
- The root bridge is the only bridge in a network that does not have root ports; all ports on a root bridge are Designated Forwarding (DF).
- Only one path towards a root bridge can exist on a given segment; otherwise, loops can occur.

Port roles: designated forwarding role

MSTP and RSTP designated forwarding roles are as follows:

- All bridges connected on a segment monitor the BPDUs of all other bridges. The bridge that sends the best BPDU is the root bridge for the segment.
- The corresponding port on the bridge is referred to as a Designated Forwarding Port.

Port roles: alternate blocking role

MSTP and RSTP alternate blocking roles are as follows:

- A blocked port is defined as not being the designated or root port. An alternate port provides an alternate path to the root and can replace the root port if it fails.
- An alternate blocked port is a port that is blocked because it received better path cost BPDUs from another bridge.

Port roles: backup blocking role

MSTP and RSTP backup blocking roles are as follows:

- A backup port receives the more useful BPDUs from the bridge on which the port exists.

Edge port

RSTP uses a parameter called the edge port. After a port connects to a nonswitch device, such as a PC or a workstation, it must be configured as an edge port. An active edge port enters the forwarding state without delay. An edge port becomes a nonedge port if it receives a BPDU.

Path cost values

RSTP and MSTP recommend new path cost values that support a wide range of link speeds. The following table lists the recommended path cost values.

Table 25: Recommended path cost values

Link speed	Recommended value
Less than or equal to 100 Kb/s	200 000 000
1 Mb/s	20 000 000
10 Mb/s	2 000 000
100 Mb/s	200 000
1 Gb/s	20 000
10 Gb/s	2000
100 Gb/s	200
1 Tb/s	20
10 Tb/s	2

RSTP negotiation process

The following section describes the negotiation process between switches that takes place before PCs can exchange data (see the following figure).

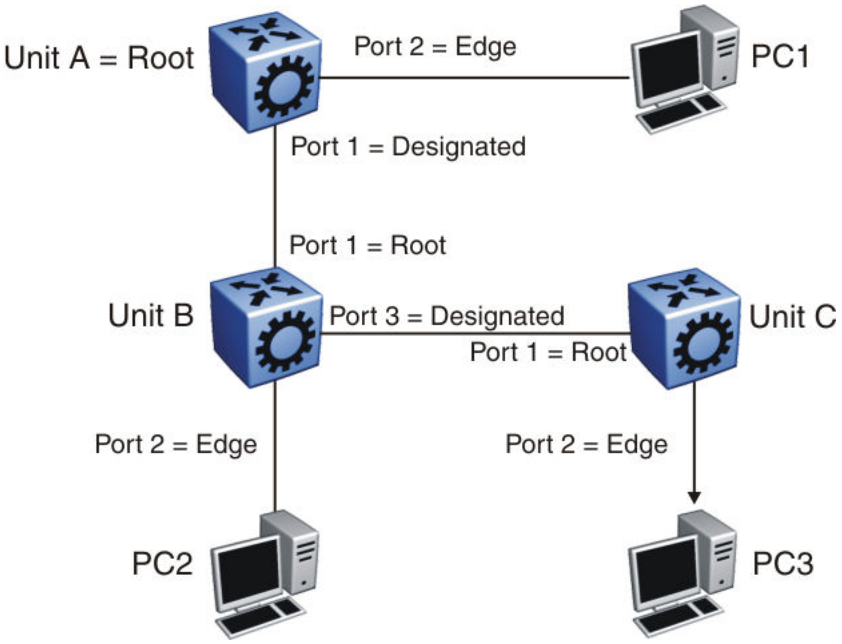


Figure 7: RSTP negotiation process

After turning on, all ports assume the role of designated ports. All ports are in the discarding state except edge ports. Edge ports go directly into the forwarding state without delay.

Unit A port 1 and Unit B port 1 exchange BPDUs. Unit A knows that it is the root and that Unit A port 1 is the designated port. Unit B learns that Unit A has higher priority. Unit B port 1 becomes the root port. Both Unit A port 1 and Unit B port 1 are still in the discarding state.

Unit A starts the negotiation process by sending a BPDU with the proposal bit set.

Unit B receives the proposal BPDU and configures its nonedge ports to discarding state. This operation occurs during the synchronization process.

Unit B sends a BPDU to Unit A with the agreement bit set.

Unit A configures port 1 to the forwarding state, and Unit B configures port 1 to the forwarding state. PC 1 and PC 2 can now communicate. The negotiation process now moves on to Unit B port 3 and its partner port. PC 3 cannot exchange data with either PC 1 or PC 2 until the negotiation process between Unit B and Unit C finishes.

The RSTP convergence time depends on how quickly the switch can exchange BPDUs during the negotiation process, and on the number of switches in the network.

Chapter 7: Spanning Tree configuration using ACLI

This chapter describes how to configure the Spanning Tree mode, MSTP, and RSTP using Avaya Command Line Interface (ACLI) commands.

Important:

> The switch supports up to 64 STGs on a device, however, SPBM uses STG 63 and MSTI 62 for internal use. STG 63 or MTSI 62 cannot be used by other VLANs or MSTIs.

Configuring Spanning Tree

Configure the STP mode to configure the spanning tree mode on the device.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Configure the STP mode:

   `boot config flags spanning-tree-mode {rstp|mstp}`

Example

Configure the STP mode:

```
Switch:1(config)#boot config flags spanning-tree-mode mstp
Warning: Please save the configuration and reboot the switch
         for this to take effect.
Warning: Please carefully save your configuration files before
         starting configuring the switch in RSTP or MSTP mode.
```

Variable definitions

Use the data in the following table to use the `boot config flags spanning-tree-mode` command.

Table 26: Variable definitions

Variable	Value
rstp|mstp	Specifies the Spanning Tree modes: Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP).

Configuring Rapid Spanning Tree Protocol

Configure Rapid Spanning Tree Protocol (RSTP) to reduce the recovery time after a network breakdown.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Configure RSTP:

```
spanning-tree rstp [forward-time <400-3000>] [group-stp enable]
[hello-time <100-1000>] [max-age <600-4000>] [pathcost-type <bits16|
bits32>] [priority <0-61440>] [tx-holdcount <1-10>] [version <rstp|
stp-compatible>]
```

Example

Configure RSTP:

```
Switch:1(config)# spanning-tree rstp forward-time 1000 hello-time 200 max-
age 4000 pathcost-type bits16 priority 4096 tx-holdcount 10 version rstp
group-stp enable
```

Variable definitions

Use the data in the following table to use the `spanning-tree rstp` command.

Table 27: Variable definitions

Variable	Value
forward-time <400-3000>	Configures the RSTP forward delay for the bridge in hundredths of a second.
group-stp enable	Enables or disables RSTP for a specific STG. Enter the no form of the command to disable RSTP for the

Table continues…

Variable	Value
	STG (`no spanning-tree rstp group-stp enable`).
hello-time <100-1000>	Assigns the RSTP hello time delay for the bridge in hundredths of a second.
max-age <600-4000>	Assigns the RSTP maximum age time for the bridge in hundredths of a second.
pathcost-type {bits16|bits32}	Assigns the RSTP default pathcost version. The default is 32 bits.
priority <0-61440>	Assigns the RSTP bridge priority.
tx-holdcount <1-10>	Assigns the RSTP transmit hold count from 1 to 10. The default value is 6.
version {rstp/stp-compatible}	Sets the version to RSTP or STP compatible.

Configuring Rapid Spanning Tree Protocol for a port

Configure RSTP to reduce the recovery time after a network breakdown.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   
   configure terminal
   
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform 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.

2. Configure RSTP:

   ```
   spanning-tree rstp cost <1-200000000> edge-port <false|true> p2p
   <auto|force-false|force-true> priority <0-240> protocol-migration
   <false|true> stp enable
   ```

Example

Configure RSTP:

```
Switch:1(config-if)#spanning-tree rstp cost 100 edge-port true p2p auto
priority 32 protocol-migration true stp enable
```

Variable definitions

Use the data in the following table to use the `spanning-tree rstp` command.

Table 28: Variable definitions

Variable	Value
cost *<1–200000000>*	Specifies the contribution of this port to the path cost.
edge-port <false|true>	Configures the edge-port value for the port. A value of true indicates that this port is an edge-port, and a value of false indicates that this port is a nonedge-port.
p2p <auto|force-false|force-true>	Specifies the point-to-point status of the LAN segment attached to this port. A value of force-true indicates that this port is treated as if it connects to a point-to-point link. A value of force-false indicates that this port is treated as having a shared media connection. A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotation or by management means.
priority *<0-240>*	Assigns the RSTP bridge priority in a range of 0–240. The value has to increment in steps of 16.
protocol-migration <false|true>	If you chose true, the option initiates protocol migration for a port. If you chose false, the option terminates protocol migration for a port. An RSTP-compatible port transmits and receives only RSTP BPDUs. If an RSTP port receives an STP BPDU, it becomes an STP port. User intervention is required to change this port back to RSTP mode. This process is called Port Protocol Migration.
stp enable	Configures STP for the port.

Configuring the Rapid Spanning Tree Protocol version

Perform this procedure to specify the RSTP mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Configure Rapid Spanning Tree Protocol version:

   ```
   spanning-tree rstp version {rstp|stp-compatible}
   ```

Example

Configure Rapid Spanning Tree Protocol version:

```
Switch:1(config)# spanning-tree rstp version rstp
```

Variable definitions

Use the data in the following table to use the `spanning-tree rstp version` command.

Table 29: Variable definitions

Variable	Value
rstp version *{rstp|stp-compatible}*	Sets the version to RSTP or to STP compatible. The default is RSTP.

Viewing the global RSTP configuration information

View the global RSTP configuration information to display the Rapid Spanning Tree Protocol (RSTP) configuration details.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View global RSTP configuration information:

   ```
   show spanning-tree rstp config
   ```

Example

View global RSTP configuration information:

```
Switch:1> show spanning-tree rstp config
```

```
==============================================================
                 RSTP Configuration
==============================================================
Rstp Module Status             : Enabled
Priority                       : 32768 (0x8000)
Stp Version                    : rstp Mode
Bridge Max Age                 : 20 seconds
Bridge Hello Time              : 2 seconds
Bridge Forward Delay Time      : 15 seconds
Tx Hold Count                  : 6
PathCost Default Type          : 32-bit
```

Viewing RSTP statistics

Perform this procedure to view RSTP statistics.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RSTP statistics:

   `show spanning-tree rstp statistics`

Example

View RSTP statistics:

```
Switch:1> show spanning-tree rstp statistics
```

```
=====================================================================
                      RSTP Statistics
=====================================================================
Rstp UP Count                  : 1
Rstp Down Count                : 0
Count of Root Bridge Changes   : 0
Stp Time since Topology change: 0 day(s), 00H:00M:00S
Total No. of topology changes : 0
```

Viewing the RSTP status

View the RSTP status to display the RSTP related status information for the selected bridge.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View the RSTP status:

   `show spanning-tree rstp status`

Example

View the RSTP status:

```
Switch:1> show spanning-tree rstp status
```

```
===================================================================
                     RSTP Status Information
===================================================================
Designated Root                 : 80:00:00:24:7f:9f:60:00
Stp Root Cost                   : 0
Stp Root Port                   : cpp
Stp Max Age                     : 20 seconds
Stp Hello Time                  : 2 seconds
Stp Forward Delay Time          : 15 seconds
```

Viewing the RSTP configuration information

View the RSTP configuration information to display the RSTP-related port level configuration details.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View RSTP configuration information:

   `show spanning-tree rstp port config {slot/port[/sub-port][-slot/port[/sub-port]][,...]}`

Example

View RSTP configuration information:

```
Switch:1> show spanning-tree rstp port config 1/1
```

```
========================================================================
                      RSTP Port Configurations
========================================================================
Port Number                  : 1/1
Port Priority                : 128 (0x80)
Port PathCost                : 200000000
Port Protocol Migration      : False
Port Admin Edge Status       : False
Port Oper Edge Status        : False
Port Admin P2P Status        : Auto
Port Oper  P2P Status        : False
Port Oper  Protocol Version : Rstp
```

Variable definitions

Use the data in the following table to use optional parameters with the `show spanning-tree rstp port config` command.

Table 30: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform 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.

Viewing the RSTP status for a port

View the RSTP status for a port to display the RSTP-related status information for a selected port.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View the RSTP status for a port:

   `show spanning-tree rstp port status {slot/port[/sub-port][-slot/port[/sub-port]][,...]}`

Example

View the RSTP status for a port:

```
Switch:1> show spanning-tree rstp port status 1/2
==============================================================================
                             RSTP Port Status
                          (Port Priority Vector)
==============================================================================
Port Number                       : 1/2
Port Designated Root              : 80:00:00:24:7f:9f:60:00
Port Designated Cost              : 0
Port Designated Bridge            : 80:00:00:24:7f:9f:60:00
Port Designated Port              : 80:c1
```

Variable definitions

Use the data in the following table to use optional parameters with the `show spanning-tree rstp port status` command.

Table 31: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform 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.

Viewing RSTP information for a selected port

View the RSTP information for a selected port to display the RSTP-related configuration information for the selected port.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. View the RSTP information for a selected port:

   `show spanning-tree rstp port statistics [slot/port[-slot/port][,...]]`

Example

View the RSTP information for a selected port:

```
Switch:1# show spanning-tree rstp port statistics 1/4
========================================================================
                       RSTP Port Statistics
========================================================================
Port Number                          : 1/4
Number of Fwd Transitions            : 0
Rx RST BPDUs Count                   : 0
Rx Config BPDU Count                 : 0
Rx TCN BPDU Count                    : 0
Tx RST BPDUs Count                   : 9
Tx Config BPDU Count                 : 0
Tx TCN BPDU Count                    : 0
Invalid RST BPDUs Rx Count           : 0
Invalid Config BPDU Rx Count         : 0
Invalid TCN BPDU Rx Count            : 0
Protocol Migration Count             : 0
```

Variable definitions

Use the data in the following table to use optional parameters with the `show spanning-tree rstp port statistics` command.

Table 32: Variable definitions

Variable	Value
[slot/port[-slot/port][,...]]	Specifies the port or list of ports.

Viewing the RSTP role

View the RSTP role to display the RSTP information.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View the RSTP role:

```
show spanning-tree rstp port role [slot/port[-slot/port][,...]]
```

Example

View the RSTP role:

```
Switch:1> show spanning-tree rstp port role 1/3
```

```
==============================================================================
                          RSTP Port Roles and States
==============================================================================
Port-Index  Port-Role    Port-State   PortSTPStatus  PortOperStatus
------------------------------------------------------------------------------
1/3        Designated   Forwarding   Enabled        Enabled
```

Variable definitions

Use the data in the following table to use optional parameters with the `show spanning-tree rstp port role` command.

Table 33: Variable definitions

Variable	Value
[slot/port[-slot/port][,...]]	Specifies the port or list of ports

Viewing spanning tree configuration

Perform this procedure to view configuration and status information for spanning tree in your network.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View spanning tree configuration information:

   ```
   show spanning-tree config
   ```

3. View spanning tree status information:

   ```
   show spanning-tree status
   ```

Example

View spanning tree configuration information:

```
Switch:1> show spanning-tree config
```

```
==============================================================================
                             Spanning Tree Config
==============================================================================
              BRIDGE  BRIDGE     FORWARD
ID   PRIORITY MAX_AGE HELLO_TIME DELAY   STATE
```

```
--------------------------------------------------------------------------------
0    32768    20      0          15      Enabled
1    32768    20      0          15      Enabled

     TAGGBPDU                   PORT
ID   ADDRESS            TYPE    MEMBER
--------------------------------------------------------------------------------
0    01:80:c2:00:00:00  mstp   1/1-1/9,1/11-1/48
1    01:80:c2:00:00:00  mstp   1/10

Total number of Spanning Tree IDs :  2
```

View spanning tree status information:

```
Switch:1> show spanning-tree status
```

```
================================================================================
                              Spanning Tree Status
================================================================================
STG  BRIDGE            NUM   PROTOCOL      TOP
ID   ADDRESS           PORTS SPECIFICATION CHANGES
--------------------------------------------------------------------------------
0    00:24:7f:a1:70:00 47    ieee8021s     1
1    00:24:7f:a1:70:00 1     ieee8021s     1

STG  DESIGNATED              ROOT  ROOT  MAX  HELLO  HOLD  FORWARD
ID   ROOT                    COST  PORT  AGE  TIME   TIME  DELAY
--------------------------------------------------------------------------------
0    80:00:00:24:7f:a1:70:00 0     cpp   20   0      1     15
1    80:00:00:24:7f:a1:70:00 0     cpp   20   0      1     15

Total number of Spanning Tree IDs :  2
```

Configuring Multiple Spanning Tree Protocol

Use the following procedure to configure the Multiple Spanning Tree Protocol.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure MSTP:

   ```
   spanning-tree mstp
   ```

Example

Configure Multiple Spanning Tree Protocol to configure the MSTP configuration version.

```
Switch:1(config)# spanning-tree mstp forward-time 500 max-age 3000 max-hop
200 pathcost-type bits32 priority 8192 tx-holdcount 10 version mstp
```

Variable definitions

Use the data in the following table to use the `spanning-tree mstp` command.

Table 34: Variable definitions

Variable	Value
forward-time <400-3000>	Configures the MSTP forward delay for the bridge from 400 to 3000 hundredths of a second.
max-age <600-4000>	Assigns the MSTP maximum age time for the bridge from 600 to 4000 one hundredths of a second.
max-hop <100-4000>	Assigns the MSTP bridge maximum hop count. The range is 100 to 4000 one hundredths of a second. The original MIB erroneously designated the value in hundredths of a second, when it should have been in hops. The new MIB left the range at 100-4000 to stay backwards compatible. To convert this value to hops, divide by 100 so 100-4000 equals 1-40 hops.
msti <1-63> priority <0–65535>	Assigns the MSTP MSTI instance parameter.
pathcost-type {bits16|bits32}	Assigns the MSTP default pathcost type to either 16 bits or 32 bits. The default is 32 bits.
priority <0-61440>	Assigns the MSTP bridge priority in a range of 0 to 61440 in steps of 4096.
region [config-id-sel <0-255>] [region-name <WORD 1-32>] [region-version <0-65535>]	Assigns the MSTP region commands: • config-id-sel—Assigns the MSTP region configuration ID number. The range is 0 to 255. • region-name—Assigns the MSTP region name. The character string can be a range of 1 to 32 characters • region-version—Assigns the MSTP region version. The range is 0 to 65535.
tx-holdcount <1-10>	Assigns the MSTP transmit hold count. The range is 1 to 10.The default value is 3.
version {mstp|rstp|stp-compatible}	Assigns the bridge version. Although STP and MSTP are variations of the same spanning tree protocol, they communicate information differently. A switch in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with Avaya STP. MSTP spanning tree groups are not the same as Avaya STP spanning tree groups. Using a switch in MSTP mode with another chassis in STP mode can create a loop in the network.

Table continues…

Variable	Value
	You must configure protocol migration to true on all spanning-tree enabled interfaces when you change the spanning tree version from STP-compatible to MSTP for those interfaces to work in the proper mode.

Configuring MSTP MSTI options

Use the following procedure to configure MSTP multiple spanning tree instance (MSTI) options.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure MSTP MSTI:

   ```
   spanning-tree mstp msti <1-63> priority <0-65535>
   ```

Example

Configure MSTP MSTI:

```
Switch:1(config)#spanning-tree mstp msti 62 priority 4096
```

Variable definitions

Use the data in the following table to use the `spanning-tree mstp msti <1-63> priority <0–65535>` command.

Table 35: Variable definitions

Variable	Value
<1-63>	Specifies the instance ID.
<0–65535>	Specifies the priority value. Enter values in increments of 4096: • 4096 • 8192 • 12288 • 16384 • 20480 • 24576

Table continues…

Variable	Value
	- 28672 - 32768 - 36864 - 40960 - 45056 - 49152 - 53248 - 57344 - 61440

Configuring Ethernet MSTP

Configure Ethernet MSTP on a port to enable this feature.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform 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.

2. Configure Ethernet MSTP:

   ```
   spanning-tree mstp [cost <1-200000000>] [edge-port <false|true>]
   [force-port-state enable] [hello-time <100-1000>] [msti <1-63>] [p2p
   {auto|force-false|force-true}] [port {slot/port[/sub-port]}]
   [priority <0-240>] [protocol-migration <false|true>]
   ```

Example

Configure Ethernet MSTP:

```
Switch:1(config)#spanning-tree mstp cost 1 edge-port true force-port-
state enable hello-time 100 p2p auto priority 2 protocol-migration true
```

Variable definitions

Use the data in the following table to use the `spanning-tree mstp` command.

Table 36: Variable definitions

Variable	Value
cost *<1–200000000>*	Configures the path cost for a port. Valid values are 1 to 200000000
edge-port *<false*|*true>*	Enables or disables the port as an edge port.
force-port-state enable	Enables STP.
hello-time *<100–1000>*	Configures the hello-time for a port.
msti *<1–63>*	Configures the port MSTP MSTI.
p2p *{auto*|*force-false*|*force-true}*	Enables or disables point-to-point for a port.
{slot/port[/sub-port]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform 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.
priority *<0–240>*	Configures priority for the port.
protocol-migration *{false*|*true}*	If you chose true, the option initiates protocol migration for a port. If you chose false, the option terminates protocol migration for a port. An MSTP-compatible port transmits and receives only RSTP BPDUs. If an MSTP port receives an STP BPDU, it becomes an STP port. User intervention is required to change this port back to MSTP mode. This process is called Port Protocol Migration. You must configure protocol migration to true on all spanning-tree enabled interfaces when you change the spanning tree version from STP-compatible to MSTP for those interfaces to work in the proper mode.

Configuring Ethernet MSTP MSTI

Use the following procedure to configure the Ethernet MSTP MSTI parameters on a port.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
```

Note:

If your platform 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.

2. Configure Ethernet MSTP MSTI:

```
spanning-tree mstp msti <1-63> [cost <1-200000000>] [force-port-state enable] [port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}] [priority <0-240>]
```

Example

Configure Ethernet MSTP MSTI:

```
Switch(config-if)# spanning-tree mstp msti 62 priority 32
```

Variable definitions

Use the data in the following table to use the `spanning-tree mstp msti <1-63>` command.

Table 37: Variable definitions

Variable	Value
<1–63>	Specifies the instance ID.
cost <1–200000000>	Configures the path cost for the port
force-port-state enable	Enables MSTI learning for the port.
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform 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.
priority <0–240>	Configures the priority for the port. Enter the priority value (0–240) as increments of 16.

Viewing MSTP configurations

View the MSTP configurations to display the MSTP-related bridge-level VLAN and region information.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View the MSTP configurations:

   `show spanning-tree mstp config`

Example

View the MSTP configurations:

```
Switch:1> show spanning-tree mstp config
================================================================================
                              MSTP Configurations
================================================================================
Mstp Module Status            : Enabled
Number of Msti Supported      : 64
Cist Bridge Priority          : 32768 (0x8000)
Stp Version                   : Mstp Mode
Cist Bridge Max Age           : 20 seconds
Cist Bridge Forward Delay     : 15 seconds
Tx Hold Count                 : 3
PathCost Default Type         : 32-bit
Max Hop Count                 : 2000
Msti Config Id Selector       : 0
Msti Region Name              : 00:15:e8:9e:10:01
Msti Region Version           : 0
Msti Config Digest            : b2:96:8d:23:9d:73:39:e4:4f:bd:94:c2:14:d4:8d:09
```

Viewing MSTP status

View the MSTP status to display the MSTP-related status information known by the selected bridge.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View the MSTP status:

   `show spanning-tree mstp status`

Example

View the MSTP status:

```
Switch:1> show spanning-tree mstp status
========================================================================
                               MSTP Status
========================================================================
------------------------------------------------------------------------
```

```
Bridge Address                  : 00:15:e8:9e:10:01
Cist Root                       : 80:00:00:15:e8:9e:10:01
Cist Regional Root              : 80:00:00:15:e8:9e:10:01
Cist Root Port                  : cpp
Cist Root Cost                  : 0
Cist Regional Root Cost         : 0
Cist Instance Vlan Mapped       : 1-9,11-12,14-100,102-1024
Cist Instance Vlan Mapped2k     : 1025-2048
Cist Instance Vlan Mapped3k     : 2049-3072
Cist Instance Vlan Mapped4k     : 3073-3999,4001-4094
Cist Max Age                    : 20 seconds
Cist Forward Delay              : 15 seconds
```

Viewing MSTP port information

View the MSTP port information to display the MSTP, CIST port, and MSTI port information maintained by every port of the common spanning tree.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. View the MSTP port information:

   `show spanning-tree mstp port role [slot/port[/sub-port][-slot/port[/sub-port]][,...]]`

Example

View the MSTP port information:

```
Switch:1> show spanning-tree mstp port role 1/3
```

```
============================================================================
                           CIST Port Roles and States
============================================================================

Port-Index  Port-Role    Port-State   PortSTPStatus  PortOperStatus
----------------------------------------------------------------------------
1/3         Disabled    Discarding      Enabled        Disabled
```

Viewing MSTP MSTI information

View MSTP MSTI information to ensure the feature is configured correctly for your network.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Show MSTI information:

   `show spanning-tree mstp msti [config <1-63>] [port <config {slot/port[/sub-port][-slot/port[/sub-port]][,...]}|role {slot/port[/sub-`

```
port][-slot/port[/sub-port]][,...]}|statistics {slot/port[/sub-port]
[-slot/port[/sub-port]][,...]}]
```

Example

Show MSTI information:

```
Switch:1>show spanning-tree mstp msti config 62
```

```
============================================================================
                              MSTP Instance Status
============================================================================
Instance Id                         : 62
Msti Bridge Regional Root           : 80:00:00:15:e8:9e:10:01
Msti Bridge Priority                : 32768 (0x8000)
Msti Root Cost                      : 0
Msti Root Port                      : cpp
Msti Instance Vlan Mapped           :
Msti Instance Vlan Mapped2k         :
Msti Instance Vlan Mapped3k         :
Msti Instance Vlan Mapped4k         : 4000
```

```
Switch(config)#show spanning-tree mstp msti port statistics 1/1
```

```
================================================================================
                  MSTP Instance-specific Per-Port Statistics

================================================================================
Port Number                      : 1/1
Instance Id                      : 1
Msti Port Fwd Transitions        : 0
Msti Port  Received BPDUs        : 0
Msti Port Transmitted BPDUs      : 0
Msti Port Invalid BPDUs Rcvd     : 0
```

Variable definitions

Use the data in the following table to use the `show spanning-tree mstp msti` command.

Table 38: Variable definitions

Variable	Value
config *[<1-63>]*	Shows the configuration for one or all MSTP instance IDs.
port	Shows the configuration, role, or statistics information of a MSTP port. • config {slot/port[/sub-port][-slot/port[/sub-port]][,...]} • role {slot/port[/sub-port][-slot/port[/sub-port]][,...]} • statistics {slot/port[/sub-port][-slot/port[/sub-port]][,...]}

Viewing MSTP statistics

View MSTP MSTI information to ensure the feature is configured correctly for your network.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Show MSTP statistics:

   `show spanning-tree mstp statistics`

Example

Show MSTP statistics:

```
Switch:1>show spanning-tree mstp statistics
===========================================================================
                             MSTP Bridge Statistics
===========================================================================
Mstp UP Count                       : 1
Mstp Down Count                     : 0
Region Config Change Count          : 4
Time Since Topology Change          : 0 seconds
Topology Change Count               : 0
New Root Bridge Count               : 1
```

Chapter 8: Spanning Tree configuration using EDM

This chapter describes how to create, manage, and monitor spanning tree groups (STG). It also describes how to configure the Rapid Spanning Tree Protocol (RSTP) and the Multiple Spanning Tree Protocol (MSTP) using Enterprise Device Manager (EDM).

Important:

The switch supports up to 64 STGs in a device, however, SPBM uses STG 63 and MSTI 62 for internal use. STG 63 or MTSI 62 cannot be used by other VLANs or MSTIs.

Configuring the Spanning Tree mode

Configure the Spanning Tree mode to change the mode to MSTP or RSTP mode.

Important:

After you change the mode, restart the system for the changes to take effect.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.
2. Click **Globals**.
3. Select the required spanning tree mode.
4. Click **Apply**.

   The system notifies you that the setting takes effect after you save the configuration and restart the server.

   Important:

   After the mode is changed, save the configuration file, and then restart the system for the changes to take effect.

Globals field descriptions

Use the data in the following table to use the **Globals** tab.

Name	Description
SpanningTreeAdminMode	Configures the spanning tree mode as either RSTP or MSTP. The default is MSTP.
SpanningTreeOperMode	Specifies the current mode of the spanning tree.

Restarting the switch

Restart the switch so that changes to the bootconfig parameters (or other parameters) take effect. For example, you must restart the device to enable a change to the Spanning Tree mode.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. In the System tab, locate the **ActionGroup1** box.
4. Select **saveRuntimeConfig** .
5. Click **Apply**.
6. In the **ActionGroup4** box, select **softReset** .
7. Click **Apply**.

Configuring RSTP global parameters

Perform this procedure to configure the RSTP global parameters.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.
2. Click **RSTP**.
3. Configure the parameters as required.
4. Click **Apply**.

Globals field descriptions

Use the data in the following table to use the **Globals** tab.

Name	Description
PathCostDefault	Specifies the version of the spanning tree default path costs that are used by this bridge. A value of 8021d1998 indicates the use of the 16-bit default path costs from IEEE Std. 802.1d-1998. A value of stp8021t2001 indicates the use of the 32-bit default path costs from IEEE Std. 802.1t.
TxHoldCount	Specifies the value used by the port transmit state machine to limit the maximum transmission rate. The default is 3.
Version	Specifies the version of STP that the bridge currently runs. The value stpCompatible indicates that the Spanning Tree Protocol as specified in IEEE 802.1d is in use; rstp indicates that the Rapid Spanning Tree Protocol as specified in IEEE 802.1w is in use.
EnableStp	Indicates whether the spanning tree protocol is active in this STG. The default is enabled.
BridgeMaxAge	Specifies the value that all bridges use for MaxAge while this bridge acts as the root.
BridgeHelloTime	The value that all bridges use for HelloTime while this bridge acts as the root.
BridgeForwardDelay	Specifies the value that all bridges use for forward delay while this bridge acts as the root.
DesignatedRoot	Specifies the unique bridge identifier of the bridge recorded as the root in the configuration BPDUs transmitted by the designated bridge for the segment to which the port is attached.
RootCost	Specifies the cost of the path to the root from this bridge.
RootPort	Specifies the port number of the port which offers the lowest cost path from this bridge to the root bridge.
MaxAge	Specifies the maximum age of Spanning Tree Protocol information in hundredths of a second learned from the network on any port before the port is discarded.
HelloTime	Specifies the amount of time in hundredths of a second between the transmission of configuration bridge PDUs by this node on any port while it is the

Table continues…

Name	Description
	root of the spanning tree (or trying to become the root).
ForwardDelay	Specifies a time value, measured in hundredths of a second, controls how fast a port changes its spanning state after moving towards the forwarding state. The 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 after a topology change is detected, and is underway, to age all dynamic entries in the forwarding database.
RstpUpCount	Specifies the number of times the RSTP module is enabled. A trap is generated on the occurrence of this event.
RstpDownCount	Specifies the number of times the RSTP module is disabled. A trap is generated on the occurrence of this event.
NewRootIdCount	Specifies the number of times this bridge detects a root identifier change. A trap is generated on the occurrence of this event.
TimeSinceTopology Change	Specifies the time (in hundredths of a second) since the TcWhile Timer for any port in this bridge was nonzero for Common Spanning Tree.
TopChanges	Specifies the number of times that there was at least one nonzero TcWhile Timer on this bridge for Common Spanning Tree.

Configuring RSTP ports

Configure RSTP to reduce the recovery time after a network breakdown.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.
2. Click **RSTP**.
3. Click the **RSTP Ports** tab.
4. Use the fields in the **RSTP Ports** tab to configure the RSTP ports.
5. Click **Apply**.

RSTP Ports field descriptions

Use the data in the following table to use the **RSTP Ports** tab.

Name	Description
Port	Specifies a unique value, greater than zero, indicating the port number.
Priority	Specifies the value of the priority field.
PathCost	Specifies the contribution of this port to the path cost of paths towards the root that includes this port.
ProtocolMigration	Specifies a port to transmit RSTP BPDUs if operating in RSTP mode. Any other operation on this object has no effect, and RSTP mode returns false if read.
AdminEdgePort	Specifies the administrative value of the Edge Port parameter. A value of true indicates that this port is an edge-port, and a value of false indicates that this port is a nonedge-port.
OperEdgePort	Specifies the operational value of the Edge Port parameter. The object is initialized to the value of AdminEdgePort and is configured to false on reception of a BPDU.
AdminPointToPoint	Specifies the administrative point-to-point status of the LAN segment attached to this port. A value of forceTrue indicates that this port is treated as if it is connected to a point-to-point link. A value of forceFalse indicates that this port is treated as having a shared media connection. A value of auto indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotiation or by management means.
OperPointToPoint	Specifies the operational point-to-point status of the LAN segment attached to this port. It indicates whether a port is considered to have a point-to-point connection or not. The value is determined by management or by autodetection as described in the AdminPointToPoint object.
OperVersion	Indicates if the port is in MSTP mode, RSTP mode or STP-compatible mode. MSTP mode transmits MST BDUs, RSTP mode transmits RST BPDUs and STP-compatible transmits Config/TCN BPDUs.

Viewing RSTP port status

View the RSTP port status to ensure proper functioning of RSTP.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.
2. Click **RSTP**.
3. In the RSTP tab, click the **RSTP Status** tab.

RSTP Status field descriptions

Use the data in the following table to use the **RSTP Status** tab.

Name	Description
Port	Specifies a unique value, greater than zero, indicating the port number.
State	Specifies the current state of the port as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame.
Role	Indicates the current port role assumed by this port.
OperVersion	Indicates whether the port is operationally in the RSTP- or STP-compatible mode; that is, whether the port transmits RSTP BPDUs or Config/TCN BPDUs.
EffectivePortState	Specifies the effective operational state of the port. This object is configured to true if the port is operationally up in the Interface Manager, and if Force Port State for this port and the specified port state is enabled. Otherwise, this object is configured to false.

Configuring MSTP global parameters

Configure the global MSTP parameters to determine how MSTP operates for the system. Interface-level parameters override global settings.

Before you begin

- The system must be in MSTP mode.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.
2. Click **MSTP**.
3. Click the **Globals** tab.
4. Configure MSTP as required.
5. Click **Apply**.

Globals field descriptions

Use the data in the following table to use the **Globals** tab.

Name	Description
PathCostDefaultType	Specifies the version of the spanning tree default path costs to be used by this bridge. A value of 8021d1998 denotes the use of the 16-bit default path costs from IEEE 802.1d-1998. A value of stp8021t2001 denotes the use of the 32-bit default path costs from IEEE 802.1t.
TxHoldCount	Specifies the value used by the port transmit state to limit the maximum transmission rate. The default is 3.
MaxHopCount	Assigns the MSTP bridge maximum hop count. The range is 100 to 4000 one hundredths of a second. The original MIB erroneously designated the value in hundredths of a second, when it should have been in hops. The new MIB left the range at 100-4000 to stay backwards compatible. To convert this value to hops, divide by 100 so 100-4000 equals 1-40 hops.
NoOfInstancesSupported	Indicates the maximum number of spanning tree instances supported.
MstpUpCount	The number of times the MSTP module is enabled. A trap is generated on the occurrence of this event.
MstpDownCount	The number of times the MSTP module is disabled. A trap is generated on the occurrence of this event.
ForceProtocolVersion	Specifies the version of Spanning Tree Protocol that the bridge currently runs. stpCompatible indicates that the Spanning Tree Protocol as specified in IEEE 802.1d is in use; rstp indicates that the Rapid Spanning Tree Protocol as specified in IEEE 802.1w is in use; and mstp indicates that the multiple

Table continues…

Name	Description
	spanning tree protocol as specified in IEEE 802.1s is in use. Although STP and MSTP are variations of the same spanning tree protocol, they communicate information differently. A switch in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with Avaya STP. MSTP spanning tree groups are not the same as Avaya STP spanning tree groups. Using a switch in MSTP mode with a chassis in STP mode can create a loop in the network. The default is MSTP.
BrgAddress	Specifies the MAC address used by this bridge if it must be referred to in a unique fashion. Avaya recommends that this is the numerically smallest MAC address of all ports that belong to this bridge. If concatenated with MstCistBridgePriority or MstBridgePriority, a unique bridge identifier is formed, which is used in the STP.
Root	Specifies the bridge identifier of the root of the common spanning tree as determined by the STP by this node. This value is used as the CIST root identifier parameter in all configuration bridge PDUs originated by this node.
RegionalRoot	Specifies the bridge identifier of the root of the multiple spanning tree region as determined by the STP as executed of this node. This value is used as the common and internal spanning tree (CIST) regional root identifier parameter in all configuration bridge PDUs originated by this node.
RootCost	Specifies the cost of the path to the CIST root from this bridge.
RegionalRootCost	Specifies the cost of the path to the CIST regional root from this bridge.
RootPort	Specifies the port number of the port which offers the lowest path cost from this bridge to the CIST root bridge.
BridgePriority	Specifies the value of the writable portion of the bridge identifier comprising the first two octets. The values you enter for bridge priority must be in steps of 4096. The default is 32768.
BridgeMaxAge	Specifies the value that all bridges use for MaxAge while this bridge acts as the root. The granularity of this timer is specified as 1 second. An agent can

Table continues…

Name	Description
	return a bad value error if you attempt to configure a value which is not a whole number of seconds. The default is 2000.
BridgeForwardDelay	Specifies the value that all bridges use for forward delay if this bridge acts as the root. Note that 802.1d specifies that the range for this parameter is related to the value of BridgeMaxAge. The granularity of this timer is specified as 1 second. An agent can return a bad value error if you attempt to configure a value which is not a whole number of seconds. The default is 1500.
HoldTime	Determines the interval length in hundredths of a second during which no more than two configuration bridge PDUs can be transmitted by this node.
MaxAge	Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded. This is the value that this bridge currently uses.
ForwardDelay	Specifies the time value, measured in units of hundredths of a second, that controls how fast a port changes its spanning state after moving towards the forwarding state. This value determines how long the port stays in a particular state before moving to the next state.
TimeSinceTopology Change	Specifies the time (in hundredths of a second) since the TcWhile Timer for any port in this bridge was nonzero for Common Spanning Tree.
TopChanges	Specifies the number of times that there was at least one nonzero TcWhile Timer on this bridge for Common Spanning Tree.
NewRootBridgeCount	Specifies the number of times this bridge detects a root bridge change for Common Spanning Tree. A trap is generated on the occurrence of this event.
RegionName	Specifies the name for the region configuration. By default, the region name is equal to the bridge MAC Address.
RegionVersion	Specifies the version of the MST region.
ConfigIdSel	Specifies the configuration identifier format selector used by the bridge. This has a fixed value of 0 to indicate RegionName. RegionVersions are specified as in the standard.
ConfigDigest	Specifies the configured MD5 digest value for this region, which must be 16 octets long.

Table continues…

Name	Description
RegionConfigChange Count	Specifies the number of times a region configuration identifier change is detected. A trap is generated on the occurrence of this event.

Configuring CIST ports for MSTP

Configure Common and Internal Spanning Tree (CIST) ports to configure ports for MSTP.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.
2. Click **MSTP**.
3. Click the **CIST Port** tab.

   ❗ **Important:**

   The MSTP, CIST Port tab contains information for each port that is common to all bridge and spanning tree instances.
4. Use the fields in the **CIST Port** box to configure the MSTP CIST port.
5. Click **Apply**.

CIST Port field descriptions

Use the data in the following table to use the **CIST Port** tab.

Name	Description
Port	Specifies the port number of the port for which this entry contains spanning tree information.
PathCost	Specifies the contribution of this port to the path cost of paths towards the CIST root that includes this port.
Priority	Specifies the four most significant bits of the port identifier of the spanning tree instance which are modified by setting the CistPortPriority value. The values that are configured for port priority must be in steps of 16. Although port priority values can range from 0 to 255, only the following values are used: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. The default is 128.

Table continues…

Name	Description
DesignatedRoot	Specifies the unique bridge identifier of the bridge recorded as the CIST root in the configuration BPDUs transmitted.
DesignatedCost	Specifies the path cost of the designated port of the segment that connects to this port.
DesignatedBridge	Specifies the unique bridge identifier of the bridge which that port considers to be the designated bridge for the ports segment.
DesignatedPort	Specifies the port identifier of the port on the designated bridge for this port segment.
RegionalRoot	Specifies the unique bridge identifier of the bridge recorded as the CIST regional root identifier in the configuration BPDUs transmitted.
RegionalPathCost	Specifies the contribution of this port to the path cost of paths towards the CIST regional root that include this port.
ProtocolMigration	Indicates the protocol migration state of this port. If you chose true, the option initiates protocol migration for a port. If you chose false, the option terminates protocol migration for a port. An MSTP-compatible port transmits and receives only RSTP BPDUs. If an MSTP port receives an STP BPDU, it becomes an STP port. User intervention is required to change this port back to MSTP mode. This process is called Port Protocol Migration. You must configure protocol migration to true on all spanning-tree enabled interfaces when you change the spanning tree version from STP-compatible to MSTP for those interfaces to work in the proper mode.
AdminEdgeStatus	Specifies the administrative value of the Edge Port parameter. A value of true indicates that this port is an edge-port, and a value of false indicates that this port is a nonedge-port.
OperEdgeStatus	Specifies the operational value of the Edge Port parameter. The object is initialized to the value of AdminEdgeStatus and is configured to false on reception of a BPDU.
AdminP2P	Specifies the administrative point-to-point status of the LAN segment attached to this port. A value of forceTrue indicates that this port is treated as if it connects to a point-to-point link. A value of forceFalse indicates that this port is treated as having a shared media connection. A value of auto

Table continues…

Name	Description
	indicates that this port is considered to have a point-to-point link if it is an aggregator and all of its members are aggregatable, or if the MAC entity is configured for full-duplex operation, either through autonegotation or by management means.
OperP2P	Specifies the operational point-to-point status of the LAN segment attached to this port. It indicates whether a port is considered to have a point-to-point connection or not. The value is determined by management or by autodetection as described in the AdminP2P object.
HelloTime	Specifies the amount of time in hundredths of a second between the transmission of configuration bridge PDUs by this node on this port.
OperVersion	Indicates whether the port is operationally in the MSTP mode, the RSTP mode, or the STP-compatible mode; that is, whether the port transmits MST BPDUs, RST BPDUs, or Config/TCN BPDUs. Although STP and MSTP are variations of the same spanning tree protocol, they communicate information differently. A switch in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with Avaya STP. MSTP spanning tree groups are not the same as Avaya STP spanning tree groups. Using a switch in MSTP mode with another chassis in STP mode can create a loop in the network.
EffectivePortState	Specifies the effective operational state of the port for CIST. This is true only if the port is operationally up at the interface and protocol levels for CIST. This is configured to false for all other conditions.
State	Specifies the current state of the port as defined by the common spanning tree protocol. It can be disabled, discarding, learning, or forwarding.
ForcePortState	Specifies the current state of the port. You can change the port to either Disabled or Enabled for the base spanning tree instance.
SelectedPortRole	Specifies the selected port role of the port for this spanning tree instance.
CurrentPortRole	Specifies the current port role of the port for this spanning tree instance.

Configuring MSTI bridges for MSTP

Perform this procedure to configure multiple spanning tree instance (MSTI) bridges for MSTP.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.
2. Click **MSTP**.
3. Click the **MSTI Bridges** tab.

   Important:

   The systems generates MSTI bridge instances after you create a VLAN in MSTP mode.
4. Use the fields in the **MSTI Bridges** box to configure the MSTP bridge.
5. Click **Apply**.

MSTI Bridges field descriptions

Use the data in the following table to use the **MSTI Bridges** tab.

Name	Description
Instance	Specifies the spanning tree instance to which this information belongs.
RegionalRoot	Specifies the MSTI regional root identifier value for the instance. This value is used as the MSTI regional root identifier parameter in all configuration bridge PDUs originated by this node.
Priority	Specifies the writable portion of the MSTI bridge identifier comprising the first two octets. The values that are configured for bridge priority must be in steps of 4096. The default is 32768.
RootCost	Specifies the cost of the path to the MSTI regional root as seen by this bridge.
RootPort	Specifies the port number of the port that offers the lowest path cost from this bridge to the MSTI region root bridge.
TimeSinceTopologyChange	Specifies the time (in hundredths of a second) since the TcWhile Timer for any port in this bridge was nonzero for this spanning tree instance.
TopChanges	Specifies the number of times that there was at least one nonzero TcWhile Timer on this bridge for this spanning tree instance.

Table continues…

Name	Description
NewRootCount	Specifies the number of times this bridge detects a root bridge change for this spanning tree instance. A trap is generated on the occurrence of this event.
InstanceUpCount	Specifies the number of times a new spanning tree instance is created. A trap is generated on the occurrence of this event.
InstanceDownCount	Specifies the number of times a spanning tree instance is deleted. A trap is generated on the occurrence of this event.

Configuring MSTI ports for MSTP

Perform the following procedure to configure MSTI ports for MSTP.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.
2. Click **MSTP**.
3. Click the **MSTI Port** tab.

   Important:

   Port members you select on the VLAN, **Basic** tab appear in the **MSTI Port** tab.
4. Use the fields in the **MSTI Port** box to configure the MSTP.
5. Click **Apply**.

MSTI Port field descriptions

Use the data in the following procedure to use the **MSTI Port** tab.

Name	Description
Port	Specifies the port number of the port for which this entry contains spanning tree information.
Instance	Specifies the spanning tree instance to which the information belongs.
PathCost	Specifies the contribution of this port to the path cost of paths towards the MSTI root that includes this port.

Table continues…

Name	Description
Priority	Specifies the four most significant bits of the port identifier for a given spanning tree instance can be modified independently for each spanning tree instance supported by the bridge. The values configured for port priority must be in steps of 16. The default is 128.
DesignatedRoot	Specifies the unique bridge identifier of the bridge recorded as the MSTI regional root in the configuration BPDUs transmitted.
DesignatedBridge	Specifies the unique bridge identifier of the bridge that this port considers to be the designated bridge for the port segment.
DesignatedPort	Specifies the port identifier of the port on the designated bridge for this port segment.
State	Specifies the current state of the port, as defined by the MSTP. A port which is in forwarding state in one instance can be in discarding (blocking) state in another instance.
ForcePortState	Specifies the current state of the port, that is changed to either disabled or enabled for the specific spanning tree instance.
DesignatedCost	Specifies the path cost of the designated port of the segment connected to this port.
CurrentPortRole	Specifies the current port role of the port for this spanning tree instance.
EffectivePortState	Specifies the effective operational state of the port for a specific instance. This is configured to true if the port is operationally up at the interface and protocol levels for the specific instance. This is configured to false at all other times.

Glossary

Avaya command line interface (ACLI)	A textual user interface. When you use ACLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.
Bridge Protocol Data Unit (BPDU)	A data frame used to exchange information among the bridges in local or wide area networks for network topology maintenance.
common and internal spanning tree (CIST)	The single spanning tree calculated by the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP) to ensure that all LANs in a bridged Local Area Network (LAN) are simply and fully connected.
common spanning tree (CST)	The single spanning tree calculated by STP, RSTP, and MSTP to connect multiple spanning tree (MST) regions.
Enterprise Device Manager (EDM)	A web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.
forwarding database (FDB)	A database that maps a port for every MAC address. If a packet is sent to a specific MAC address, the switch refers to the forwarding database for the corresponding port number and sends the data packet through that port.
Institute of Electrical and Electronics Engineers (IEEE)	An international professional society that issues standards and is a member of the American National Standards Institute, the International Standards Institute, and the International Standards Organization.
Internet Control Message Protocol (ICMP)	A collection of error conditions and control messages exchanged by IP modules in both hosts and gateways.
Layer 2	Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.
Local Area Network (LAN)	A data communications system that lies within a limited spatial area, uses a specific user group and topology, and can connect to a public switched telecommunications network (but is not one).

mask	A bit string that the device uses along with an IP address to indicate the number of leading bits in the address that correspond with the network part.
Media Access Control (MAC)	Arbitrates access to and from a shared medium.
MultiLink Trunking (MLT)	A method of link aggregation that uses multiple Ethernet trunks aggregated to provide a single logical trunk. A multilink trunk provides the combined bandwidth of multiple links and the physical layer protection against the failure of a single link.
multiple spanning tree bridge	A bridge that supports the common spanning tree (CST) and one or more multiple spanning tree instances (MSTI) and selectively maps frames classified in a VLAN to the CST or an MSTI.
multiple spanning tree configuration identifier	A name for the revision level and summary of a given allocation of VLANs to spanning trees.
multiple spanning tree configuration table	Allocates every possible VLAN to the CST or a specific MSTI.
multiple spanning tree instance (MSTI)	One of a number of spanning trees calculated by the Multiple Spanning Tree Protocol (MSTP) within an MST region, to provide a simple and fully connected active topology for frames that belong to a VLAN mapped to the MSTI.
Multiple Spanning Tree Protocol (MSTP)	Configures multiple instances of the Rapid Spanning Tree Protocol (RSTP) on the switch.
multiple spanning tree region	A set of LANs and MST bridges physically connected by ports on the MST bridges.
Point-to-Point Protocol (PPP)	Point-to-Point Protocol is a basic protocol at the data link layer that provides its own authentication protocols, with no authorization stage. PPP is often used to form a direct connection between two networking nodes.
port	A physical interface that transmits and receives data.
quality of service (QoS)	QoS features reserve resources in a congested network, allowing you to configure a higher priority for certain devices. For example, you can configure a higher priority for IP deskphones, which need a fixed bit rate and split the remaining bandwidth between data connections if calls in the network are more important than the file transfers.
Rapid Spanning Tree Protocol (RSTP)	Reduces the recovery time after a network breakdown. RSTP enhances switch-generated Topology Change Notification (TCN) packets to reduce network flooding.

Routing Information Protocol (RIP)	A distance vector protocol in the IP suite, used by IP network-layer protocol, that enables routers in the same AS to exchange routing information by means of periodic updates. You often use RIP as a very simple interior gateway protocol (IGP) within small networks.
Simple Loop Prevention Protocol (SLPP)	Simple Hello Protocol that prevents loops in a Layer 2 network (VLAN).
Simple Network Management Protocol (SNMP)	SNMP administratively monitors network performance through agents and management stations.
Source Service Access Point (SSAP)	A source service access point (SSAP) is the individual address for access into the upper layers of the network protocol stack. SSAP is an eight bit field address.
spanning tree	A simple, fully-connected active topology formed from the arbitrary physical topology of connected bridged Local Area Network components by relaying frames through selected bridge ports. The protocol parameters and states that are used and exchanged to facilitate the calculation of the active topology and to control the bridge relay function.
Spanning Tree Group (STG)	A collection of ports in one spanning-tree instance.
trunk	A logical group of ports that behaves like a single large port.
trunk port	A port that connects to the service provider network such as the MPLS environment.
virtual router forwarding (VRF)	Provides traffic isolation between customers operating over the same node. Each virtual router emulates the behavior of a dedicated hardware router by providing separate routing functionality, and the network treats each VRF as a separate physical router.