Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 9000

Release 4.1
NN46250-500
Issue 07.01
October 2015

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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.

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: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

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

result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

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

Downloading Documentation

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

Contact Avaya Support

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

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

Purpose

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 the Avaya Virtual Services Platform 9000. This document provides instructions to use Avaya Command Line Interface (ACLI) and Enterprise Device Manager (EDM).

Related resources

Documentation

See *Documentation Reference for Avaya Virtual Services Platform 9000,* NN46250-100 for a list of the documentation for this product.

Training

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

Course code	Course title
4D00010E	Knowledge Access: ACIS - Avaya ERS 8000 and VSP 9000 Implementation
5D00040E	Knowledge Access: ACSS - Avaya VSP 9000 Support

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.

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 release

The following sections describe what is new in *Configuring VLANs and Spanning Tree on Avaya Virtual Services Platform 9000,* NN46250-500 for Release 4.1.

Features

See the following sections for information about feature-related changes.

MAC Learning tab

Release 4.1 updates the **MAC Security** tab in EDM to be the **MAC Learning** tab. For more information, see Configuring MAC learning parameters on page 104 and VLAN MAC-layer filtering database and MAC security on page 29.

The VSP switch offers a different feature known as MACsec. MACsec, based on the IEEE 802.1ae standard, allows authorized systems in a network to transmit data confidentially and to protect against data transmitted or modified by unauthorized devices. In addition to host level authentication, data confidentiality, and data integrity between authenticated hosts or systems, MACsec protects data from external hacking while the data passes through the public network to reach a receiver host. For more information on MACsec, see *Configuring Security on Avaya Virtual Services Platform 9000,* NN46250-601.

Show vlan name command added

Release 4.1 adds the **`show vlan name`** command. The **`show vlan name`** command allows you to see the full VLAN name configured on the system. Other VLAN commands only display a portion of the name. For more information, see Viewing VLAN information on page 62.

Other changes

There are no other changes.

Chapter 3: VLAN fundamentals

This section describes the virtual local area network (VLAN) features supported on the Avaya Virtual Services Platform 9000.

For more information about the user interface, see *Using ACLI and EDM on Avaya Virtual Services Platform 9000,* NN46250-103.

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 Virtual Services Platform 9000 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 3/1 (the first port in the input/output [I/O] module in chassis slot 3) 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 3/1 in the sales VLAN now is a member of the marketing VLAN.

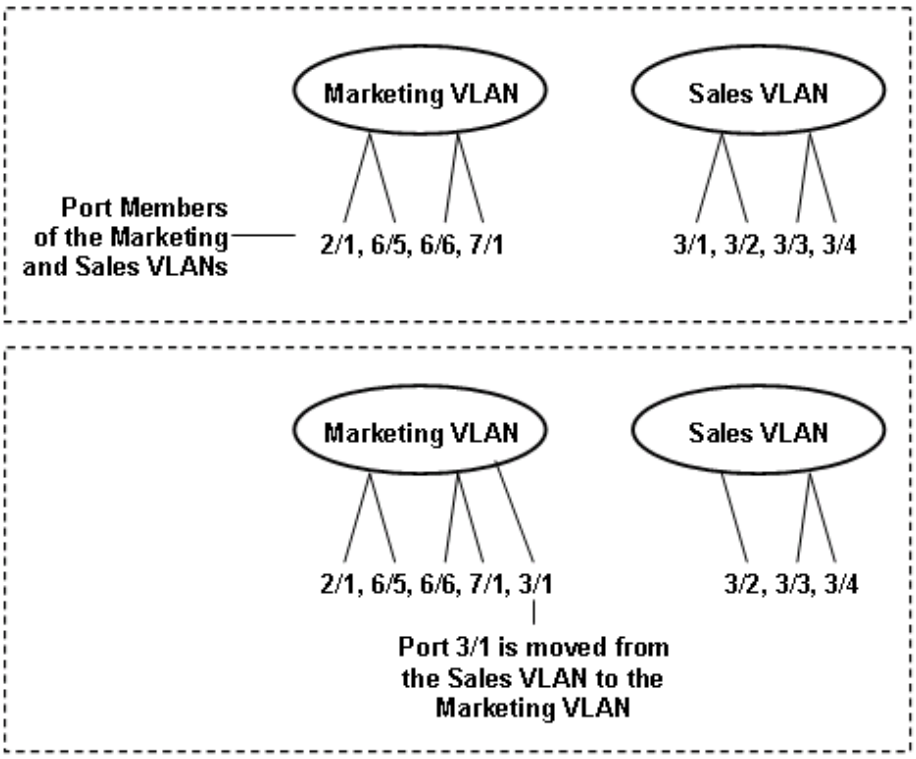

Figure 1: Port-based VLAN

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. You can base a policy on protocol, IP subnet, or source MAC address.

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 of that VLAN expires.

All members of the Spanning Tree Group associated with a protocol-based or IP subnet-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 or a subnet-based VLAN, put the port in the disallowed list. The only exception to this is source-MAC address-based VLANs. For source-MAC-based VLANs, no ports are added as potential port members. The VLANs behave like port-based VLANs and you must add the port members.

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 1: 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 2: Supported policy-based VLAN types

VLAN type	Virtual Services Platform 9000
Protocol-based	supported
Source-MAC address-based	supported
IP subnet-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. Traffic generated by network protocol—Appletalk, Point-to-Point Protocol over Ethernet (PPPoE)—can be automatically confined to its own VLAN.

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 Virtual Services Platform 9000 supports the following protocol-based VLANs:

- IP version 4 (IP)
- AppleTalk on Ethernet Type 2 and Ethernet SNAP frames (AppleTalk)
- Digital Equipment Corporation Local Area Transport (DEC LAT) Protocol (decLat)
- Other DEC protocols (decOther)
- International Business Machines Systems Network Architecture (IBM SNA) on IEEE 802.2 frames (sna802dot2)
- IBM SNA on Ethernet Type 2 frames (snaEthernet2)
- NetBIOS Protocol (netBIOS)
- Xerox Network Systems (XNS)
- Banyan VINES (vines)
- Reverse Address Resolution Protocol (RARP)
- Point-to-Point Protocol over Ethernet (PPPoE)
- ipv6
- ipx802dot2
- ipx802dot3
- ipxEthernet2
- ipxSnap
- user-defined protocols

Multiple protocol-based VLANs cannot be defined for the same protocol.

The maximum number of protocol-based VLANs that can be configured is 16. This restriction is based on a table of 16 entries. Some protocols create more than one entry in the table. For example, an IP protocol-based VLAN creates two entries; one entry for IP ProtocolId= (0x800) and another for ARP ProtocolId=(0x806). If you configure an IP protocol-based VLAN, you can configure only 14 more protocol-based VLANs. For example, configuring a DecOther protocol VLAN takes up nine table entries, leaving only seven remaining. The following is a table of standard protocol VLANs supported on the VSP 9000 and the number of records created for each.

Table 3: Records types created for standard protocol VLAN types

Protocol	Protocol ID	Encapsulation	Number of records
IP	800	Ether2	2
	806	Ether2	
IPv6	0x86DD	Ether2	1
Ipx802.2	0xE0E0	LLC	1
Ipx802.3	0xFFFF	SNAP	1

Table continues…

Protocol	Protocol ID	Encapsulation	Number of records
IpxEther2	0x8137	Ether2	2
	0x8138	Ether2	
IpxSnap	0x8137	SNAP	2
	0x8138	SNAP	
AppleTalk	0x809b	Ether2	4
	0x809b	SNAP	
	0x80F3	Ether2	
	0x80F3	SNAP	
DecLat	0x6004	Ether2	1
DecOther	0x6000	Ether2	9
	0x6001	Ether2	
	0x6002	Ether2	
	0x6003	Ether2	
	0x6005	Ether2	
	0x6006	Ether2	
	0x6007	Ether2	
	0x6008	Ether2	
	0x6009	Ether2	
NetBios	0xF0F0	LLC	1
PPPoE	0x8863	Ether2	2
	0x8864	Ether2	
RARP	0x8035	Ether2	1
SnaEther2	0x80D5	Ether2	1
sna802dot2	0x04xx	LLC	2
	xx04	LLC	
Vines	0xBAD	Ether2	1
XNS	0x600	Ether2	2
	0x807	Ether2	

Example of a PPPoE protocol-based VLAN

With PPPoE, you can connect multiple computers on an Ethernet to a remote site through a device, such as a modem, so that multiple users can share a common line connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dial-up connections, with the Ethernet protocol, which supports multiple users in a local area network (LAN) by encapsulating the PPP frame within an Ethernet frame.

PPPoE occurs in two stages—a discovery stage and a PPP session stage. The Ether_Type field in the Ethernet frame identifies the stage:

- The discovery stage uses 0x8863 Ether_Type.

- The session stage uses 0x8864 Ether_Type.

In the following figure, VLAN 2 is a protocol-based VLAN that transports PPPoE traffic to the Internet Service Provider (ISP) network. The traffic to the ISP is bridged.

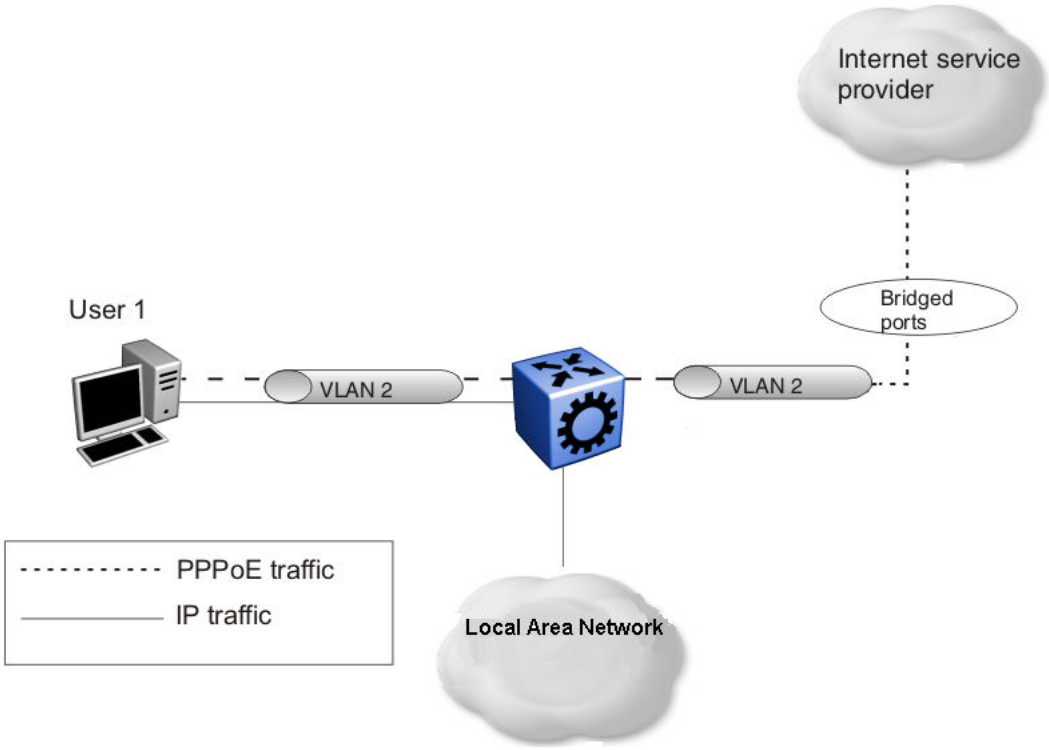

Figure 2: PPPoE and IP configuration

User-defined protocol-based VLANs

You can create user-defined protocol-based VLANs to support networks with nonstandard protocols. For user-defined protocol-based VLANs, you specify the Protocol Identifier (PID) for the VLAN. You also specify an encapsulation type: Etherent2, SNAP, or LLC (802.2). The PID in a frame is encapsulated according to the encapsulation type. Frames that match the specified PID are assigned to that user-defined VLAN:

- the ethertype for Ethernet type 2 frames
- the PID in Ethernet Sub-Network Access Protocol (SNAP) frames
- the Destination Service Access Point (DSAP) or Source Service Access Point (SSAP) value in Ethernet 802.2 frames

The following table lists reserved, predefined policy-based PIDs that cannot be used as user-defined PIDs.

Table 4: PIDs that cannot be used for user-defined protocol-based VLANs

PID (hex)	Description
04xx, xx04	sna802.2
F0xx, xxF0	netBIOS
0000-05DC	Overlaps with 802.3 frame length
0600, 0807	xns
0BAD	VINES
4242	IEEE 802.1d Bridge Protocol Data Units (BPDUs)
6000-6003, 6005-6009	decOther
6004	decLat
0800, 0806	ip
8035	RARP
809B, 80F3	AppleTalk
8100	Reserved by IEEE 802.1Q for tagged frames
80D5	snaEthernet2
8808	IEEE 802.3x pause frames
9000	Used by diagnostic loopback frames
8863, 8864	PPPoE

Source MAC address-based VLANs

You can use source media access control (MAC) address VLANs so the Virtual Services Platform 9000 modules associate frames with a VLAN based on the frame content. With source MAC-based VLANs, a frame is associated with a VLAN if the source MAC address is one of the MAC addresses explicitly associated with the VLAN. To create a source MAC-based VLAN, first create the VLAN and then associate the desired MAC addresses with the VLAN.

You can configure a maximum of 100 source MAC addresses for each chassis. For example, if you configure 60 source MAC addresses for one single VLAN, you can create only 40 more source MAC based VLANs on that chassis.

Use source MAC-based VLANs to enforce a MAC level security scheme to differentiate groups of users. For example, in a university environment, the students are part of a student VLAN with certain services and access privileges, and the faculty are part of a source MAC-based VLAN with faculty services and access privileges. Therefore, a student and a faculty member can plug into the same port, but have access to a different range of services. To provide the correct services throughout the campus, the source MAC-based VLAN must be defined on Virtual Services Platform 9000 devices throughout the campus, which entails administrative overhead. A large list of MAC addresses can cause the administrative overhead to be quite high.

Unlike other types of policy-based VLANs, when you create a source MAC VLAN the port members of the Spanning Tree Group (STG) are not made potential members of the VLAN by default. You must assign static port members to the VLAN to ensure that the source MAC addresses are explicitly associated with the ports in the VLAN and not with the entire network.

IP subnet-based VLANs

Virtual Services Platform 9000 modules support policy-based VLANs based on IP subnets. An untagged frame is classified to a subnet-based VLAN if its source IP address matches the network and mask defined for the VLAN. This allows you to group traffic based on the originating IP subnet, for instance to assign different priorities to traffic arriving on a single port from different subnets, similar to multinetting.

If possible, avoid IP subnet-based VLANs on segments that act as a transit network.

The following figure shows two examples of the incorrect use of IP subnet-based VLANs that result in traffic loss.

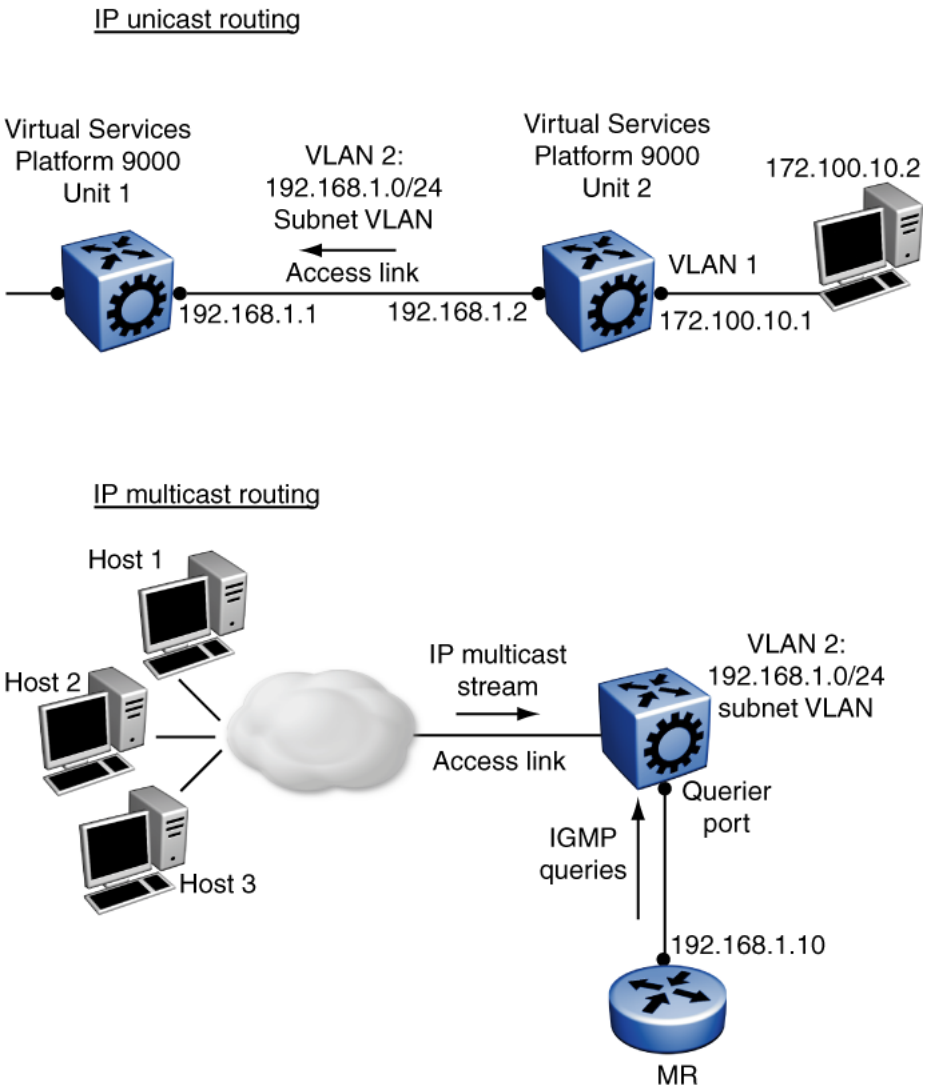

Figure 3: Incorrect use of an IP subnet-based VLAN

In the IP unicast routing example, the host on 172.100.10.2 sends traffic to Unit 2 (172.100.10.1) destined for the router in Unit 1 (192.168.1.1). Unit 2 attempts to route the IP traffic, but that traffic does not arrive at the router in Unit 1. Unit 1 cannot assign this frame to the IP subnet-based VLAN 2 because the IP address of the traffic source does not match the IP subnet assigned to VLAN 2. If

the access link in VLAN 2 that connects Units 1 and 2 were a tagged link, the traffic would be associated with the VLAN tag, not the IP address, and would be forwarded correctly to Unit 1.

In the IP multicast routing example, the multicast stream is on an access link that is part of the IP subnet-based VLAN 2. If the source IP address in the multicast data packets received on the access port is not within the subnet of VLAN 2 (a likely scenario), the multicast stream cannot reach the multicast router (MR).

SPBM B-VLAN

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

Note:

SPB internally uses spanning tree group (STG) 63 or Multiple Spanning Tree Instance (MSTI) 62. STG 63 or MSTI 62 cannot be used by another VLAN or MSTI. For non-SPB customer networks, if you use STG 63 or MSTI 62 in the configuration, you must delete STG 63 or MSTI 62 before you can configure SPBM.

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 Virtual Services Platform 9000 supports the IEEE 802.1Q specification for tagging frames and coordinating VLANs across multiple switches.

Figure 4: VLAN tag insertion on page 21 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.

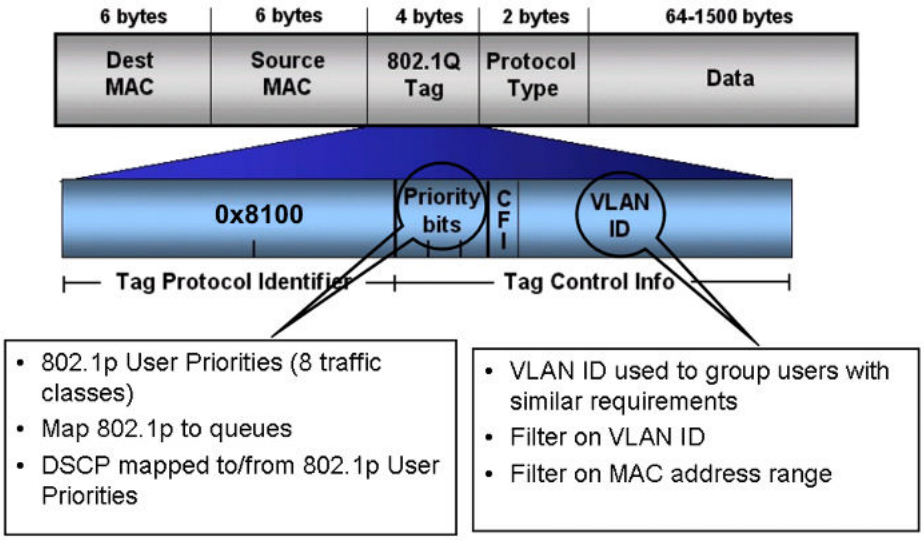

Figure 4: VLAN tag insertion

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.

On the Virtual Services Platform 9000, 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 Virtual Services Platform 9000 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 Virtual Services Platform 9000 removes the tag from the frame before sending it to the port.

Treatment of tagged and untagged frames

The Virtual Services Platform 9000 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 Virtual Services Platform 9000 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 (0). 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 Virtual Services Platform 9000 tries to associate untagged frames with a VLAN in the following order:

- Does the frame belong to a source MAC-based VLAN?
- Does the frame belong to an IP subnet-based VLAN?
- 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 a Virtual Services Platform 9000. 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.

In the case of the Virtual Services Platform 9000, after an IP phone is attached to an untagged port and configured into an IP subnet-based VLAN, 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.

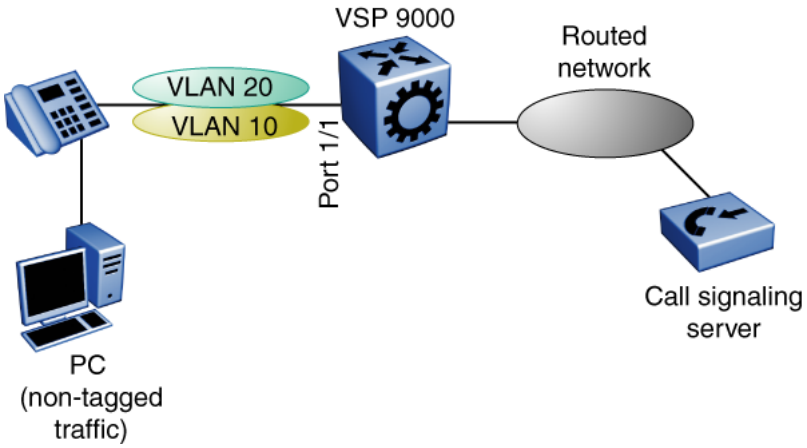

Figure 5: Network with IP phone and PC

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

Virtual Services Platform 9000 modules support IP routing on the following types of VLANs:

- Port-based VLANs
- Source IP subnet-based VLANs
- IP protocol-based VLANs
- Source MAC-based VLANs
- Management VLAN 4092: the VLAN comprising the VSP 9000 Management interface

IP routing is not supported on VLANs based on other protocols, including user-defined protocol-based VLANs.

VLAN implementation

This section describes how to implement VLANs on the Virtual Services Platform 9000 and describes default VLANs, the unassigned (NULL) VLAN, and brouter ports. This section also summarizes the defaults and rules regarding VLAN creation on the Virtual Services Platform 9000.

- Default VLAN on page 23
- NULL VLAN on page 24
- Brouter ports on page 24

Default VLAN

Virtual Services Platform 9000 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, Virtual Services Platform 9000 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 Virtual Services Platform 9000:

- Virtual Services Platform 9000 can support up to 4084 configurable VLANS. VLAN IDs range from 1 to 4084. VLAN IDs 4085 to 4094 are reserved for 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. Virtual Services Platform 9000 supports up to 16 protocol-based VLANs, but see Protocol-based VLANs on page 14 for limitations.
- The VLAN membership of a frame is determined by the following order of precedence, if applicable:
  1. IEEE 802.1Q tagged VLAN ID
  2. IP subnet-based VLAN
  3. source MAC-based VLAN
  4. protocol-based VLAN
  5. port-based VLAN default VLAN of the receiving port
- The IP subnet-based VLAN must not be assigned to a transit network (for example, a network routed to a bridged subnet).

VLAN feature support

The following table summarizes features supported on Virtual Services Platform 9000 modules.

Refer to the release notes that come with your device to obtain the latest scalability information.

Table 5: VLAN support on Virtual Services Platform 9000

Feature	Description
Number of VLANs	4084
Port-based VLANs	Supported
Policy-based VLANs • Protocol-based • Source MAC-based • Source IP subnet-based	Supported
User-defined protocol VLANs	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.

Virtual Services Platform 9000 interoperates with NLB clusters operating in the following modes:

- Unicast mode
- Multicast mode
- IGMP multicast mode

You must configure NLB to use the same mode as Virtual Services Platform 9000.

Note:

Virtual Services Platform 9000 supports static ARP entries for NLB multicast and NLB multicast IGMP. Virtual Services Platform 9000 does not support static ARP entries for NLB unicast.

For interoperability with NLB, Virtual Services Platform 9000 provides configuration options at the global level, and at the VLAN level.

The following configuration options are available at the 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 Virtual Services Platform 9000. ARP responses from the Virtual Services Platform 9000 are sent to the virtual MAC address (rather than to the hardware MAC address).

You can configure Virtual Services Platform 9000 for NLB unicast mode support. After you enable the NLB unicast option, the Virtual Services Platform 9000 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 Avaya Virtual Services Platform 9000,* NN46250-401.

NLB clustering in multicast mode

When the cluster is running in NLB multicast mode, a multicast virtual MAC address with the format 03-bf-x-x-x-x (where x-x-x-x is the cluster IP address) is bound to all cluster hosts but the real MAC address of the network adapter is retained. The multicast MAC address is used for client-to-cluster traffic and the real MAC address of the adapter is used for network traffic specific to the host server.

You can configure Virtual Services Platform 9000 for NLB multicast mode support. If you enable NLB multicast mode, the Virtual Services Platform 9000 learns which ports on the VLAN are directly connected to cluster servers by using the ARP replies that the cluster sends. The Virtual Services Platform 9000 internally maps the NLB multicast MAC (03:bf:x:x:x:x) to the ports on which the ARP replies are received. Only VLAN ports with connected NLB servers are added to the internal NLB MAC entries.

Virtual Services Platform 9000 also uses the multicast MAC to create an ARP entry for the NLB cluster.

Rather than flooding traffic destined to the cluster IP address to all ports on the VLAN, Virtual Services Platform 9000 forwards cluster traffic only to the cluster ports. For information about software scaling capabilities in multicast mode, see *Release Notes for Avaya Virtual Services Platform 9000,* NN46250-401.

Note:

SPBM supports Network Load Balancing (NLB) unicast. SPBM does not support NLB-multicast and NLB-multicast with IGMP. For more information on SPBM, see *Configuring Avaya Fabric Connect on Avaya Virtual Services Platform 9000,* NN46250-510.

NLB clustering in IGMP-multicast mode

When the cluster operates in NLB IGMP-multicast mode, a multicast virtual MAC address in the format 01–00–5e–7f–x–x is bound to all cluster hosts and the real MAC address of the network

adapter is retained. In this case, the x-x at the end of the multicast virtual MAC address are the last two bytes of the cluster IP address. The multicast MAC address is used for client-to-cluster traffic, and the real MAC address is used for network traffic specific to the host computer.

You can configure Virtual Services Platform 9000 for NLB IGMP-multicast mode support. If you enable NLB IGMP-multicast mode, the Virtual Services Platform 9000 learns the cluster ports on the VLAN by using the IGMP reports that the cluster sends. The Virtual Services Platform 9000 internally maps the NLB multicast MAC (01:00:5e:7f:x:x) to the ports on which the IGMP reports are received.

Virtual Services Platform 9000 uses the multicast MAC to create an ARP entry for the NLB cluster.

Similar to multicast mode, rather than flooding traffic destined to the cluster IP address to all ports on the VLAN, the Virtual Services Platform 9000 forwards cluster traffic only to the cluster ports.

NLB multicast mode considerations

After you activate NLB multicast mode, the Virtual Services Platform 9000 does not automatically show the cluster server ports in the NLB table. In multicast mode, the switch adds the server ports to the NLB table based on the ARP replies it receives from the cluster hosts.

NLB IGMP-multicast mode considerations

After you activate NLB IGMP-multicast mode, the Virtual Services Platform 9000 does not automatically show the cluster server ports in the NLB table. In IGMP multicast mode, the switch adds the server ports to the NLB table based on the IGMP reports it receives from the cluster hosts.

Note:

To use IGMP-multicast mode, you must also enable IGMP snooping. If you do not enable IGMP snooping, IGMP-multicast mode remains disabled. For more information on IGMP snooping, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 9000,* NN46250-504.

Global IP ARP Multicast MAC Flooding

In addition to the VLAN-level configurations described in the preceding sections, you can also alter the operation of NLB clustering on the Virtual Services Platform 9000 by configuring the global IP ARP Multicast MAC flooding feature. If you enable IP ARP multicast MAC flooding, all traffic sent to the virtual IP address for the cluster floods across all VLAN ports.

You can configure IP ARP Multicast MAC flooding with multicast or IGMP multicast mode. The following table describes the multicast configuration options and the resulting actions on Virtual Services Platform 9000.

NLB mode configured	IP ARP Multicast MAC flooding status	Result on Virtual Services Platform 9000
Multicast mode	Disabled	• Learns cluster server ports using ARP replies. • Forwards cluster traffic only to the cluster ports. • Supports one NLB cluster for each VLAN.

Table continues…

NLB mode configured	IP ARP Multicast MAC flooding status	Result on Virtual Services Platform 9000
		• To support more than one cluster on a VLAN, you must create static multicast ARP entries for the additional NLB clusters. • Does not support connectivity to a secondary virtual IP address.
Multicast mode	Enabled	• Forwards cluster traffic to all the ports in the VLAN. • Supports an unlimited number of NLB clusters for each VLAN. • If you later disable IP ARP Multicast MAC flooding, the system deletes the ARP entries, and then begins to learn ARP entries from the server-connected ports. • Supports connectivity to a secondary virtual IP address with Global IP ARP Multicast MAC flooding enabled.
IGMP multicast mode	Disabled	• Learns cluster server ports using IGMP reports rather than ARP replies. • Forwards cluster traffic only to the cluster ports. • Supports one NLB cluster for each VLAN. • To support more than one cluster on a VLAN, you must create static multicast ARP entries for the additional NLB clusters. • Does not support connectivity to a secondary virtual IP address.
IGMP multicast mode	Enabled	• Forwards cluster traffic to all the ports in the VLAN. • Supports an unlimited number of NLB clusters for each VLAN. • If you later disable IP ARP Multicast MAC flooding, the system deletes the ARP entries, and then begins to learn ARP entries from the server-connected ports.

Table continues…

NLB mode configured	IP ARP Multicast MAC flooding status	Result on Virtual Services Platform 9000
		• Supports connectivity to a secondary virtual IP address with Global IP ARP Multicast MAC flooding enabled.

VLAN MAC-layer filtering database and MAC security

To perform MAC-layer bridging, the device must know the destination MAC-layer address of each device on each attached network, so it can forward packets to the appropriate destination. MAC-layer addresses are stored in the bridge forwarding database (FDB) table, and you can forward packet traffic based on the destination MAC-layer address information.

MAC security

Use MAC security to control traffic from specific MAC addresses. You can also limit the number of allowed MAC addresses. You can enable this feature at two levels: globally and at the port level.

Note:

The VSP switch offers a different feature known as MACsec. MACsec, based on the IEEE 802.1ae standard, allows authorized systems in a network to transmit data confidentially and to protect against data transmitted or modified by unauthorized devices. In addition to host level authentication, data confidentiality, and data integrity between authenticated hosts or systems, MACsec protects data from external hacking while the data passes through the public network to reach a receiver host. For more information on MACsec, see *Configuring Security on Avaya Virtual Services Platform 9000,* NN46250-601.

At the global level this feature is a filter mechanism to filter out (drop) packets that contain certain MAC addresses as the source or destination. You configure a set of MAC addresses. The system drops a packet that contains one of these configured addresses as the source or destination.

Port-level MAC security provides more flexibility over the global configuration. Port—level security applies to traffic for all VLANs received on that port.

Port-level MAC security provides two options:

- unknown-discard: After you enable this feature, the port drops received packets with an unknown source MAC address and adds the MAC addresses to the FDB table with the status of discard. This option provides some control over the number of MAC addresses that are learned and forwarded:
  - allow-mac: You can configure a group of MAC addresses. The port processes packets that match these MAC addresses even if you enable unknown-mac-discard.
  - auto-learning: Configure a number of MAC addresses for the port to learn, even if you enable unknown-mac-discard. The port learns source MAC addresses for received packets up to a maximum value that you configure. After the number of addresses exceeds the maximum value, the port discards packets and does not learn more MAC addresses until an existing address ages out of the table.

- auto-learning learning-mode: Specifies the learning mode as one of the following:
  - one-shot: The auto-learned addresses do not age out. When the VLAN mac-address entry is flushed, the auto-learned addresses are not flushed.
  - continuous: In continuous mode the aging of the auto-learned MAC is subject to the normal aging. When the system flushes the VLAN MAC address entry, the system also flushes the auto-learned addresses.
- lock-learning-MAC: If you enable this option, then no MAC addresses are auto-learned. The port drops packets that it receives and adds the MAC addresses to the FDB table with the status of discarded.

- limit-learning: This option protects the FDB from traffic from too many MAC addresses, which fill the FDB table.

  This option limits the number of MAC addresses a port learns. You can specify a maximum and minimum number of addresses. After the number of addresses exceeds the maximum, learning stops. MAC address learning resumes after enough existing addresses age out that only the minimum number of addresses remain. This option does not affect packet forwarding; it limits only MAC learning.

Important:

Do not enable limit-learning and auto-learning for a port simultaneously.

Prevention of IP spoofing within a VLAN

You can prevent VLAN logical IP spoofing by blocking the external use of the device IP address. A configurable option is provided, for each port, which detects a duplicate IP address (that is, an address that is the same as the device VLAN IP address) and blocks all packets with a source or destination address equal to that address.

If an ARP packet is received that has the same source IP address as the logical VLAN IP address of the receiving port, all traffic coming to that port (with this MAC address as source/destination address) is discarded by the hardware. After detecting a duplicate IP address, the device sends a gratuitous ARP packet to inform devices on the VLAN about the correct MAC address for that IP address. You can specify a time on a configurable global timer after which the MAC discard record is deleted, and the device resumes accepting packets from that MAC address.

If you use Split MultiLink Trunking (SMLT), you must configure this option on both SMLT aggregation devices to avoid connectivity issues.

Important:

After you enable the IP spoofing feature, you must restart the device.

VLAN loop detection and prevention

The loop detection feature is used at the edge of a network to prevent loops. It detects whether packets with the same source MAC address for a VLAN are received on different ports. If the same MAC address for the same VLAN is detected on two different ports five times in a configurable amount of time, a configured loop detect action is performed.

The loop detection feature also offers an optional parameter, known as ARP detect, to detect Layer 3 loops.

Enable the loop detection feature on SMLT ports. Do no use loop-detect on IST ports or core SMLT square or full mesh ports.

Important:

If you attempt to enable loop-detect on an existing IST port, the system prevents you from doing so. However, if you have a port with loop-detect already enabled, and you add that port to an IST, the system does not prevent you from doing so, causing potential system errors.

The loop detection feature is configured for each device. If a loop detection event takes place, peer devices are not notified.

The loop detection feature has the following traits:

- If a source MAC address is found to loop, and the specified loop detect action is MAC-discard, the MAC address is disabled. The incoming packets with this source or destination MAC address can be discarded for that VLAN.
- If a source MAC address is found to loop, and the specified loop detect action is Port Down, the port on which the loop was detected is disabled.
- Ports and MAC addresses that have been disabled by the loop detection feature are reenabled for automatic recovery.
- The link flap feature configures ports to operational down rather than admin down.
- Loop detection cannot be enabled on interswitch trunk ports.

To detect loops on a VLAN, Virtual Services Platform 9000 also supports Simple Loop Prevention Protocol.

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. The system sends SLPP packets using Layer 2 multicast. A switch only looks at its own SLPP packets or at its peer SLPP packets. It ignores SLPP packets from other parts of the network. 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. 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 and never on IST 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.

The loop detection functionality of Virtual Services Platform 9000 must not be used under normal operating conditions. Only use it if directed by the technical configuration guides (TCG) or if directed by Avaya technical support personnel.

You cannot configure the EtherType for SLPP. Virtual Services Platform 9000 uses an EtherType of 0x8102 . For more information about how to design your network with SLPP, see *Network Design Reference for Avaya Virtual Services Platform 9000,* NN46250-200.

IGMP Layer 2 Querier

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 normally provides the IGMP querier function. You can use the IGMP Layer 2 Querier 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, Virtual Services Platform 9000 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.

For more information about how to configure IGMP Layer 2 Querier, see *Configuring IP Multicast Routing Protocols on Avaya Virtual Services Platform 9000,* NN46250-504.

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, add or remove ports in the VLAN, configure priority, change a VLAN name, or perform other operations.

Important:

You can also configure loop detection and other features.

Creating a VLAN

Use this procedure to create VLANs.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Create a VLAN:

   ```
   vlan create <2-4084> [name WORD<0-64>] type {ipsubnet-mstprstp
   <0-63> {A.B.C.D/X}|port-mstprstp <0-63>|protocol-mstprstp <0-63>
   {appleTalk|decLat|decOther|ip|ipv6|ipx802dot2|ipx802dot3|
   ipxEthernet2|ipxsnap|netBios|PPPoE|rarp|sna802dot2|snaEthernet2|
   userDefined|vines|xns}|spbm-bvlan|srcmac-mstprstp<0-63>} [color <0-
   32>]
   ```

Example

Create a VLAN:

```
VSP-9012:1(config)# vlan create 2 name test type ipsubnet-mstprstp 63
15.15.15.2/255.255.255.0 color 32
```

Variable definitions

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

Variable	Value
<2-4084>	Specifies the VLAN ID in the range of 2-4084.
color *<0-32>*	Specifies the color of the VLAN.
name *WORD<0-64>*	Specifies the VLAN name. The name attribute is optional. **Note:** Do not use the name Mgmt when you specify a name for the VLAN that you create. The VSP 9000 creates a management VLAN at boot up with the assigned name Mgmt. The show command does not show the management VLAN.
type ipsubnet-mstprstp *<0-63>* *<A.B.C.D/X>*	Creates a VLAN by IP subnet: • *<0-63>* is the STP instance ID in the range of 0-63. • *A.B.C.D/X* is the subnet address or mask {a.b.c.d/x | a.b.c.d/x.x.x.x}.
type port-mstprstp *<0-63>*	Creates a VLAN by port: • *<0-63>* is the STP instance ID from 0 to 63.
type protocol-mstprstp *<0-63>* {appleTalk|decLat|decOther|ip|ipv6|ipx802dot2|ipx802dot3|ipxEthernet2|ipxsnap|netBios|PPPoE|rarp|sna802dot2|snaEthernet2|userDefined|vines|xns}	Creates a VLAN by protocol: • *<0-63>* is the STP instance ID. • appleTalk is the AppleTalk on Ethernet Type 2 and Ethernet SNAP frames Protocol. • decLat is the Digital Equipment Corporation Local Area Transport (DEC LAT) Protocol. • decOther is the DEC other Protocols. • ip is the IP version 4 Protocol. • ipv6 is the IP version 6 protocol. • ipx802dot2 specifies the Novell Internetwork Packet Exchange (IPX) on IEEE 802.2 frames. • ipx802dot3 specifies the Novell Internetwork Packet Exchange (IPX) on Etherent 802.3 frames. • ipxEthernet2 specifies the Novell IPX on Ethernet type 2 frames. • ipxsnap specifies the Novell IPX on Ethernet Standard Network Access Protocol (SNAP) frames.

Table continues…

Variable	Value
	• netbios is the NetBIOS Protocol. • PPPoE is the Point-to-Point Protocol Over Ethernet (PPPoE). • rarp is the Reverse Address Resolution Protocol (RARP). • sna802dot2 is the International Business Machines Systems Network Architecture (IBM SNA) on IEEE 802.2 frames. • snaethernet2 is the IBM SNA on Ethernet Type 2 frames. • vines is the Banyan VINES Protocol. • xns is the Xerox Network Systems Protocol.
type protocol-mstprstp *<0-63>* userDefined *{0x0000|<decimal value>}*][encap {ethernet-ii|llc|snap}]	Creates a VLAN using a user defined protocol. • *<0-63>* is the STP instance ID in the range of 0-63. • *{0x0000|<decimal value>}* is the protocol ID in hexadecimal or decimal value. • *encap* specifies the frame encapsulation header type as Ethernet II, IEEE 802.2 Logic Link Control (LLC) encapsulation or SubNetwork Access Protocol (SNAP). The encapsulation type is only for user-defined protocol-based VLANs. The encap parameter is not meaningful for other types of VLAN. By default, there is no encapsulation method configured for the VLAN.
spbm-bvlan	Creates 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. 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

Table continues…

Variable	Value
	• Source address learning is disabled • Unknown MAC discard is disabled Essentially the VLAN becomes a header indicating the SPBM network to use. Modification of the VLAN behavior is necessary to ensure proper control over the SPBM traffic. **Note:** SPB internally uses spanning tree group (STG) 63 or Multiple Spanning Tree Instance (MSTI) 62. STG 63 or MSTI 62 cannot be used by another VLAN or MSTI. For non-SPB customer networks, if you use STG 63 or MSTI 62 in the configuration, you must delete STG 63 or MSTI 62 before you can configure SPBM.
type srcmac-mstprstp *<0-63>*]	Creates a VLAN by source MAC address: • *<0-63>* is the STP instance ID in the range of 0-63.

Assigning an IP address to a VLAN

Assign an IP address to a VLAN.

Before you begin

- You must create the VLAN.

Procedure

1. Enter VLAN Interface Configuration mode:

   ```
   enable
   configure terminal
   interface vlan <1-4084>
   ```

2. Assign an IP address to a VLAN:

   ```
   ip address <A.B.C.D/X>|<A.B.C.D> <A.B.C.D> [<0-1535>]
   ```

Example

Log on to VLAN Interface Configuration:

```
VSP-9012:1(config)#interface vlan 10
```

Assign an IP address to a VLAN:

```
VSP-9012:1(config-if)#ip address 16.16.16.1/255.255.255.0 200
```

Variable definitions

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.
[<0-1535>]	Specifies the MAC-offset value. The value is in the range of 0–1535.

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 <1-4084> {none|flushMacFdb|flushArp|flushIp|
   flushDynMemb|triggerRipUpdate|all}
   ```

Example

Perform a general VLAN action.

```
VSP-9012:1(config)#vlan action 1 none
VSP-9012:1(config)#vlan action 1 flushMacFdb
VSP-9012:1(config)#vlan action 1 flushIp
VSP-9012:1(config)#vlan action 1 flushDynMemb
VSP-9012:1(config)#vlan action 1 triggerRipUpdate
```

Variable definitions

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

Variable	Value
none	Configures action to none. This action performs no updates.

Table continues…

Variable	Value
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.
triggerRipUpdate	Configures action to triggerRipUpdate. After you execute this command the Virtual Services Platform 9000 immediately sends a RIP request to solicit the updated RIP routes.
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 <1-4084> <0x00:0x00:0x00:0x00:0x00:0x00>
   {slot/port[-slot/port][,...]}
   ```

Example

Configure a static MAC address of a VLAN.

```
VSP-9012:1(config)#vlan mac-address-static 1 0x00:0x00:0x00:0x00:0x00:0x01 4/1
```

Variable definitions

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

Variable	Value
<1-4084>	Specifies the VLAN ID in the range of 1–4084. VLAN IDs 1 to 4084 are configurable; VLAN IDs 4085-4094 are reserved for internal use.
<0x00:0x00:0x00:0x00:0x00:0x00:0x00>	Indicates the MAC address.
{slot/port[-slot/port][,...]}	Specifies the port number using slot/port notation.

Enabling global MAC security

Enable global MAC security to filter out (drop) packets that contain certain MAC addresses as source or destination. Configure a set of MAC addresses. The system drops a packet that contains one of these configured MAC addresses as source or destination.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable MAC security:

   ```
   mac-security mac-da-filter add 0x00:0x00:0x00:0x00:0x00:0x00
   ```

3. Show the MAC addresses in the security filter:

   ```
   show fdb-filter
   ```

   OR

   ```
   show mac-security mac-da-filter
   ```

Example

Enable MAC security:

```
VSP-9012:1(config)#mac-security mac-da-filter add 00:08:09:07:08:09
```

Show the MAC addresses in the security filter:

```
VSP-9012:1(config)#show mac-security mac-da-filter

================================================================================
                              Global Fdb Filter
================================================================================
MAC ADDRESS
--------------------------------------------------------------------------------
00:08:09:07:08:09
```

Limiting MAC address learning

Configure the MAC security feature to control traffic from specific MAC addresses. You can also limit the number of allowed MAC addresses. You can enable this feature at two levels: global level and port level.

About this task

Limit MAC address learning to limit the number of forwarding database (FDB) entries learned on a particular port to a user-specified value. After the number of learned forwarding database entries reaches the maximum limit, packets with unknown source MAC addresses are flooded to all member ports.

Control the number of MAC addresses that are learned and forwarded. The system can drop all packets that do not match configured MAC addresses. It also allows you to learn a certain number after which the system drops all packets.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable

   configure terminal

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

2. Protect the FDB from hits by too many MAC addresses:

   ```
   mac-security port {slot/port [-slot/port][,...]} limit-learning
   enable [max-addrs <1-64000>] [min-addrs <0-64000>] [snmp-trap]
   [violation-down-port]
   ```

Example

Protect the FDB from hits by too many MAC addresses.

```
VSP-9012:1(config)#interface gigabitethernet 4/5
VSP-9012:1(config-if)#mac-security limit-learning enable
VSP-9012:1(config-if)#mac-security limit-learning max-addrs 5000
VSP-9012:1(config-if)#mac-security limit-learning min-addrs 3000
```

Variable definitions

Use the data in the following table to use the **`mac-security limit-learning`** command.

Variable	Value
enable	Limits the MAC learning for the port. This feature does not affect the forwarding of the packets. If you enable limit-learning, the FDB entry for each port is limited to the number you specify in max-addrs.

Table continues…

Variable	Value
	If you enable the auto-learn parameter, after the maximum addresses are learned, all the new SA MAC packets are dropped. This feature provides no value if you enable unknown-mac-discard and disable auto-learn because all unknown packets are dropped. Do not enable auto-learning and limit-learning simultaneously.
max-addrs *<1–64000>*	Specifies the maximum number of MAC addresses to learn. After the maximum value is reached, no further MAC learning occurs. The system does not drop packets; it forwards packets. The default is 1024.
min-addrs *<0–64000>*	Specifies the minimum number of MAC addresses to learn. MAC learning restarts after the FDB entry count reaches the value you specify in min-addrs. The default is 512.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
snmp-trap	Enable logging and SNMP traps for violations. The default is disabled.
violation-down-port	Disables the port on violation. The default is disabled.

Configuring auto-learning and allowed MAC addresses

Configure auto-learning so the system processes packets with an unknown MAC address. You configure the number of addresses the system learns by configuring a maximum number of addresses.

Before you begin

- You must enable the `unknown-discard` option for the port.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

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

2. Enable the unknown discard option:

```
mac-security [port {slot/port[-slot/port][,...]}] unknown-discard
enable
```

3. Configure the set of MAC addresses with matching source MAC addresses to allow:

```
mac-security [port {slot/port[-slot/port][,...]}] unknown-discard
allow-mac 0x00:0x00:0x00:0x00:0x00:0x00 [auto]
```

4. Enable auto-learning:

```
mac-security [port {slot/port[-slot/port][,...]}] unknown-discard
auto-learning enable
```

5. Configure the system to log a violation on the port:

```
mac-security [port {slot/port[-slot/port][,...]}] unknown-discard
violation-logging
```

6. Configure the system to send an authentication trap on violation:

```
mac-security [port {slot/port[-slot/port][,...]}] unknown-discard
violation-send-authentication-trap
```

7. Configure the port to shutdown on violation:

```
mac-security [port {slot/port[-slot/port][,...]}] unknown-discard
violation-down-port
```

8. Configure the learning mode:

```
mac-security [port {slot/port[-slot/port][,...]}] unknown-discard
auto-learning learning-mode <one-shot|continuous>
```

9. Determine if auto-learned addresses save in the configuration file:

```
mac-security [port {slot/port[-slot/port][,...]}] unknown-discard
auto-learning lock-learning-mac
```

10. Configure the maximum number of unknown MAC addresses to learn:

```
mac-security [port {slot/port[-slot/port][,...]}] unknown-discard
auto-learning max-addrs <0–2048>
```

11. View auto-learned MAC addresses:

```
show vlan autolearn-mac
```

Example

Configure the set of MAC addresses with matching source MAC addresses to allow.

```
VSP-9012:1(config-if)#mac-security unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x55
VSP-9012:1(config-if)#mac-security unknown-discard allow-mac 0x00:0x00:0x00:0x00:0x00:0x66
```

Determine if auto-learned addresses save in the configuration file.

```
VSP-9012:1(config-if)#mac-security port 4/1 unknown-discard auto-learning lock-learning-
mac
```

Configure the learning mode.

```
VSP-9012:1(config-if)#mac-security port 4/1 unknown-discard auto-learning learning-mode
continuous
```

Configure the maximum number of unknown MAC addresses to learn.

```
VSP-9012:1(config-if)#mac-security unknown-discard enable
VSP-9012:1(config-if)#mac-security unknown-discard auto-learning enable
VSP-9012:1(config-if)#mac-security port 4/1 unknown-discard auto-learning max-addr 200
```

Variable definitions

Use the data in the following table to use the **`mac-security unknown-discard`** command.

Variable	Value
allow-mac 0x00:0x00:0x00:0x00:0x00:0x00 [auto]	Configures the set of MAC addresses and frames with matching source MAC addresses that the port processes, even though `unknown-discard` is enabled. These manually entered MAC addresses are saved when you save the configuration and restored on system restart.
auto-learning enable	Enables the auto-learning option.
auto-learning learning-mode <one-shot|continuous>	Specifies the learning mode as one of the following: • one-shot: The auto-learned addresses do not age out. When the VLAN mac-address-entry is flushed, the auto-learned addresses are not flushed. • continuous: In continuous mode the aging of the auto-learned MAC is subject to the normal aging. When the VLAN mac-address-entry is flushed, the auto-learned addresses are also flushed.
auto-learning lock-learning-mac	Saves autolearned addresses when you save the configuration file.
auto-learning max-addrs *<0–2048>*	Specifies the total number of unknown MAC addresses to learn. The default is 2048.
enable	Enables the unknown-discard option. The default is disabled.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
violation-down-port	Shuts the port down on violation. The default is disabled.
violation-logging	Logs a violation. The default is enabled.

Table continues…

Variable	Value
violation-send-authentication-trap	Sends an authentication trap on violation. The default is disabled.

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 VLAN Interface Configuration mode:

   ```
   enable
   configure terminal
   interface vlan <1-4084>
   ```

2. Add ports in a VLAN:

   ```
   vlan members add <1-4084> {slot/port[-slot/port][,...]}
   [{portmember|static|notallowed}]
   ```

3. Remove ports in a VLAN:

   ```
   vlan members remove <1-4084> {slot/port[-slot/port][,...]}
   [{portmember|static|notallowed}]
   ```

Example

Add ports in a VLAN.

```
VSP-9012:1(config-if)#vlan members add 1 4/2 static
```

Remove ports in a VLAN.

```
VSP-9012:1(config-if)#vlan members remove 1 4/2 notallowed
```

Variable definitions

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

Variable	Value
<1-4084>	Specifies the VLAN ID in the range of 1–4084. VLAN IDs 1–4084 are configurable. VLAN IDs 4085-4094 are reserved for internal use.
{slot/port[-slot/port][,...]}	Specifies the port number using slot/port notation.
portmember	Configures the port type as port member.

Creating an OSPF passive interface on a VLAN

Use this procedure to form neighbor adjacencies on some ports of a VLAN while other ports on the same VLAN remain passive. If you do not use this procedure to make a port within the VLAN an OSPF passive port, all ports on the VLAN can form a neighbor adjacency.

About this task

This command is a port-level configuration to choose a specific port as a passive Open Shortest Path First (OSPF) port on the VLAN. The port configuration takes precedence over the VLAN configuration.

If you use the **ip ospf network passive** command to make the VLAN passive, all ports on the VLAN will stop forming neighbor adjacencies. For more information about how to configure OSPF on a VLAN, see *Configuring OSPF and RIP on Avaya Virtual Services Platform 9000,* NN46250-506.

OSPF will not form an adjacency over these selected ports, and it will not flood any OSPF traffic over these ports. The configuration does not affect other types of control or data traffic flow over those ports.

For an MLT, you only need to provide a single member port of the MLT.

If you add a new port to an MLT that is configured as passive OSPF in a VLAN, the newly added port inherits the MLT behavior. If you remove a port or MLT from the VLAN, the port or MLT loses the passive OSPF property.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Specify which port to make passive:

   ```
   vlan ports ospf-passive <1-4084> {slot/port[-slot/port][,...]}
   ```

Example

Create ports 4/4 through 4/6, which are members of VLAN 10, as passive.

```
VSP-switch:1>enable
VSP-switch:1#configure terminal
VSP-switch:1(config)#vlan ports ospf-passive 10 4/4-4/6
```

Variable definitions

Use the data in the following table to use the **vlan ports ospf-passive** command.

Variable	Value
<1–4084>	Specifies a VLAN ID.

Table continues…

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Adding or removing source MAC addresses for a VLAN

Add or remove a VLAN source MAC addresses to configure the source MAC address for a source MAC-based VLAN.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Add a VLAN source MAC address:

   ```
   vlan srcmac <2-4084> <0x00:0x00:0x00:0x00:0x00:0x00>
   ```

3. Remove a VLAN source MAC address:

   ```
   no vlan srcmac <2-4084> <0x00:0x00:0x00:0x00:0x00:0x00>
   ```

4. Configure a VLAN source MAC address to the default value:

   ```
   default vlan srcmac <2-4084> <0x00:0x00:0x00:0x00:0x00:0x00>
   ```

Example

Add a VLAN source MAC address.

```
VSP-9012:1(config)#vlan create 10 type srcmac-mstprstp 0
VSP-9012:1(config)#vlan srcmac 10 0x00:0x00:0x00:0x00:0x00:0x11
```

Variable definitions

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

Variable	Value
<2-4084>	Specifies the VLAN ID in the range of 2–4084.
<0x00:0x00:0x00:0x00:0x00:0x00>	Indicates the MAC address.

Configuring VLAN classification precedence

Configure classification precedence to change classification precedence between source-MAC and subnet-based VLANs for a port. You can enable or disable source-MAC-based classification and subnet-based classification for a port. You can also enable or disable protocol-based classification.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable

   configure terminal

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

2. Enable or disable source-MAC-based VLAN classification for the port:

   ```
   [default] [no] source-mac-vlan [port {slot/port[-slot/port][,...]}]
   [enable]
   ```

   The default value is enabled.

3. Enable or disable IP subnet-based VLAN classification for the port:

   ```
   [default] [no] subnet-vlan [port {slot/port[-slot/port][,...]}]
   [enable]
   ```

   The default value is enabled.

4. Enable protocol-based VLAN classification for the port:

   ```
   [default] [no] protocol-vlan [port {slot/port[-slot/port][,...]}]
   [enable]
   ```

   The default value is enabled.

5. Specify whether source-MAC or IP subnet classification takes precedence:

   ```
   policy-vlan-precedence [port {slot/port[-slot/port][,...]}] {source-
   mac|subnet}
   ```

   The default value is source-mac.

6. Configure the VLAN classification to the default value:

   ```
   default policy-vlan-precedence [port {slot/port[-slot/port][,...]}]
   ```

   The default value is source-mac.

7. Display port VLAN information:

   ```
   show interface gigabitEthernet vlan <1-4084> {slot/port[-slot/port]
   [,...]}
   ```

Example

Display port VLAN information:

```
VSP-9012:1(config)#show interfaces gigabitEthernet vlan 4/1-4/4
```

```
================================================================================
                                  Port Vlans
================================================================================
PORT          DISCARD DISCARD   DEFAULT VLAN            PORT     UNTAG    DYNAMIC
NUM   TAGGING TAGFRAM UNTAGFRAM VLANID  IDS             TYPE     DEFVLAN  VLANS
--------------------------------------------------------------------------------
4/1   disable false   false     1       1               normal   disable  M-S-P
4/2   disable false   false     1       1               normal   disable  M-S-P
4/3   enable  false   false     0       100,101,102,200 normal   disable  M-S-P
4/4   disable false   false     1       1               normal   disable  M-S-P
```

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 Avaya Virtual Services Platform 9000,* NN46250-401.

Before you begin

- For all modes, configure an IP address on the VLAN enabled with NLB.
- For IGMP-multicast mode, you must also enable IGMP snooping.
- For connectivity to a secondary virtual IP address:
  - For multicast and IGMP-multicast modes, you must complete the optional step in the following procedure to enable IP ARP Multicast MAC flooding.
  - For unicast modes, you do not need to enable IP ARP Multicast MAC flooding.

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. SPBM does not support NLB multicast or NLB multicast with IGMP.

Virtual Services Platform 9000 supports static ARP entries for NLB multicast and NLB multicast IGMP. Virtual Services Platform 9000 does not support static ARP entries for NLB unicast.

Procedure

1. Enter VLAN Interface Configuration mode:

   ```
   enable
   configure terminal
   interface vlan <1-4084>
   ```

2. Enable NLB support on an interface:

   ```
   nlb-mode unicast
   ```

   OR

   ```
   nlb-mode multicast
   ```

   OR

   ```
   nlb-mode igmp-multicast
   ```

3. Exit to Global Configuration mode:

   ```
   exit
   ```

4. **(Optional)** Enable multicast MAC flooding:

   ```
   ip arp multicast-mac-flooding
   ```

Example

Configure unicast mode for VLAN 2, and IGMP-multicast mode for VLAN 3.

```
VSP-9012:1(config)#interface vlan 2
VSP-9012:1(config-if)#nlb-mode unicast
VSP-9012:1(config-if)#exit
VSP-9012:1(config-if)#interface vlan 3
VSP-9012:1(config-if)#ip igmp snooping
VSP-9012:1(config-if)#nlb-mode igmp-mcast
```

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[-slot/port][,...]}
   ```

2. Configure a tagged port to discard untagged frames:

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

3. Discard a tagged frame on an untagged port:

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

4. Untag the default VLAN on a tagged port:

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

Example

Configure a tagged port to discard untagged frames.

```
VSP-9012:1(config-if)#untagged-frames-discard port 4/1
```

Discard a tagged frame on an untagged port.

```
VSP-9012:1(config-if)#tagged-frames-discard port 4/1 enable
```

Untag the default VLAN on a tagged port.

```
VSP-9012:1(config-if)#untag-port-default-vlan port 4/2 enable
```

Variable definitions

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

Variable	Value
[port {slot/port[-slot/port][,...]}]	Specifies the ports to change.

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 <1-4084>
   ```

Example

Enable SLPP.

```
VSP-9012:1(config)#slpp enable
```

Configure the transmission interval to 5000 milliseconds.

```
VSP-9012:1(config)#slpp tx-interval 5000
```

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

```
VSP-9012:1(config)#slpp vid 2
```

Variable definitions

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

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.
1–4084	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 6: SLPP recommended values

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

Table continues…

	Setting
Enable SLPP	
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[-slot/port][,...]}
   ```

2. Configure SLPP on a port:

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

Example

```
VSP-9012:1(config-if)#slpp port 3/1 packet-rx-threshold 5
```

Variable definitions

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

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.

Table continues…

Variable	Value
	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[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Job aid

The following table provides the Avaya recommended SLPP values.

Table 7: SLPP recommended values

	Setting
Enable SLPP	
Access SMLT	Yes
Core SMLT	No
IST	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 VLAN Interface Configuration mode:

   ```
   enable
   configure terminal
   interface vlan <1-4084>
   ```

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 <1-4084>
   ```

Example

Log on to the VLAN Interface Configuration mode.

```
VSP-9012:1(config)#interface vlan 2
```

Enable SLPP.

```
VSP-9012:1(config-if)#slpp enable
```

Configure the transmission interval to 500 milliseconds.

```
VSP-9012:1(config-if)#slpp tx-interval 500
```

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

```
VSP-9012:1(config-if)#slpp vid 2
```

Variable definitions

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

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.

Table continues…

Variable	Value
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.
1–4084	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 SLPP in an SMLT-pair recommended values.

Table 8: SLPP recommended values

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

Viewing SLPP information

Use SLPP information to view loop information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View SLPP information:

   ```
   show slpp
   ```

Example

```
VSP-9012:1#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[-slot/port][,...]}]
   ```

3. Clear SLPP packet RX counters:

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

Example

```
VSP-9012:1#show slpp interface GigabitEthernet 9/7
```

```
================================================================================
                                  Port Interface
  ==============================================================================
  PORT        PKT-RX      PKT-RX     INCOMING   SLPP PDU
  NUM                     THRESHOLD  VLAN ID    ORIGINATOR
  ------------------------------------------------------------------------------
  9/7         enabled     5

  PORT        PKT-RX      TIME LEFT
  NUM         COUNT       TO CLEAR RX COUNT
  ------------------------------------------------------------------------------
  9/7         29          21600
```

Variable definitions

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

Variable	Value
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots

Variable	Value
	and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Configuring VLAN loop detection

Configure the loop detection to detect the MAC addresses that are looping from one port to another port. After a loop is detected, the port on which the MAC addresses are learned is disabled or if a MAC address is found to loop, the MAC address is disabled for that VLAN. If arp-detect is enabled, then Layer 3 loops can be detected.

Before you begin

- On routed interfaces, you must activate ARP-Detect with loop detect.

About this task

Important:

The loop detection feature is only enabled on SMLT ports. The loop detection feature is not used on IST ports, on core full-meshed, or on square SMLT ports. If you attempt to enable loop-detect on an existing IST port, the system prevents you from doing so. However, if you have a port with loop-detect already enabled, and you add that port to an IST, the system does not prevent you from doing so, which can cause potential system errors.

A different way to detect loops is to use Simple Loop Prevention Protocol (SLPP) to detect VLAN loops.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

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

2. Configure loop detection:

   ```
   loop-detect
   ```

3. Specify the loop-detect action to take:

   ```
   loop-detect{mac-discard|port-down}
   ```

4. **(Optional)** Configure loop detection to default:

   ```
   default loop-detect [arp-detect]
   ```

5. **(Optional)** Disable loop detection

   ```
   no loop-detect [arp-detect]
   ```

6. Enable ARP loop detection:

```
loop-detect arp-detect
```

7. Configure the interval at which to monitor MAC addresses:

   ```
   mac-flap-time-limit <10-5000>
   ```

8. Display loop-detect configurations:

   ```
   show ip arp interface [gigabitethernet {slot/port[-slot/port]
   [,...]}][vlan <1-4084>]
   ```

Example

Configure loop detect to determine if the same MAC address appears on different ports and activate ARP-Detect to detect Layer 3 loops. Specify the time limit for MAC flapping to 200 milliseconds.

```
VSP-9012:1(config)#interface GigabitEthernet 4/2
VSP-9012:1(config-if)#loop-detect action mac-discard arp-detect
VSP-9012:1(config-if)#exit
VSP-9012:1(config)#mac-flap-time-limit 200
VSP65:1(config)#show ip arp interface gigabitethernet 4/2

================================================================================
                                  Port Arp
================================================================================
PORT_NUM DOPROXY    DORESP
--------------------------------------------------------------------------------
4/2      false      true


================================================================================
                                Loop Detect
================================================================================
PORTNUM                Loop Detect              Action           Arp Detect
--------------------------------------------------------------------------------
4/2                     enable                 port-down         enable
```

Variable definitions

Use the data in the following table to use optional parameters with the **`loop-detect`** command.

Variable	Value
action {mac-discard|port-down}	Specifies the loop detect action to be taken: • mac-discard **Note:** ARP-Detect does not support this action. • port-down — Shuts down the port if the system detects a flapping MAC address
arp-detect	Enables ARP-Detect. The Address Resolution Protocol (ARP)-detect feature is used for IP configured interfaces for ARP packets. Enable this feature (in addition to loop detect) on routed interfaces.

Use the data in the following table to use the **mac-flap-time-limit** command.

Variable	Value
10–5000	Specifies the time limit, in milliseconds, for MAC flapping. The default value is 500.

Job aid

The following log message and trap is generated after MAC address discarding is configured due to loop-detect:

```
MAC has been disabled due to MAC <xx:xx:xx:xx:xx:xx> flapping more than <n> times in <t>
milliseconds from <port-number> to <port-number>.
```

The following log message and trap is generated after a port, which the system disabled due to CP-Limit or link-flap, is auto-recovered:

```
port <port-num> re-enabled by auto recovery
```

The following log message and trap is generated after a port which the system disabled due to the loop detection feature is auto-recovered:

```
Loop detect action <action> cleared on port <port-num> by auto recovery
```

Configuring spoof detection

Configure spoof detection to prevent IP spoofing.

For more information about this feature, see Prevention of IP spoofing within a VLAN on page 30.

Before you begin

Important:

If you use SMLT, configure spoof detection on both SMLT aggregation devices to avoid connectivity issues.

Restart the device to enable the spoof detection feature.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

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

2. Enable or disable spoof detection:

```
spoof-detect [port {slot/port[-slot/port][,...]}] [enable]
no spoof-detect [port {slot/port[-slot/port][,...]}] [enable]
```

3. Enable or disable auto-recovery on a port:

```
auto-recover-port [port {slot/port[-slot/port][,...]}] [enable]
no auto-recover-port [port {slot/port[-slot/port][,...]}] [enable]
```

Example

Enable spoof detection.

```
VSP-9012:1(config-if)#spoof-detect port 4/1 enable
```

Enable autorecovery on a port.

```
VSP-9012:1(config-if)#auto-recover-port port 4/1 enable
```

Variable definitions

Use the data in the following table to use optional parameters with the **spoof-detect** command.

Variable	Value
enable	Enables spoof detection on the port.
{slot/port[-slot/port][,...]}	Specifies the port list.

Configuring multiple DSAP and SSAP

Configure multiple Destination Service Access Points (DSAP) and Source Service Access Points (SSAP) to create a protocol-based VLAN.

About this task

You can assign multiple Protocol Identifier (PID) or DSAP/SSAP for a protocol VLAN configured with a user-defined PID value. It is also allowed for SNA 802.2. protocol VLAN. It is not valid for any other types of VLANs.

Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <1-4084>
```

2. Configure multiple DSAP and SSAP:

```
dsapssap <0x0-0xffff|0x0-0x0>
```

Example

```
VSP-9012:1(config)#interface vlan 7
```

Configure a protocol VLAN configured with a user-defined PID value.

```
VSP-9012:1(config-if)#vlan create 7 type protocol-mstprstp 0 userDefined 0x8010 encap llc
```

Configure multiple DSAP and SSAP.

```
VSP-9012:1(config-if)#dsapssap 0x1234
VSP-9012:1(config-if)#dsapssap 0x3456
```

Variable definitions

Use the data in the following table to use **dsapssap** command.

Variable	Value
<0x0-0xffff|0x0–0x0>	A table used to maintain DSAP/SSAP values assigned to a sna802dot2 or user defined VLAN.

Viewing VLAN information

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

The **show vlan basic** command only shows full VLAN names of up to 15 characters, and the **show vlan advance** command only shows full VLAN names of up to nine characters. Larger names for the **show vlan advance** and **show vlan basic** commands show the first part of the name, followed by a tilda symbol (~). To see the full VLAN name, use the **show vlan name** command, which displays names up to 64 characters in length.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View VLAN information:

   ```
   show vlan basic [<1-4084>]
   ```

3. View advanced parameters:

   ```
   show vlan advance [<1-4084>]
   ```

4. View the full VLAN name:

   ```
   show vlan name [<1-4084>]
   ```

Example

View VLAN information for VLAN 2.

```
Switch:1>enable
Switch:1(config)#show vlan basic 2

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

--------------------------------------------------------------------------------
2     VLAN-2            byPort      1   none       N/A             N/A
```

View VLAN information:

```
Switch:1(config)#show vlan basic

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

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

2     VLAN-2            byPort      1   none       N/A             N/A

3     AdministrationB~ byPort       62  none       N/A             N/A

20    VLAN-20           byPort      0   none       N/A             N/A

21    VLAN-21           byPort      0   none       N/A             N/A

22    VLAN-22           byPort      0   none       N/A             N/A

23    VLAN-23           byPort      0   none       N/A             N/A

24    VLAN-24           byPort      0   none       N/A             N/A

25    VLAN-25           byPort      0   none       N/A             N/A

26    VLAN-26           byPort      0   none       N/A             N/A

27    VLAN-27           byPort      0   none       N/A             N/A

28    VLAN-28           byPort      0   none       N/A             N/A

29    VLAN-29           byPort      0   none       N/A             N/A

30    VLAN-30           byPort      0   none       N/A             N/A

31    VLAN-31           byPort      0   none       N/A             N/A

32    VLAN-32           byPort      0   none       N/A             N/A


--More-- (q = quit)
```

View advanced parameters.

```
Switch:1(config)#show vlan advance 3

================================================================================
                                  Vlan Advance
================================================================================
VLAN             IF    AGING MAC                USER
ID    NAME       INDEX TIME  ADDRESS            DEFINEPID ENCAP  DSAP/SSAP
--------------------------------------------------------------------------------
3     Administr~ 2051  0     00:00:00:00:00:00  0x0000
```

View full VLAN names:

```
Switch:1(config)#show vlan name

================================================================================
                                   Vlan Name
================================================================================
VLAN  IF
ID    INDEX NAME
--------------------------------------------------------------------------------
1     2049  Default
2     2050  VLAN-2
3     2051  AdministrationBuildingThirdFloorComputerLab
20    2068  VLAN-20
21    2069  VLAN-21
22    2070  VLAN-22
23    2071  VLAN-23
24    2072  VLAN-24
25    2073  VLAN-25
26    2074  VLAN-26
27    2075  VLAN-27
28    2076  VLAN-28
29    2077  VLAN-29
30    2078  VLAN-30
31    2079  VLAN-31
32    2080  VLAN-32

--More-- (q = quit)
```

Variable definitions

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

Variable	Value
<1-4084>	Specifies the VLAN ID in a range of 1–4084. VLAN IDs 1 to 4084 are configurable. VLAN IDs 4085-4094 are reserved for internal use.

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. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View brouter port information:

   ```
   show vlan brouter-port
   ```

Example

View brouter port information.

```
VSP-9012:1(config)#show vlan brouter-port
```

```
            Vlan Id         Port       VrfId
          ========        =====      ======
             2202         3/11       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. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View VLAN port member status:

   ```
   show vlan members [<1-4084>][null-vlan][port {slot/port[-slot/port]
   [,...]}]
   ```

Example

View VLAN port member status.

```
VSP-9012:1(config)#show vlan members port 3/2
```

```
================================================================================
                                  Vlan Port
================================================================================
VLAN PORT               ACTIVE             STATIC             NOT_ALLOW
ID   MEMBER             MEMBER             MEMBER             MEMBER
--------------------------------------------------------------------------------
2    3/2,3/5-3/8,3/11,  3/2,3/5-3/8,3/11,
```

```
     3/14,3/26,3/38     3/14,3/26,3/38

3    3/2,3/5-3/8,3/14,  3/2,3/5-3/8,3/14,
     3/26,3/38          3/26,3/38

4    3/1-3/2,3/5-3/8,   3/1-3/2,3/5-3/8,
     3/13-3/14,3/25-    3/13-3/14,3/25-
     3/26,3/37-3/38     3/26,3/37-3/38

100  3/2,3/14,3/23-     3/2,3/14,3/23-
     3/24,3/26-3/28,    3/24,3/26-3/28,
     3/38               3/38

300  3/2,3/5-3/8,3/14,  3/2,3/5-3/8,3/14,
     3/26,3/38          3/26,3/38
================================================================================
                           Ospf Passive Port Members
================================================================================
VLAN PORT NUM
--------------------------------------------------------------------------------
2

3

4

100

300
```

Variable definitions

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

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.
port {slot/port[-slot/port][,...]}	Specifies the port or range of ports.

Table continues…

Variable	Value
	Important: Entering a port {slot/port[-slot/port][,...]} is optional. If you enter a port {slot/port[-slot/port][,...]}, the command shows information for the port. Without the port {slot/port[-slot/port][,...]}, the command shows information for all the ports.
<1-4084>	Specifies the VLAN ID in the range of 1–4084. VLAN IDs 1 to 4084 are configurable. VLAN IDs 4085-4094 are reserved for internal use. **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 source MAC addresses

View the VLAN source MAC addresses to display the source MAC address for a source MAC-based VLAN on the device or for the specified VLAN.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View VLAN source MAC addresses:

   ```
   show vlan src-mac [<1-4084>]
   ```

Example

View VLAN source MAC addresses.

```
VSP-9012:1(config)#show vlan src-mac
```

```
================================================================
                      Vlan Srcmac
================================================================
VLAN_ID    MAC_ADDRESS
----------------------------------------------------------------
10         00:00:00:00:00:11

All 1 out of 1 Total Num of Vlan Srcmac Entries displayed
```

Variable definitions

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

Variable	Value
<1-4084>	Specifies the VLAN ID for the source MAC-based VLAN. The value ranges from 1–4084. VLAN IDs 1 to 4084 are configurable. VLAN IDs 4085-4094 are reserved for internal use. **Important:** The entry of a VLAN ID is optional. After 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 configured source MAC 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. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View VLAN forwarding database information:

   ```
   show vlan mac-address-entry [<1-4084>]
   ```

Example

View VLAN forwarding database information:

```
VSP-9012:1(config)# show vlan mac-address-entry
================================================================================
                            Vlan Fdb
================================================================================
VLAN            MAC                             SMLT
ID   STATUS     ADDRESS            INTERFACE    REMOTE TUNNEL
--------------------------------------------------------------------------------
1    mgmt       00:00:00:00:00:01  Port-4/1     false  -

1 out of 1 entries in all fdb(s) displayed.
```

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

```
VSP-9012:1(config)#show vlan mac-address-entry spbm-tunnel-as-mac
```

```
================================================================================
                                    Vlan Fdb
================================================================================
VLAN            MAC                             SMLT
ID   STATUS     ADDRESS            INTERFACE    REMOTE TUNNEL
--------------------------------------------------------------------------------
7    self       00:24:7f:9f:6a:04  Port-cpp     false  -
10   self       00:24:7f:9f:6a:00  Port-cpp     false  -

2 out of 2 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.

Variable	Value
<1-4084>	Specifies the VLAN ID in a range of 1–4084. VLAN IDs 1 to 4084 are configurable. VLAN IDs 4085-4094 are reserved for internal use.
mac <0x00:0x00:0x00:0x00:0x00:0x00:0x00>	Specifies the MAC address.
port {slot/port[-slot/port][,...]}	Specifies the port or port list.
spbm-tunnel-as-mac	Displays where entries are learned. The TUNNEL column indicates where in the SPBM network an entry is learned.

Viewing manual edit MAC addresses

Use the procedure to view the list of manual edit MAC addresses and the associated ports configured as allow-mac for MAC security.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View manual edit MAC addresses:

   ```
   show vlan manual-edit-mac
   ```

Example

View manual edit MAC addresses.

```
VSP-9012:1(config)#show vlan manual-edit-mac
```

```
================================================================
                        Manual Edit Mac
================================================================
MAC ADDRESS        PORTS
----------------------------------------------------------------
00:00:00:00:00:55  4/3
00:00:00:00:00:66  4/3

All 2 out of 2 Total Num of Manual Edit Mac Entries displayed
```

Viewing multicast MAC addresses

Use the procedure to view the multicast MAC addresses for all VLANs on the device or for the specified VLAN.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View multicast MAC addresses:

   ```
   show vlan static-mcastmac [<1-4084>]
   ```

Example

Add a Multicast MAC to a VLAN.

```
VSP-9012:1(config)#vlan static-mcastmac 1 0x81:0x00:0x00:0x00:0x00:0x22 4/5
VSP-9012:1(config)#vlan static-mcastmac 1 0x81:0x00:0x00:0x00:0x00:0x23 4/5
```

View multicast MAC addresses.

```
VSP-9012:1(config)#show vlan static-mcastmac
```

```
================================================================================
                                 Vlan Mcastmac
================================================================================
VLAN_ID    MAC_ADDRESS          PORT_LIST                     MLT_GROUPS
--------------------------------------------------------------------------------
1          81:00:00:00:00:23    4/5                           N/A
1          81:00:00:00:00:22    4/5                           N/A

Total Entries: 2
```

Variable definitions

Use the data in the following table to use the **`show vlan static-mcastmac`** command.

Variable	Value
<1-4084>	Specifies the VLAN ID in a range of 1–4084. VLAN IDs 1 to 4084 are configurable. VLAN IDs 4085-4094 are reserved for internal use.

Viewing NLB-mode information

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View NLB-mode information:

   ```
   show interface vlan nlb-mode<1-4084>
   ```

Example

View NLB-mode information.

```
VSP-9012:1(config)#show interface vlan nlb-mode
```

```
================================================================================
                                    Vlan Nlb
================================================================================
VLAN_ID  NLB_ADMIN_MODE NLB_OPER_MODE  PORT_LIST       MLT_GROUPS
--------------------------------------------------------------------------------
2        unicast        disable
3        igmp-mcast     disable

Total Entries: 2
```

Variable definitions

Use the data in the following table to use optional parameters with the **`show interface vlan nlb-mode`** command.

Variable	Value
<1-4084>	Specifies the VLAN ID in a range of 1–4084.

Viewing port-level MAC security

View port-level MAC security to review the configuration.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View port-level MAC security for unknown-discard:

   ```
   show interface gigabitethernet mac-security [{slot/port[-slot/port][,...]}]
   ```

3. View port-level MAC security for limit-learning:

   ```
   show interface gigabitethernet limit—fdb—learning [{slot/port[-slot/port][,...]}]
   ```

Example

View port-level MAC security for unknown-discard.

```
VSP-9012:1(config-if)#show interfaces gigabitEthernet mac-security 4/1-4/2
```

```
================================================================================
                            Port Unknown-Mac-Discard
================================================================================
PORT  ACTI    AUTO    AUTOLN   LOCK    DOWN            SEND    MAXMAC CURMAC
NUM   VATION  LEARN   MODE     AUTOLN  PORT    LOG     TRAP    COUNT  COUNT
--------------------------------------------------------------------------------
4/1   disable disable one-shot disable disable enable  disable 2048   0
4/2   enable  enable  one-shot disable disable enable  disable 200    0

PORT NUM  ALLOW-MAC         MANUAL/AUTO
--------------------------------------------------------------------------------
```

View port-level MAC security for limit-learning.

```
VSP-9012:1(config)#show interface gigabitethernet limit—fdb—learning 4/4-4/5
```

```
================================================================
                            Port limit-fdb-learning
================================================================
PORT  FDB      MAXMAC  MINMAC  LOG     PORT    CURMAC  MAC
NUM   PROTECT  COUNT   COUNT   TRAP    DOWN    COUNT   LEARN
----------------------------------------------------------------
4/4   dis      1024    512     dis     dis     0       true
4/5   ena      5000    3000    dis     dis     0       true
```

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 loop detection, select **LoopDetect**.
11. To enable the ARP loop detection feature on this port, select **ARPDetect**.
12. To specify the action that needs to be taken after a MAC loop is detected on a specific port, select **portDown** or **macDiscard**.

    Important:

    You can only use this feature if you also select **LoopDetect**.
13. In the Classification area, select the types of VLAN to enable.

14. Click **Apply**.
15. 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.
LoopDetect	Enables loop detection. The default is disabled.
ArpDetect	Enables or disables Address Resolution Protocol (ARP) detection on this port, if Loop Detect is checked. The default is disabled.
LoopDetectAction	Specifies the action to be taken after a loop is detected on a specific port. Options are portDown and macDiscard. The default is portDown.
SpoofDetect	Enables or disables Spoof Detect on a particular port. The default value is false.
SourceMac	Enables source MAC-based VLAN on the port. The default is enabled.
Subnet	Enables subnet-based VLAN on the port. The default is enabled.

Table continues…

Name	Description
Protocol	Enables protocol-based VLAN on the port. This feature is always enabled.
Prec	Configures the precedence for VLAN classification: either sourceMac or subnet. The default value is sourceMac.

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.

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 source IP subnet-based VLAN on page 79
- Creating a protocol-based VLAN on page 81
- Configuring user-defined protocol-based VLANs on page 82
- Configuring a source MAC address-based VLAN on page 84
- Creating an SPBM B-VLAN on page 86

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**.
13. Collapse the **VLANs** tab.

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

Basic field descriptions

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

Name	Description
Id	Specifies the VLAN ID for the VLAN.
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 • byIpSubnet • byProtocolId • bySrcMac • 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.

Table continues…

Name	Description
NotAllowToJoin	Specifies the slot/ports that are never allowed to become a member of the policy-based VLAN.
OspfPassiveMembers	Specifies the slot/ports of each Open Shortest Path First (OSPF) passive member.
ProtocolId	Specifies the network protocol for protocol-based VLANs. This value is taken from the Assigned Numbers of remote function call (RFC). • ip (IP version 4) • ipx802dot3 (Novell Internetwork Packet Exchange (IPX) on Ethernet 802.3 frames) • ipx802dot2 (Novell IPX on IEEE 802.2 frames) • ipxSnap (Novell IPX on Ethernet Standard Network Access Protocol (SNAP) frames) • ipxEthernet2 (Novell IPX on Ethernet Type 2 frames) • appleTalk [AppleTalk on Ethernet Type 2 and Ethernet Symbolic Network Analysis Program (SNAP) frames] • decLat (Digital Equipment Corporation Local Area Transport (DEC LAT) protocol) • decOther (Other DEC protocols) • sna802dot2 (IBM SNA on IEEE 802.2 frames) • snaEthernet2 (IBM SNA on Ethernet Type 2 frames) • netBIOS (NetBIOS protocol) • xns (Xerox XNS) • vines (Banyan VINES) • ipv6 (IP version 6) • usrDefined (user-defined protocol) • rarp (Reverse Address Resolution Protocol) • PPPoE (Point-to-Point Protocol over Ethernet) If the VLAN type is port-based, none is displayed in the Basic tab ProtocolId field.
SubnetAddr	Specifies the source IP subnet address (IP subnet-based VLANs only).
SubnetMask	Specifies the source IP subnet mask (IP subnet-based VLANs only).

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.)

Configuring an IP address for a VLAN

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

Table continues…

Name	Description
ReasmMaxSize	Shows the size of the largest IP datagram which this entity can reassemble from incoming IP fragmented datagrams received on this interface.
VlanId	Shows the VLAN ID associated with this entry.
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 source IP subnet-based VLAN

Create a source IP subnet-based VLAN so that a potential member becomes an active member of the VLAN if a frame is received from the specified source IP address.

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 VLAN ID.
5. In the **Name** box, type the VLAN name.

   If a name is not entered, a default name is created.
6. In the **Color Identifier** box, select a 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 **byIpSubnet**.

   The fields needed to configure IP subnet-based VLANs are activated.
9. To specify the VLAN port membership, click the ellipsis button **(...)** for one of the following fields:

   PortMembers

   OR

   StaticMembers

   OR

   NotAllowToJoin
10. Click on each port to choose the desired color:

    Yellow—Potential members

    or

    Green—Always members, static

    or

    Red—Never members, not allowed to join

    Important:

    In a source IP subnet-based VLAN, a potential member becomes an active member of the VLAN after a frame is received from an address on the specified IP network.
11. Click **OK**.
12. In the **SubnetAddr** box, enter an IP address for the VLAN.
13. In the **SubnetMask** box, enter an IP subnet mask for the VLAN.
14. In the **AgingTime** box, enter the timeout period in seconds for aging out the dynamic VLAN member ports or use the default.

15. Click **Insert**.
16. Collapse the **VLANs** tab.

    The subnet-based VLAN is added to the **Basic** tab.

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 for a Virtual Services Platform 9000, a potential member becomes an active member of the VLAN after a frame of the specified protocol is received.

11. Click **OK**.
12. In the **ProtocolId** box, select a protocol ID.
13. In the **AgingTime** box, specify the timeout period, in seconds, for aging out the dynamic member ports of the VLAN or use the default.
14. Click **Insert**.
15. Collapse the **VLANs** tab.

    The protocol-based VLAN is added to the **Basic** tab.

Configuring user-defined protocol-based VLANs

Configure user-defined protocol-based VLANs to support the networks with nonstandard protocols.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. On the **Basic** tab, click **Insert**.
4. In the **Name** box, type the VLAN name.

   If a name is not entered, a default name is created.
5. In the **Color Identifier** box, select a color or use the color provided.

   This color is used to visually distinguish the VLANs in a network.
6. In the **Type** box, select **byProtocolId**.
7. To specify the VLAN port membership, click the button **(...)** for one of the following fields:

   Port Members

   OR

   StaticMembers

   OR

   NotAllowedToJoin
8. Click each port button to achieve the desired membership color:

   Yellow: Potential members—dynamic.

OR

Green: Always members—static

OR

Red: Never members—not allowed to join

Important:

In a user-defined protocol-based VLAN on a Virtual Services Platform 9000 module, a potential member becomes an active member after a frame from the specified protocol is received.

9. In the **ProtocolId** box, select **usrDefined**.
10. In the **UserDefinedPid** box, enter the protocol ID for the protocol in the format 0x (protocol type in hexadecimal).

    Important:

    In Virtual Services Platform 9000 modules, the 16-bit Protocol Identifier (PID) assigned to a protocol-based VLAN specifies either an Ethertype, a Destination Service Access Point (DSAP)/Source Service Access Point (SSAP), or a Sub-Network Access Protocol (SNAP) PID, depending on whether the frame encapsulation is Ethernet 2, 802.2, or LLC-SNAP, respectively.

    The following PIDs are not valid:

    - PID0x0000 through 0x05dc: overlaps with the 802.3 frame length
    - PIDs of predefined protocols (for example, IP, IPX, AppleTalk)
    - PID 0x8100: reserved by 802.1Q to identify tagged frames
    - PID0x9000: used by the diagnostic loopback frames
    - PID0x8808: used by 802.3x pause frames
    - PID0x4242: overlaps with the BPDU DSAP/SSAP
11. Select the encapsulation method in the **Encap** field.
12. In the **AgingTime** box, specify the timeout period, in seconds, for aging out the dynamic member ports of the VLAN or use the default.
13. Click **Insert**.
14. Collapse the **VLANs** tab.

    The protocol-based VLAN is added to the **Basic** tab.

Configuring a source MAC address-based VLAN

Use source MAC-based VLANs to associate a packet with a VLAN if the source MAC address is one of the MAC addresses explicitly associated with the VLAN.

Before you begin

- Verify that source MAC VLAN is enabled for each port that is to be a member of a source MAC VLAN.

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 a unique VLAN ID.
5. In the **Name** box, type the VLAN name or use the default name.
6. In the **Color Identifier** box, select a color or use the default color.

   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 **bySrcMac**.

   The fields you require to configure the source MAC-based VLANs become active.
9. To specify the VLAN port membership, click the ellipsis button **(...)** for one of the following fields:

   PortMembers

   OR

   StaticMembers

   OR

   NotAllowToJoin
10. In the **AgingTime** box, specify the timeout period in seconds for aging out the dynamic member ports of the VLAN or use the default of 600 seconds.
11. Click **Insert**.
12. On the **Basic** tab, select the newly created VLAN.
13. Click **Mac**.
14. Click **Insert** on the VLAN MAC tab.
15. In the **MacAddr** box, specify a source MAC address for the VLAN.
16. Click **Insert**.
17. Collapse the **MAC, VLAN** tab.

Important:

In a source MAC-based VLAN, a potential member becomes an active member of the VLAN after the system receives a frame with the specified source MAC address.

Configuring source MAC addresses for a source MAC-based VLAN

Create a source MAC address for an existing source MAC VLAN.

Before you begin

- Configure the VLAN.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. In the **Basic** tab, select a source MAC address-based VLAN.
4. Click **Mac**.
5. To manually insert a MAC address, click **Insert**, and then enter it in the form nn:nn:nn:nn:nn:nn.

   OR
6. To add a MAC address from a file, select **File**, **Add From File**.
7. Use the selection box to browse for the file location.
8. To save a MAC address to a file, select it, select **File**, **Save to File**, and then use the selection box to browse for a save location.
9. To delete a MAC address, select it, and then select **Delete Members On Device**.
10. Click **Yes**.
11. Click **Close**.

    The Edit MAC box closes.

VLAN MAC field descriptions

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

Name	Description
MacAddr	Specifies the MAC addresses associated with this VLAN.

Creating an SPBM B-VLAN

Create a Shortest Path Bridging MAC (SPBM) Backbone VLAN (B-VLAN).

Note:

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

About this task

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:

SPB internally uses spanning tree group (STG) 63 or Multiple Spanning Tree Instance (MSTI) 62. STG 63 or MSTI 62 cannot be used by another VLAN or MSTI. For non-SPB customer networks, if you use STG 63 or MSTI 62 in the configuration, you must delete STG 63 or MSTI 62 before you can configure SPBM.

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, QoS level, and NLB mode. 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.
Name	Specifies the name of the VLAN.
IfIndex	Specifies the logical interface index assigned to the VLAN.
Type	Specifies the type of VLAN: • byPort • byIpSubnet • byProtocolId • bySrcMac • spbm-bvlan
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. This value is taken from the Assigned Numbers RFC: • ip (IP version 4) • ipx802dot3 (Novell IPX on Ethernet 802.3 frames) • ipx802dot2 (Novell IPX on IEEE 802.2 frames) • ipxSnap (Novell IPX on Ethernet SNAP frames) • ipxEthernet2 (Novell IPX on Ethernet Type 2 frames) • appleTalk (AppleTalk on Ethernet Type 2 and Ethernet SNAP frames) • decLat (DEC LAT protocol) • decOther (Other DEC protocols) • sna802dot2 (IBM SNA on IEEE 802.2 frames)

Table continues…

Name	Description
	• snaEthernet2 (IBM SNA on Ethernet Type 2 frames) • netBIOS (NetBIOS protocol) • xns (Xerox XNS) • vines (Banyan VINES) • ipv6 (IP version 6) • usrDefined (user-defined protocol) • RARP (Reverse Address Resolution protocol) • PPPoE (Point-to-point protocol over Ethernet) If the VLAN type is not protocol-based, None is displayed in the Basic tab ProtocolId field.
Encap	Specifies the encapsulation method. Values are: • Ethernet II • SNAP — SubNetwork Access Protocol (SNAP) • LLC — IEEE 802.2 Logic Link Control (LLC) This is the encapsulation type for user-defined protocol-based VLANs. The **Encap** option is not meaningful for other types of VLAN. By default, there is no encapsulation method configured for the VLAN.
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.
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, ARP replies, or Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) frames.
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.

Table continues…

Name	Description
	• 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. • flushSnoopMemb: This action is not supported. • triggerRipUpdate: Configures action to triggerRipUpdate. After you execute this command the Virtual Services Platform 9000 immediately sends a RIP request to solicit the updated RIP routes. • flushSnoopMRtr: This action is not supported. The default is none.
Result	Specifies the result code after you perform an action.
UserDefinedPid	Specifies the 16-bit user-defined network protocol identifier of a protocol-based VLAN with User Defined protocol.
NlbMode	Specifies if the NLB administrative privileges are enabled or disabled. The default value is disable.

Configuring NLB support

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 Avaya Virtual Services Platform 9000,* NN46250-401.

Before you begin

- The VLAN exists and has an associated IP address.
- For IGMP-multicast mode, you must also enable IGMP snooping.
- For connectivity to a secondary virtual IP address:
  - For multicast and IGMP-multicast modes, you must complete the optional step in the following procedure to enable IP ARP multicast MAC flooding
  - For unicast modes, you do not need to enable IP ARP multicast MAC flooding

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. SPBM does not support NLB multicast or NLB multicast with IGMP.

Virtual Services Platform 9000 supports static ARP entries for NLB multicast and NLB multicast IGMP. Virtual Services Platform 9000 does not support static ARP entries for NLB unicast.

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**.
7. Collapse the **VLANs** tab.

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 9: SLPP recommended values

	Setting
Enable SLPP	
Access SMLT	Yes
Core SMLT	No
IST	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. Click the ellipsis button to select from a list of VLANs.
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 10: SLPP recommended values

	Setting
Enable SLPP	
Access SMLT	Yes
Core SMLT	No
IST	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 VLAN loop detection

Configure loop detect to determine if the same MAC address appears on different ports. Use the optional ARP-Detect feature to account for ARP packets on IP configured interfaces.

About this task

Configure loop detection to detect the MAC addresses that loop from one port to another port. After a loop is detected, the port on which the MAC addresses are learned is disabled or if a MAC address is found to loop, the MAC address is disabled for that VLAN.

Important:

The loop detection feature is only enabled on SMLT ports. The loop detection feature is not used on IST ports, on core full-meshed or on square SMLT ports.

A different way to detect loops is to use Simple Loop Prevention Protocol (SLPP) to detect VLAN loops.

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. Check the **LoopDetect** check box to enable the LoopDetectAction options.
6. If required, select the **ArpDetect** check box.
7. In the **LoopDetectAction** box, select the action to be taken if a loop is detected.

   Important:

   If **portDown** is selected, the access switch recovers by detecting the failed link. If **macDiscard** is selected, the MAC address that was learned on multiple ports is disabled. If desired, enable **ArpDetect**. If **ArpDetect** is enabled, then Layer 3 loops can be detected.
8. Click **Apply**.
9. To view the loop detection status for a port in a VLAN, click **LoopDetect**.
10. Click **Close**.

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 a VLAN.
4. Click **IP**.
5. Click the **Direct Broadcast** tab.
6. Select **DirectBroadcastEnable**.

   Important:

   Configure multiple VLANs or IPs in the same subnet but in different systems simultaneously.
7. 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 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. This feature is enabled by default. With the feature enabled, the Control Processor (CP) module 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

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

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 **FdbAging** tab.
6. Type an interval, in seconds, for aging out dynamically learned forwarding information, or keep the default.
7. 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 (in seconds) used for aging out FDB entries of this VLAN. The default is 600.

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.
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 0 indicates a self-assigned MAC address.
SmltRemote	Specifies if the VLAN is a SMLT remote.
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 a specific VLAN 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.

Forwarding field descriptions

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

Name	Description
VlanId	Specifies the ID of the VLAN.
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 0 indicates a self-assigned MAC address.
SmltRemote	Specifies whether this is an SMLT VLAN.
BMac	Shows the backbone MAC address if the entry is learned from a Shortest Path Bridging MAC (SPBM) network.

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

Clear learned MAC addresses for all VLANs by port 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 a VLAN.
4. Click **Bridge**.
5. In the Bridge, VLAN tab, click the **Static** tab.
6. Click **Insert**.
7. In the **MacAddress** box, enter a forwarding destination MAC address.
8. In the **Port** box, click the ellipsis button **(...)**.
9. Select the port on which the frame is received.
10. Click **Ok**.
11. 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.
Status	Specifies the status of the VLAN.

Configuring static multicast for a bridge

Configure static multicast for a bridge to add a multilink trunk.

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 **Multicast** tab.
6. Click **Insert**.
7. In the **Address** box, enter the source MAC address for the VLAN.
8. Click the ellipsis **(...)** button beside **ForwardingPorts** to select the required ports.
9. Click the ellipsis **(...)** button beside **MltIds** to select the required MLT.
10. Click **Insert**.

Multicast field descriptions

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

Name	Description
VlanId	Specifies the VLAN ID.

Table continues…

Name	Description
Address	Specifies the source MAC address.
ForwardingPorts	Specifies the ports that forward the source MAC address.
MltIds	Specifies a list of MLTs to which this MAC address is forwarded.
NumMltIds	Specifies the number of MLT IDs.

Enabling global MAC security

Enable global MAC security to filter out (drop) packets that contains certain MAC addresses as source or destination globally on the switch. Configure a set of MAC addresses. The system drops a packet that contains one of these configured MAC addresses as source or destination.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **Global Mac Filtering**.
3. Click the **Mac Filter** tab.
4. Click **Insert**.
5. Type the address.
6. Click **Insert**.

Mac Filter field descriptions

Use the data in the following use the **Mac Filter** tab

Name	Description
GlobalMacFilterAddress	Specifies a MAC address that the switch discards globally.

Configuring multiple DSAPs and SSAPs

Configure multiple Destination Service Access Points (DSAP) and Source Service Access Points (SSAP) to add a VLAN to the DSAP for each port.

Before you begin

- Create a user-defined or an sna802.2 VLAN before performing the following procedure.

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. Select the VLAN to which you want to add a DSAP and click **DSAP/SSAP**.
5. Click **Insert**.
6. Enter a DSAP/SSAP value in hexadecimal form.
7. Click **Insert**.

DSAP/SSAP field descriptions

Use the data in the following table to use the **DSAP/SSAP** tab.

Name	Description
VlanID	Specifies the VLAN ID.
DSAP/SSAP	Specifies a DSAP or SSAP value.

Enabling unknown MAC discard

After you configure a port with UnknownMacDiscard enabled, the port drops packets with unknown source MAC addresses.

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 **Interface** tab.
5. Select **UnknownMacDiscard**.
6. Click **Apply**.

Configuring MAC learning parameters

Configure MAC learning parameters to control high-security environments that restrict access to the network. This feature is based on the Layer 2 MAC address of the network devices connected to the Avaya Virtual Services Platform 9000.

Before you begin

- To use MAC learning features, you must enable UnknownMacDiscard on the port.

About this task

After you configure a port with UnknownMacDiscard enabled, the port drops packets with unknown source MAC addresses. Use the auto-learning feature to configure the number of unknown MAC addresses to learn on a port. Use the allow MAC learning feature to permit forwarding of packets from specific source MAC addresses for specific ports.

Configure auto-learning so the system processes packets with an unknown MAC address. You configure the number of address the system learns by configuring a maximum number of addresses.

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 **MAC Learning** tab.
5. Configure the parameters as required.
6. Click **Apply**.

MAC Learning field descriptions

Use the data in the following table to use the **MAC Learning** tab.

Name	Description
AutoLearnEnable	Configures the port to auto-learn addresses for the allowed MAC table. You must enable auto-learn for the remainder of the configuration on this tab to apply. The default is disabled.
AutoLearnMode	Configures the auto-learn mode on the port for populating the allowed MAC table. The default value is one-shot.
AutoLearnTableMode	Configures the allowed MAC table to the current state. If you configure this parameter to locked, no new MAC addresses are learned. The default is unlock.

Table continues…

Name	Description
LogViolations	Enables the system to create a system log entry after a disallowed MAC address attempts to send traffic through the selected port. The default value is enable.
SendTrap	Indicates whether a trap is sent to the management station after a MAC address violation is detected on the selected port. The default is disable.
DisablePort	Indicates whether the selected port is disabled if a MAC address violation is detected. Enable means that the port is disabled if this event occurs. The default is disable. The default is disable.
MacCountMax	Specifies the maximum number of MAC addresses that can be added to the selected port. The valid values are 0 to 2048. The default is 2048.
MacCountCur	Specifies the current number of MAC addresses added to the selected port. The default is 0.

Configuring MAC address learning

Configure MAC address learning on a port to limit traffic on that port to data to and from specific MAC addresses. This configuration only applies to ports configured with MAC learning auto-learn enabled. Specify the MAC addresses that can be learned.

Before you begin

- You must enable auto-learn.
- The allow-mac and auto-learning attributes are part of the unknownMacDiscard feature at the port level. These attributes take effect only if you enable unknownMacDiscard for the port.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **MAC Security**.
3. Click the **Allow MAC** tab.
4. Click **Insert**.
5. In the **Address** box, enter the source MAC address.
6. In the **Ports** box, click the ellipsis button **(...)**.
7. Select the ports you want to configure.
8. Click **Ok**.
9. Click **Insert**.

Allow MAC field descriptions

Use the data in the following table to use the **Allow MAC** tab.

Name	Description
Address	Specifies the source MAC address of an entry.
Ports	Specifies the allowed ports on which the MAC address of this entry are learned.

Modifying auto-learned MAC addresses

Modify the auto-learned MAC addresses to change a MAC address that is automatically learned to one that can be manually edited. Manually edited MAC addresses do not count towards the maximum number of addresses that can be learned.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**.
2. Click **MAC Security**.
3. Click the **Auto Learn** tab.
4. Double-click in the **Auto Learn Action** field for the address you want to change and then select **ConvertToManualEdit** from the list.
5. Click **Apply**.

Auto Learn field descriptions

Use the data in the following table to use the **Auto Learn** tab.

Name	Description
Address	Specifies the source MAC address of the auto-learned entries.
Port	Specifies the port where the MAC address is learned.
Auto Learn Action	Converts an auto-learned MAC address entry to a manual edit MAC address entry. The variable provides a mechanism for you to move a MAC address entry from the auto-learned table to the Manual Edit table.

Table continues…

Name	Description
	Settings: • None • convertToManualEdit

Configuring limit learning

Limit MAC address learning to limit the number of forwarding database (FDB) entries learned on a particular port to a user-specified value. After the number of learned forwarding database entries reaches the maximum limit, packets with unknown source MAC addresses are flooded to all member ports.

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 **Limit-Learning** tab.
5. Configure the parameters as required.

Limit Learning field descriptions

Use the data in the following table to use the **Limit-Learning** tab.

Name	Description
PortNum	Shows the slot and port number to configure.
MaxMacCount	Configures the number of entries in the MAC table for the port that causes learning to stop. The default is 1024.
MinMacCount	Configures the number of entries in the MAC table for the port at which learning can resume. The default is 512.
CurrentMacCount	Shows the number of entries currently in the MAC table for the port.
Enable	Enables or disables limit learning for the port.
MacLearning	Shows if MAC learning is enabled or disabled for the port.

Table continues…

Name	Description
ViolationLogTrap	Configures the system to send a trap to the management station after a MAC address violation is detected on the port. The default is disable.
ViolationDownPort	Configures the system to disable the port after a MAC address violation is detected. The default is disable.

Chapter 6: Spanning tree fundamentals

This section describes the spanning tree features supported on Avaya Virtual Services Platform 9000.

Virtual Services Platform 9000 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. Virtual Services Platform 9000 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.

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.

Virtual Services Platform 9000 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. Virtual Services Platform 9000 supports up to 64 STGs.

Although STP and MSTP are variations of the same spanning tree protocol, they communicate information differently. A VSP 9000 in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with Nortel STP. MSTP spanning tree groups are not the same as Nortel STP spanning tree groups. Using a VSP 9000 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.

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, Virtual Services Platform 9000 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

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 11: 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 12: 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).

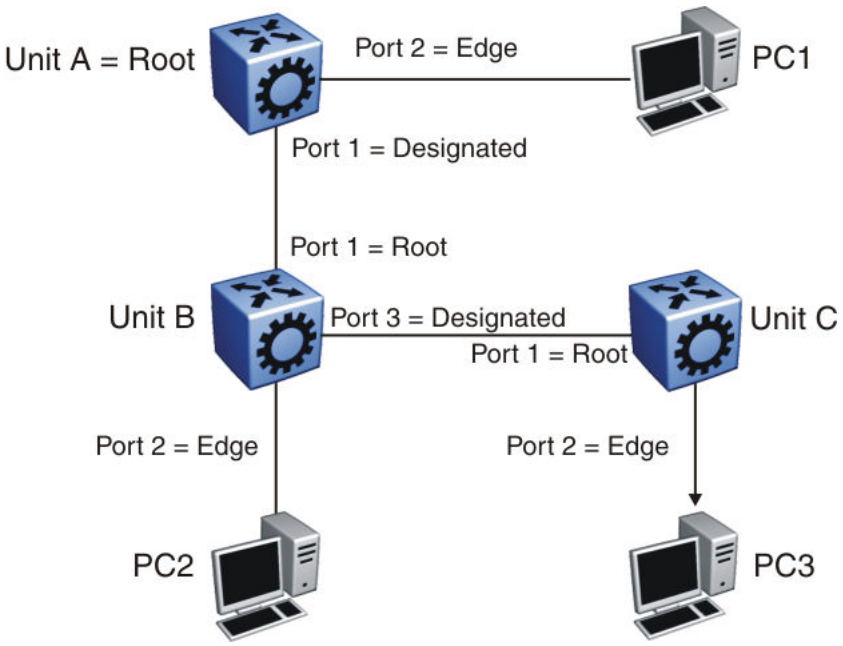

Figure 6: RSTP negotiation process

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 Virtual Services Platform 9000 can exchange BPDUs during the negotiation process, and on the number of switches in the network.

BPDU Filtering

Virtual Services Platform 9000 supports Bridge Protocol Data Unit (BPDU) Filtering for STGs, RSTP, and MSTP.

Overview

Spanning Tree eliminates loops in a network. A bridge that participates in spanning tree uses BPDUs to exchange information with other bridges. The bridges select a single bridge as the root bridge based on the BPDU information exchange. The bridge with the lowest priority becomes the root bridge. If all bridges share the same priority, the bridge with the lowest bridge ID becomes the root bridge. This process is the root selection process.

After you add a new bridge to the network, or remove an existing bridge, the bridges repeat the root selection process, and then select a new root bridge.

Use BPDU Filtering to achieve the following results:

- Block the root selection process after an edge device, such as a laptop that uses Linux with STP enabled, is added to the network. Blocking the root selection process prevents unknown devices from influencing the spanning tree topology.
- Block BPDU flooding of the switch from an unknown device.

Operation

You can enable or disable BPDU Filtering on an individual port basis, regardless of the spanning tree state. Each port uses a timer to determine port-state recovery.

After you enable BPDU Filtering on a port and the port receives a BPDU, the following actions occur:

1. The filter disables the port.
2. The switch generates an SNMP trap and the following log message:

   ```
   Port X is shut down by BPDU Filter
   ```

3. The port timer begins.
4. The port remains in the disabled state until the timer expires.

If you disable BPDU Filtering before the timer expires, the timer stops and the port remains in the disabled state. You must manually enable the port.

Limitations

Virtual Services Platform 9000 does not support BPDU Filtering on the following ports:

- MultiLink Trunking (MLT)
- Interswitch Trunking (IST)
- Split Multilink Trunking (SMLT)
- Routed Split Multilink Trunking (RSMLT)

If a BPDU filter disables a port, and then you save the configuration, the port status remains non-operational after a chassis reboot.

If you hot swap an interface module, the switch preserves the BPDU Filtering state of a port if the module type is the same. If the new module is not the same type as the original module, the switch removes the BPDU Filtering configuration for the port.

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:

Avaya Virtual Services Platform 9000 supports up to 64 STGs in a device.

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.

```
VSP-9012:1(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.

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

Configuring BPDU Filtering

Configure BPDU Filtering to block the root selection process or to prevent BPDU flooding from unknown devices.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

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

2. Enable BPDU Filtering for the port:

   ```
   spanning-tree bpdu-filtering enable
   ```

3. **(Optional)** Configure the timer for port-state recovery:

   ```
   spanning-tree bpdu-filtering timeout <0-65535>
   ```

4. **(Optional)** Enable BPDU Filtering on an additional port or group of ports:

   ```
   spanning-tree bpdu-filtering port {slot/port[-slot/port][,...]}
   enable
   ```

5. **(Optional)** Configure the timer for port-state recovery for an additional port or group of ports:

   ```
   spanning-tree bpdu-filtering port {slot/port[-slot/port][,...]}
   timeout <0-65535>
   ```

6. Verify the configuration:

   ```
   show spanning-tree bpdu-filtering [GigabitEthernet {slot/port[-slot/
   port][,...]}] [{slot/port[-slot/port][,...]}]
   ```

Example

Enable BPDU Filtering on port 6/44, and specify a timer value of 200 seconds. Verify the configuration.

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
VSP-9012:1(config)#interface gigabitEthernet 6/44
VSP-9012:1(config-if)#spanning-tree bpdu-filtering enable
VSP-9012:1(config-if)#spanning-tree bpdu-filtering timeout 200
VSP-9012:1(config-if)#show spanning-tree bpdu-filtering 6/44
```

```
Port MLTID Admin   Oper Link LinkTrap Timeout    TimerCount BpduFiltering
---- ----- ------- ---- ---- -------- ---------- ---------- -------------
6/44       Enable  Up   Up   Enabled         200          0 Enabled
```

Variable definitions

Use the data in the following table to use the **spanning-tree bpdu-filtering** commands.

Variable	Value
enable	Enables BPDU Filtering on the port. The default is disabled.
port {slot/port[-slot/port][,...]	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
timeout *<0-65535>*	Specifies the value to use for port-state recovery. After a BPDU filter disables a port, the port remains in the disabled state until this timer expires. You can configure a value from 10 to 65535. The default is 120 seconds. If you configure the value to 0, you disable the timer. If you disable the timer and the port receives a BPDU, the filter disables the port and the port remains disabled. You must manually enable the port.

Use the data in the following table to use the **show spanning-tree bpdu-filtering** command.

Variable	Value
{slot/port[-slot/port][,...]	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

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 <600–400>] [pathcost-type <bits16|
bits32>] [priority <0–61440>] [tx-holdcount <1–10>] [version <rstp|
stp-compatible>]
```

Example

Configure RSTP:

```
VSP-9012:1(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.

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 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.

Before you begin

Ensure the port is operationally up before you issue the **spanning-tree rstp protocol-migration true** command.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable

   configure terminal

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

2. Configure RSTP:

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

   Note:

   After you change the RSTP edge-port variable, you must disable and reenable the port for the change to take effect.

3. Disable the port:

   ```
   shutdown
   ```

4. Reenable the port:

   ```
   no shutdown
   ```

Example

Configure RSTP.

```
VSP-9012:1(config-if)#spanning-tree rstp cost 100 edge-port true p2p auto priority 32
protocol-migration true stp enable
VSP-9012:1(config-if)#shutdown
VSP-9012:1(config-if)#no shutdown
```

Variable definitions

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

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.

Table continues…

Variable	Value
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.
port {slot/port}	Configures the port value.
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.

```
VSP-9012:1(config)#spanning-tree rstp version rstp
```

Variable definitions

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

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. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View global RSTP configuration information:

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

Example

View global RSTP configuration information.

```
VSP-9012:1(config)#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. Enter Privileged EXEC mode:

```
enable
```

2. View RSTP statistics:

```
show spanning-tree rstp statistics
```

Example

View RSTP statistics.

```
VSP-9012:1(config)#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. Enter Privileged EXEC mode:

```
enable
```

2. View the RSTP status:

```
show spanning-tree rstp status
```

Example

View the RSTP status.

```
VSP-9012:1(config)#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. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View RSTP configuration information:

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

Example

View RSTP configuration information.

```
VSP-9012:1(config)#show spanning-tree rstp port config 3/1
```

```
================================================================================
                      RSTP Port Configurations
================================================================================
Port Number                  : 3/1
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.

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

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. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the RSTP status for a port:

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

Example

View the RSTP status for a port.

```
VSP-9012:1(config)#show spanning-tree rstp port status 3/2

================================================================================
                            RSTP Port Status
                          (Port Priority Vector)
================================================================================
Port Number                    : 3/2
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.

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

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.

```
VSP-9012:1(config)#show spanning-tree rstp port statistics 3/1

================================================================================
                        RSTP Port Statistics
================================================================================
Port Number                        : 3/1
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.

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 related statistics for the selected port.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the RSTP role:

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

Example

View the RSTP role.

```
VSP-9012:1(config)#show spanning-tree rstp port role 3/1
```

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

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. Enter Privileged EXEC mode:

   ```
   enable
   ```

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.

```
VSP-9012:1(config)#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   4/1-4/9,4/11-4/48
1    01:80:c2:00:00:00  mstp   4/10

Total number of Spanning Tree IDs :  2
```

View spanning tree status information.

```
VSP-9012:1(config)#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
CB-SWB:1(config)#show spanning-tree config
```

Configuring Multiple Spanning Tree Protocol

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

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.

```
VSP-9012:1(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.

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.
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.

Table continues…

Variable	Value
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 VSP 9000 in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with Nortel STP. MSTP spanning tree groups are not the same as Nortel STP spanning tree groups. Using a VSP 9000 in MSTP mode with another chassis in STP mode can create a loop in the network. 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

Configure MSTP multiple spanning tree instance (MSTI) options to configure the configuration version.

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.

```
VSP-9012:1(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.

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 • 28672 • 32768 • 36864 • 40960 • 45056 • 49152 • 53248 • 57344 • 61440

Configuring Ethernet MSTP on a port

Configure Ethernet MSTP on a port to enable this feature.

Before you begin

Ensure the port is operationally up before you issue the **spanning-tree mstp protocol-migration true** command.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

```
configure terminal

interface GigabitEthernet {slot/port[-slot/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}] [priority <0–240>]
[protocol-migration <false|true>]
```

Note:

After you change the MSTP edge-port variable, you must disable and reenable the port for the change to take effect.

3. Disable the port:

```
shutdown
```

4. Reenable the port:

```
no shutdown
```

Example

Configure Ethernet MSTP.

```
VSP-9012:1(config)#spanning-tree mstp cost 1 edge-port true force-port-state enable hello-
time 100 p2p auto priority 2 protocol-migration true
VSP-9012:1(config)#shutdown
VSP-9012:1(config)#no shutdown
```

Variable definitions

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

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.
port *{slot/port}*	Specifies the port list.
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.

Table continues…

Variable	Value
	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

Configure Ethernet MSTP MSTI to configure the Ethernet MSTP MSTI parameters on a port.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable

   configure terminal

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

2. Configure Ethernet MSTP MSTI:

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

Example

Configure Ethernet MSTP MSTI.

```
VSP-9012:1(config)#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.

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.

Table continues…

Variable	Value
port {slot/port[-slot/port][,...]}	Specifies the port or ports.
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. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the MSTP configurations:

   ```
   show spanning-tree mstp config
   ```

Example

View the MSTP configurations.

```
VSP-9012:1(config)#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. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the MSTP status:

   ```
   show spanning-tree mstp status
   ```

Example

View the MSTP status.

```
VSP-9012:1(config)#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. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the MSTP port information:

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

Example

View the MSTP port information.

```
VSP-9012:1(config)#show spanning-tree mstp port role 3/1
```

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

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

Viewing MSTP MSTI information

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Show MSTI information:

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

Example

Show MSTI information.

```
VSP-9012:1(config)#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

VSP-9012:1(config)#show spanning-tree mstp msti port statistics 3/1

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

================================================================================
Port Number                  : 3/1
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.

Variable	Value
config *[<1-63>]*	Shows the configuration for one or all MSTP instance IDs.

Table continues…

Variable	Value
port	Shows the configuration, role, or statistics information of a MSTP port. • config {slot/port[-slot/port][,...] } • role {slot/port[-slot/port][,...] } • statistics {slot/port[-slot/port][,...] }

Viewing MSTP statistics

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Show MSTP statistics:

   ```
   show spanning-tree mstp statistics
   ```

Example

Show MSTP statistics.

```
VSP-9012:1(config)#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).

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 pane, 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 Avaya Virtual Services Platform 9000

Restart the Avaya Virtual Services Platform 9000 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 pane, 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 BPDU Filtering

Configure BPDU Filtering to block the root selection process or to prevent BPDU flooding from unknown devices.

About this task

To configure multiple ports simultaneously, select more than one port in the Device Physical View tab. The **BPDU Filter** tab appears as a table-based tab. For more information about how to use a table-based tab, see *Using ACLI and EDM on Avaya Virtual Services Platform 9000,* NN46250-103.

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 **BPDU Filter** tab.
5. Select **BpduFilteringAdminEnabled** to enable BPDU Filtering for the port.

6. **(Optional)** Type a value in **BpduFilteringTimeout** to configure the timer for port-state recovery
7. Click **Apply**.

BPDU Filter field descriptions

Use the data in the following table to use the **BPDU Filter** tab.

Name	Description
BpduFilteringAdminEnabled	Enables BPDU Filtering on the port. The default is disabled.
BpduFilteringOperEnabled	Shows the current status of BPDU Filtering on the port.
BpduFilteringTimeout	Specifies the value to use for port-state recovery. After a BPDU filter disables a port, the port remains in the disabled state until this timer expires. You can configure a value of 0 or from 1000 to 6553500. The default is 12000 (1/100 seconds). A value of 1000 equals 10 seconds. **Note:** If you configure the value to 0, you disable the timer. If you disable the timer and the port receives a BPDU, the filter disables the port and the port remains disabled. You must manually enable the port.
BpduFilteringTimerCount	Shows the time, starting at 0, since the port became disabled. When the BpduFilteringTimerCount reaches the BpduFilteringTimeout value, the port is enabled. Displays in 1/100 seconds.

Configuring RSTP global parameters

Perform this procedure to configure the RSTP global parameters.

Procedure

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

4. Configure the parameters as required.
5. 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.

Table continues…

Name	Description
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 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 pane, 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 pane, 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 pane, 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	Indicates the maximum hop count. The granularity of this timer is specified to be 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 2000.
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 spanning tree protocol as specified in IEEE 802.1s is in use.

Table continues…

Name	Description
	Although STP and MSTP are variations of the same spanning tree protocol, they communicate information differently. A VSP 9000 in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with Nortel STP. MSTP spanning tree groups are not the same as Nortel STP spanning tree groups. Using a VSP 9000 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 return a bad value error if you attempt to configure a value which is not a whole number of seconds. The default is 2000.

Table continues…

Name	Description
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.
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 pane, 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, on the Virtual Services Platform 9000, 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.
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.

Table continues…

Name	Description
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 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.

Table continues…

Name	Description
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 VSP 9000 in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with Nortel STP. MSTP spanning tree groups are not the same as Nortel STP spanning tree groups. Using a VSP 9000 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 pane, 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.
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.

Table continues…

Name	Description
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 pane, 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.
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

Table continues…

Name	Description
	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.
boundary port	A bridge port that attaches a Multiple Spanning Tree (MST) bridge to a LAN in another region.
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.
Control Processor (CP) module	The Control Processor module runs all high level protocols (BGP, OSPF) and distributes the results (routing updates) to the rest of the system. The CP manages and configures the IO and Switch Fabric modules, and maintains and monitors the health of the chassis.
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.
Global routing engine (GRE)	The base router or routing instance 0 in the Virtual Routing and Forwarding (VRF).
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.
Internet Group Management Protocol (IGMP)	IGMP is a host membership protocol used to arbitrate membership in multicast services. IP multicast routers use IGMP to learn the existence of host group members on their directly attached subnets.
interswitch trunking (IST)	A feature that uses one or more parallel point-to-point links to connect two aggregation switches. The two aggregation switches use this channel to share information and operate as a single logical switch. Only one interswitch trunk can exist on each Split Multilink Trunking (SMLT) aggregation switch.
Layer 2	Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.
Layer 3	Layer 3 is the Network Layer of the OSI model. An example of a Layer 3 protocol is Internet Protocol (IP).
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).
Logical Link Control (LLC)	A protocol used in LANs to transmit protocol data units between two end stations. This LLC layer addresses and arbitrates data exchange between two endpoints.
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.
Network Basic Input/ Output System (NetBIOS)	An application programming interface (API) that augments the DOS BIOS by adding special functions for Local Area Networks (LAN).
Packet Capture Tool (PCAP)	A data packet capture tool that captures ingress and egress (on Ethernet modules only) packets on selected ports. You can analyze captured packets for troubleshooting purposes.
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.
Reverse Address Resolution Protocol (RARP)	A protocol that maintains a database of mappings between physical hardware addresses and IP addresses.
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.

Service Advertisement Protocol (SAP)	Used by printers, file servers, and gateways to announce their availability to nodes on the network.
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.
single spanning tree bridge	A bridge that can support only a single spanning tree, the common spanning tree (CST).
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.