Configuring VLANs, Spanning Tree, and NLB for VOSS

Contents

Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

Purpose

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

- Extreme Networks VSP 4000 Series (includes VSP 4450 Series)
- Extreme Networks VSP 4900 Series
- Extreme Networks VSP 7200 Series
- Extreme Networks VSP 7400 Series
- Extreme Networks VSP 8000 Series (includes VSP 8200 Series and VSP 8400 Series)
- Extreme Networks VSP 8600 Series
- Extreme Networks XA1400 Series

  ⊛ **Note:**

  VOSS is licensed on the XA1400 Series as a Fabric Connect VPN (FCVPN) application, which includes a subset of VOSS features. FCVPN transparently extends Fabric Connect services over third-party provider networks.

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 VOSS platforms. This document also provides instructions to use Command Line Interface (CLI) and Enterprise Device Manager (EDM).

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

For information about how to connect an external MSTP or RSTP network to a Fabric Connect network in a loop-free topology, see Configuring Fabric Basics and Layer 2 Services for VOSS.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product.
	Note	Useful information or instructions.
	Important	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon.

Table continues…

Convention	Description
	Examples:
	• Click **OK**.
	• On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command.
	For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command.
	For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed.
	For example, if the command syntax is `ethernet/2/1 [ <parameter> <value> ]...`, you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages.
	Examples:
	• `show ip route`
	• `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths.
	For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.
Vertical Line (	)	A vertical line (	) separates choices for command keywords and arguments. Enter only one choice. Do

Table continues…

Convention	Description
	not type the vertical line when you enter the command.
	For example, if the command syntax is `access-policy by-mac action { allow	deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and software compatibility for Extreme Networks products
Extreme Optics Compatibility
Other resources such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

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

Extreme Portal   Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub   A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC   For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

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

• Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products

- A description of the failure

- A description of any actions already taken to resolve the problem

- A description of your network environment (such as layout, cable type, other relevant environmental information)

- Network load at the time of trouble (if known)

- The device history (for example, if you have returned the device before, or if this is a recurring problem)

- Any related RMA (Return Material Authorization) numbers

Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.

2. Complete the form (all fields are required).

3. Select the products for which you would like to receive notifications.

   ✳ **Note:**
   You can modify your product selections or unsubscribe at any time.

4. Select **Submit**.

Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.

- Improvements that would help you find relevant information in the document.

- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.

- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.

- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this Document

The following sections detail what is new in this document.

DEMONSTRATION FEATURE - DvR One IP Enhancement

⊛ **Note:**

DvR One IP Enhancement is a demonstration feature on VOSS platforms. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment.

For information about platform support, see the VOSS Feature Support Matrix.

You can now use a single IP address in the subnet for every Controller by configuring the DvR VLAN IP to be the same as the DvR gateway IP.

For more information, see Configure a Single IP Address for All DvR Controllers on a VLAN Subnet on page 68.

Notice about Feature Support

This document includes content for multiple hardware platforms across different software releases. As a result, the content can include features not supported by your hardware in the current software release.

If a documented command, parameter, tab, or field does not display on your hardware, it is not supported.

For information about physical hardware restrictions, see your hardware documentation.

Chapter 3: VLAN configuration

This chapter provides concepts and procedures to configure the virtual local area network (VLAN) features supported on the switch.

For information about the user-configuration interfaces, see Configuring User Interfaces and Operating Systems for VOSS.

VLAN fundamentals

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

The practical applications of VLAN include the following:

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

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

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

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

Port-based VLANs

A port-based VLAN is a VLAN in which you explicitly configure the ports to be in the VLAN. When you create a port-based VLAN on a device, you assign a VLAN identification number (VLAN ID) and specify the ports that belong to the VLAN. These port members are always active port members.

The VLAN ID is used to coordinate VLANs across multiple switches. Any type of frame can be classified to a port-based VLAN.

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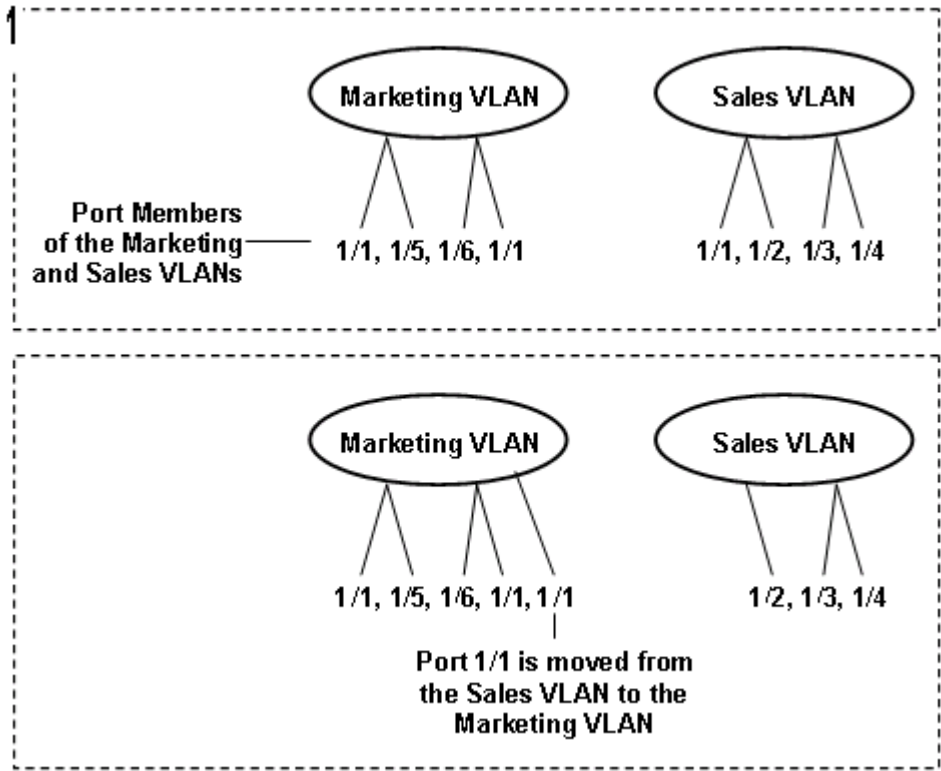
Figure 1: Port-based VLAN

Private VLANs

Table 3: E-Tree and Private VLANs product support

Feature	Product	Release introduced
For configuration details, see the following documents: • E-Tree - Configuring Fabric Basics and Layer 2 Services for VOSS • Private VLANs - Configuring VLANs, Spanning Tree, and NLB for VOSS • MLT and Private VLANs - Configuring Link Aggregation, MLT, SMLT and vIST for VOSS		

Table continues…

Feature	Product	Release introduced
E-Tree and Private VLANs	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 4.1
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported

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

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

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

Port types

Table 4: Port types for private VLANs

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

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

The following figure shows a basic private VLAN topology with private VLAN configured on five switches. All ports connecting to other switches are trunk type ports and all other ports are either promiscuous or isolated ports. On the secondary VLAN, spokes can communicate with hubs, hubs can communicate with all spokes in the same private VLAN using the primary VLAN, but spokes cannot communicate with other spokes.
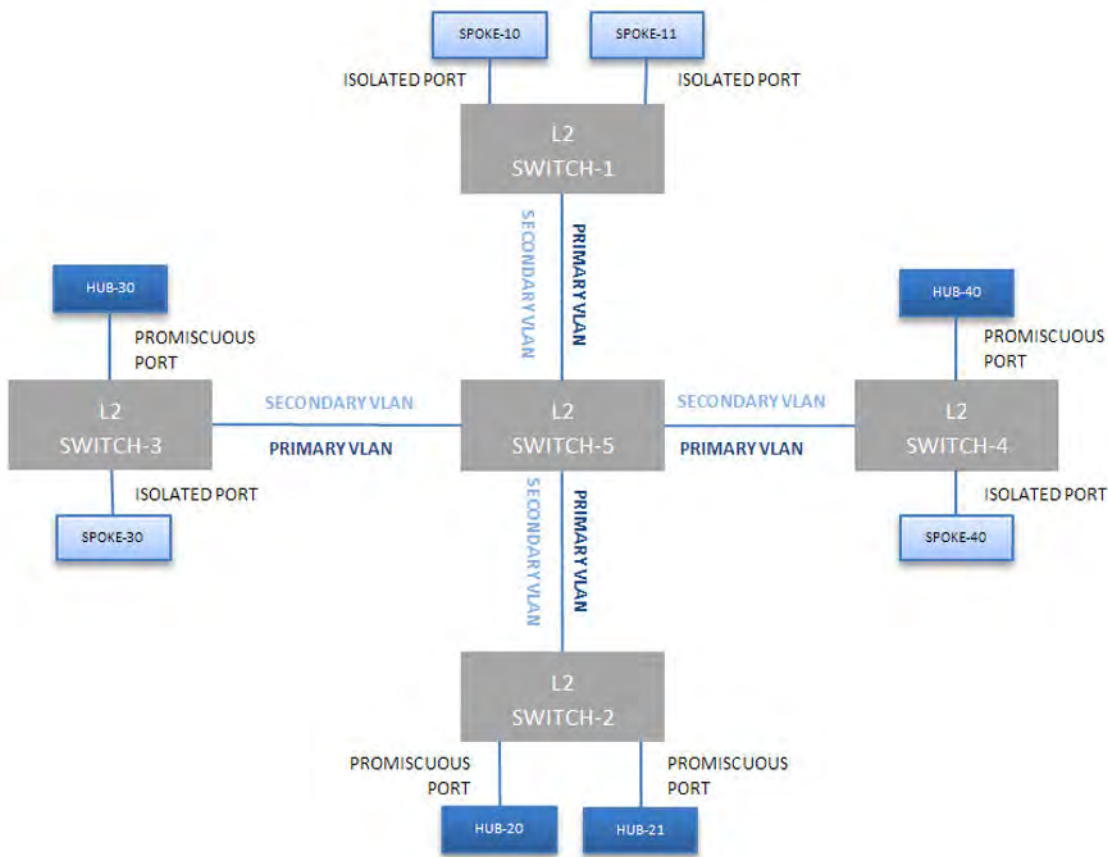
Figure 2: Private VLAN topology

E-Tree

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

For more information about E-Tree and SPBM configuration, see Configuring Fabric Basics and Layer 2 Services for VOSS.

Private VLAN Configuration Rules

The following are private VLAN rules for the switch:

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

Policy-based VLANs

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

Port membership types

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

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

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

Static port members are always members of the VLAN. Static port members are not aged out due to inactivity and they are not removed from the active list. If a server or router connects to a port, designate that port as a static member of a VLAN. If a server connects to a port that is only a potential member and the server sends very little traffic, a client fails to reach the server if the server port is timed out of the VLAN. It is recommended 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 5: 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 6: Supported policy-based VLAN types

VLAN type	Support
Protocol-based	supported

Protocol-based VLANs

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

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

The switch supports IPv6 protocol-based VLAN only.

SPBM B-VLAN

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

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

> ✳ **Note:**
>
> 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 MAC address learning is disabled
- Unknown MAC discard is enabled

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

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

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

VLAN tagging and port types

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

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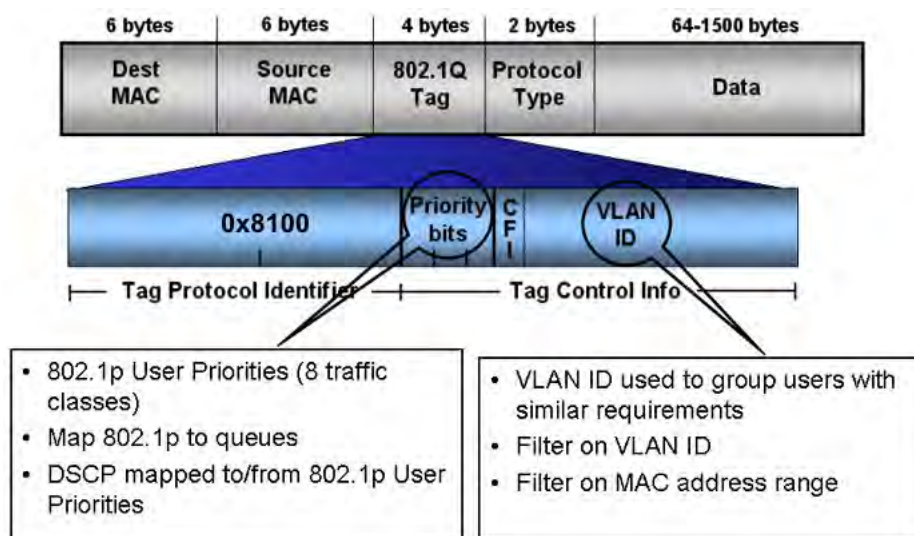
Figure 3: VLAN tag insertion

802.1Q tagged ports

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

Whether tagged frames are sent depends on what you configure at the port level. Tagging is configured as true or false for the port, and is applied to all VLANs on that port.

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

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

Treatment of tagged and untagged frames

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

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

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

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

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

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

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

Untagging default VLAN on a tagged port feature

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

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

For more information about the Network with IP phone and PC, see the following figure.
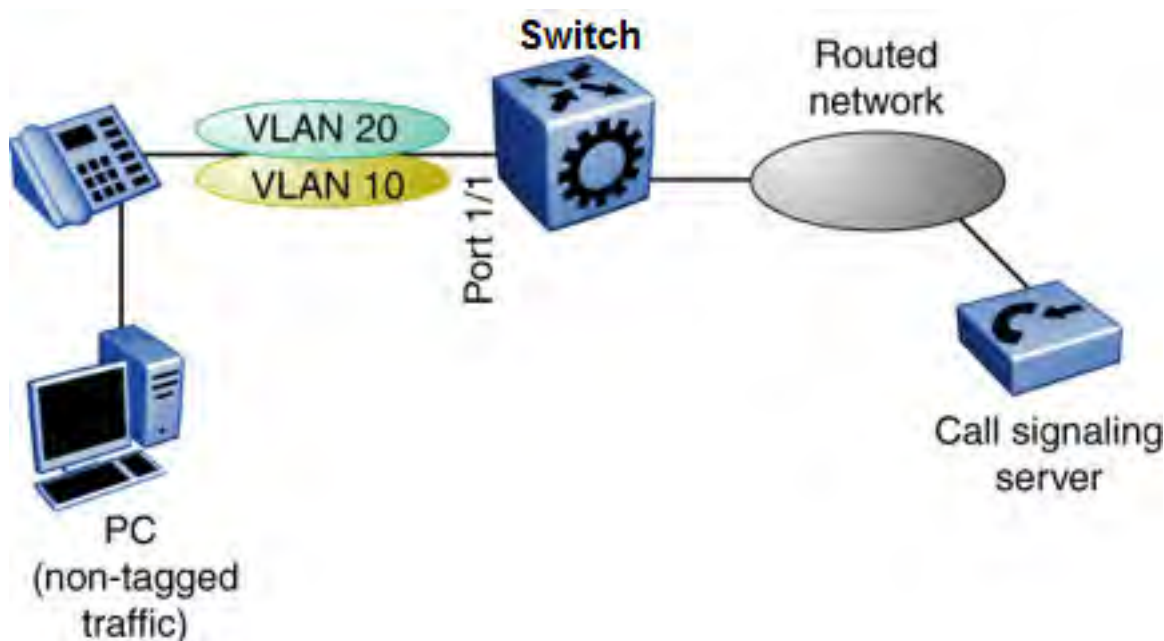
Figure 4: Network with IP phone and PC

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

VLAN router interfaces

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

IP routing and VLANs

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

- Port-based VLANs
- IP protocol-based VLANs

VLAN implementation

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

- Default VLAN on page 21
- NULL VLAN on page 21
- Brouter ports on page 21

Default VLAN

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

NULL VLAN

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

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

Brouter ports

A brouter port is actually a one-port VLAN with an IP interface. The difference between a brouter port and a standard IP protocol-based VLAN configured to perform routing is that the routing interface of the brouter port is not subject to the spanning tree state of the port. A brouter port can

be in the blocking state for nonroutable traffic and still route IP traffic. Because a brouter port is a single-port VLAN, it uses one VLAN ID. Each brouter port decreases the number of available VLANs by one.

VLAN configuration rules

The following are VLAN rules for the switch:

- The switch supports configurable VLANs in the range of 1 to 4059. VLAN 0 is invalid. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. VLAN IDs on the switch range from 2 to 4094 but, by default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

- A tagged port can belong to multiple VLANs in multiple Spanning Tree Groups.

- Under the default configuration, the default Spanning Tree Group is number 1 if the chassis configuration permits multiple STGs.

- An untagged port can belong to only one port-based VLAN.

- You can configure only one protocol-based VLAN for a given protocol.

- The VLAN membership of a frame is determined by the following order of precedence, if applicable:

  1. IEEE 802.1Q tagged VLAN ID

  2. protocol-based VLAN

  3. port-based VLAN default VLAN of the receiving port

- You cannot configure a VLAN name that uses all numbers, for example, 222.

VLAN Feature Support

The following table summarizes supported features.

For the latest scalability information, see Release Notes for VOSS.

Table 7: VLAN support

Feature	Description
Number of VLANs	4059
Port-based VLANs	Supported
Policy-based VLANs	
• Protocol-based	
• SPBM-based	Supported

Table continues…

Feature	Description
IEEE 802.1Q tagging	Supported
IP routing and VLANs	Supported
Special VLANs • Default VLAN • Null VLAN • Brouter ports • Private VLAN	 Supported

Network Load Balancing

Table 8: Network Load Balancing product support

Feature	Product	Release introduced
For configuration details, see Configuring VLANs, Spanning Tree, and NLB for VOSS.		
Network Load Balancing (NLB) - multicast operation	VSP 4450 Series	Not Supported
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.0
	VSP 8400 Series	VOSS 6.0
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported
Network Load Balancing (NLB) - unicast operation	VSP 4450 Series	Not Supported
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	Not Supported

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 the following mission critical, IP-based services:

- Web
- VPN
- Streaming media
- Firewalls

NLB also provides high availability by detecting host failures and automatically redistributing traffic to remaining operational hosts.

NLB considerations and restrictions

Although the switch interoperates with NLB clusters that operate in Unicast mode and Multicast mode, the following restrictions apply:

- True egress mirroring is not supported on all VOSS hardware platforms. Because packets are mirrored prior to the completion of packet processing, egress mirrored packets can differ from the packets egressing the port. Therefore, NLB Unicast traffic and NLB Multicast traffic destined to the NLB Virtual Mac Address are not mirrored correctly.

  > ⊛ **Note:**
  >
  > To mirror the egress traffic of VOSS hardware platforms, you can use the NEXT-hop device ingress mirroring to capture the egress packets of the switch.

  Of the VOSS hardware platforms, only VSP 4000 supports true egress mirroring.

- Inter-VRF routing is not supported between an NLB client and an NLB cluster VLAN in Unicast mode or Multicast mode.
- You must configure NLB to use the same mode as the NLB Server.
- Static ARP entries are not supported for NLB Unicast or NLB Multicast.
- For interoperability with NLB, the switch provides configuration options at the VLAN level.
- ARP entries for NLB server IP addresses do not age out when there is still client traffic coming to the NLB servers, even after the NLB servers are no longer reachable.

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 in hexadecimal form). All traffic destined to this MAC address is sent to all the servers in the cluster. The virtual MAC address is specified in the Sender MAC Address field of the Address Resolution Protocol (ARP) reply from the cluster to the switch. ARP responses from the switch are sent to the virtual MAC address (rather than to the hardware MAC address).

You can configure the switch for NLB unicast mode support. After you enable the NLB unicast option, the switch floods traffic destined to the cluster IP address to all ports on the VLAN. Unicast mode supports connectivity to a secondary virtual IP address. For information about software scaling capabilities in unicast mode, see [Release Notes for VOSS](#).

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 in hexadecimal form) 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 the switch for NLB multicast mode support. When you enable NLB multicast mode on a VLAN, the routed traffic destined to the NLB cluster is flooded by default on all ports of the VLAN. All VLANs support multiple cluster IPs by default. You can connect up to 200 NLB clusters to a single VLAN. For information about software scaling capabilities, see Release Notes for VOSS.

> ⊛ **Note:**
>
> Shortest Path Bridging MAC (SPBM) supports NLB Unicast and Multicast modes. For more information on SPBM, see Configuring Fabric Basics and Layer 2 Services for VOSS.

Supported NLB Topologies

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

Supported NLB topology–example 1

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

The following figure illustrates this configuration where the NLB Server and the NLB Client workstations connect to different aggregation switches, which connect to the switch using different VLANs and different ports.
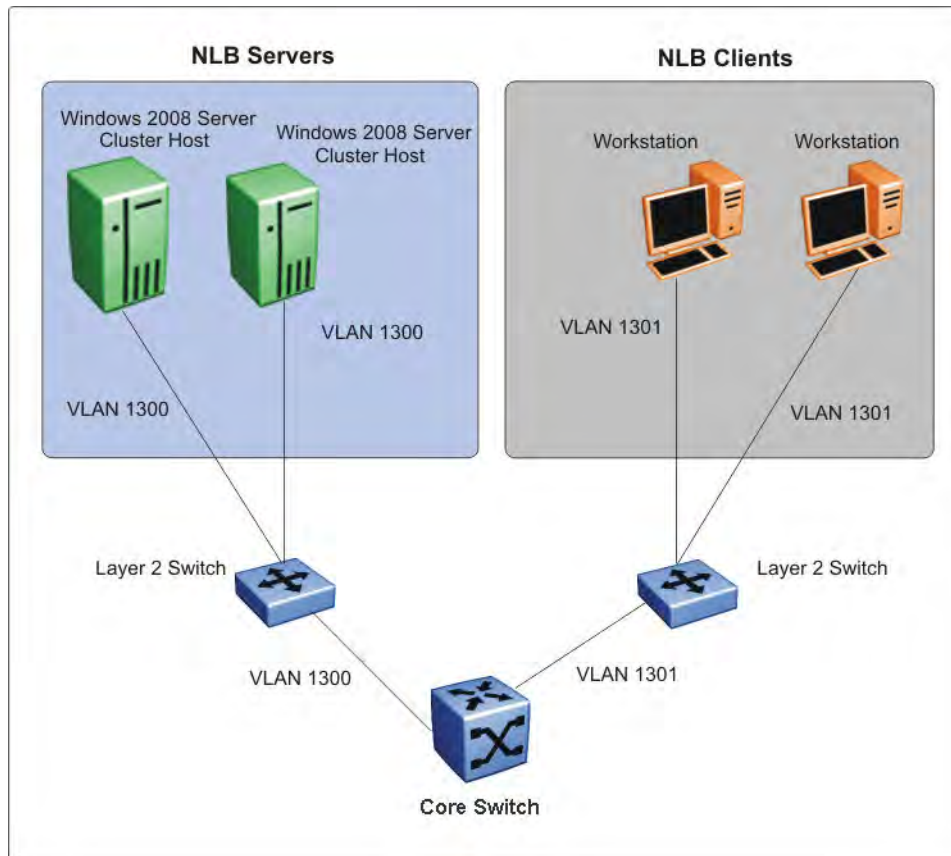
Figure 5: Supported NLB topology–example 1

Supported NLB topology–example 2

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

> ⊛ **Note:**
>
> The switch supports Layer 3 routing between an NLB-enabled VLAN and another VLAN on the same port.
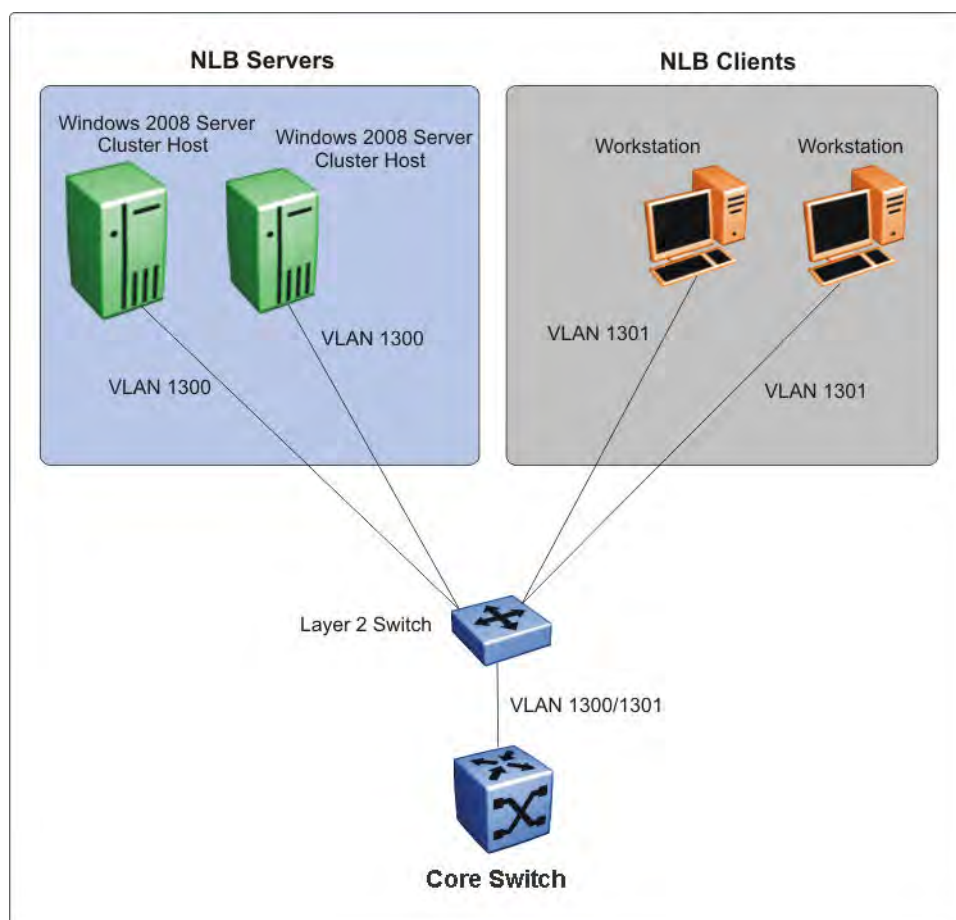
Figure 6: Supported NLB topology–example 2

Other supported NLB topologies

The switch supports NLB in the following other topologies:

- NLB cluster hosts and clients are connected to Layer 2 Ethernet switches that are SMLT connected to the SMLT cluster.

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

- NLB cluster hosts and clients are directly connected and distributed between the switches in the SMLT cluster.

- NLB cluster hosts and clients are connected to Layer 2 Ethernet switches that are SMLT connected to the SMLT cluster core.

✱ **Note:**

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

NLB and Directed Broadcast Resource Limits

NLB and Directed Broadcast consume resources from the same pool of 200 resources. When you configure either NLB or Directed Broadcast, the switch uses one resource. If you configure both NLB and Directed Broadcast, the switch uses two resources.

To avoid a situation where there is a lack of resources, adhere to the following limits:

- The number of NLB cluster IP interfaces multiplied by the number of configured clusters must be equal to, or less than, 200. The number of NLB cluster IP interfaces is the *key*, not the number of VLANs. You can configure 1 VLAN with up to 200 NLB cluster IP interfaces or configure up to 200 VLANs with 1 NLB cluster IP interface per VLAN.

  For example: `1 NLB cluster IP interface x 200 clusters = 200` or `2 NLB cluster IP interfaces x 100 clusters = 200`
- If you configure VLANs with Directed Broadcast only, you can scale up to 200 VLANs.
- If you configure VLANs with both **NLB** and **Directed Broadcast**, you can only scale up to 100 VLANs assuming there is only 1 NLB cluster IP interface per VLAN.

For information on Directed Broadcast, see Configuring Security for VOSS.

VLAN MAC-layer Filtering Database and MAC Security

Table 9: FDB Protected by Port product support

Feature	Product	Release introduced
For configuration details, see Configuring VLANs, Spanning Tree, and NLB for VOSS.		
FDB protected by port (MAC security limit-learning)	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	Not Supported
	VSP 7200 Series	Not Supported
	VSP 7400 Series	Not Supported
	VSP 8200 Series	Not Supported
	VSP 8400 Series	Not Supported
	VSP 8600 Series	Not Supported
	XA1400 Series	Not Supported

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 the port level.

Port—level security applies to traffic for all VLANs received on that port.

Port-level MAC security provides limit—learning option:

- 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 and there is room to learn new MAC addresses. 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

VLAN IP as the default gateway

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.

VRRP IP as the default gateway

Similarly, you can prevent VRRP IP spoofing by blocking the external use of the virtual 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 virtual 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 virtual 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 VRRP subnet about the correct virtual router 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.

Packet spoofing

You can stop spoofed IP packets by configuring the switch to forward only IP packets that contain the correct source IP address of your network. By denying all invalid source IP addresses, you minimize the chance that your network is the source of a spoofed DoS attack.

A spoofed packet is one that comes from the Internet into your network with a source address equal to one of the subnet addresses on your network. The source address belongs to one of the address

blocks or subnets on your network. To provide spoofing protection, you can use a filter that examines the source address of all outside packets. If that address belongs to an internal network or a firewall, the packet is dropped.

To prevent DoS attack packets that come from your network with valid source addresses, you need to know the IP network blocks in use. You can create a generic filter that:

- Permits valid source addresses
- Denies all other source addresses

To do so, configure an ingress filter that drops all traffic based on the source address that belongs to your network.

If you do not know the address space completely, it is important that you at least deny private (see RFC1918) and reserved source IP addresses. The following table lists the source addresses to filter.

Table 10: Source addresses to filter

Address	Description
0.0.0.0/8	Historical broadcast. High Secure mode blocks addresses 0.0.0.0/8 and 255.255.255.255/16. If you enable this mode, you do not need to filter these addresses.
10.0.0.0/8	RFC1918 private network
127.0.0.0/8	Loopback
169.254.0.0/16	Link-local networks
172.16.0.0/12	RFC1918 private network
192.0.2.0/24	TEST-NET
192.168.0.0/16	RFC1918 private network
224.0.0.0/4	Class D multicast
240.0.0.0/5	Class E reserved
248.0.0.0/5	Unallocated
255.255.255.255/32	Broadcast1

You can also enable the spoof-detect feature on a port.

VLAN loop prevention

Table 11: Simple Loop Prevention Protocol product support

Feature	Product	Release introduced
For configuration details, see Configuring VLANs, Spanning Tree, and NLB for VOSS.		
Simple Loop Prevention Protocol (SLPP)	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1

Table continues…

Feature	Product	Release introduced
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VSP 8200 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50
		Not Supported on Flex-UNI

Loop prevention

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

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

⊛ **Note:**

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

Configure the SLPP functionality with the following criteria:

- SLPP TX Process – You decide on which VLANs a switch can send SLPP hello packets. The packets are then replicated out all ports which are members of the SLPP-enabled VLAN. It is recommended that you enable SLPP on all VLANs.

- SLPP RX Process – You decide on which ports the switch can act when receiving an SLPP packet that is sent by the same switch or by its SMLT peer. You must enable this process only on Access SMLT ports. You can enable this process only when the design permits on SMLT CORE ports in the case of a square/full mesh core design.

- SLPP Action – The action operationally disables the ports receiving the SLPP packet. You can also tune the network failure behavior. You can choose how many SLPP packets a port needs to receives before a switch takes an action. You need to stagger these values to avoid edge switch isolation – see the recommendations at the end of this section.

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

The desire is to prevent a loop from causing network problems, while also attempting not to isolate totally the edge where the loop was detected. Total edge closet isolation is the last resort to protect

the rest of the network from the loop. With this in mind, some administrators adopt the concept of an SLPP primary switch and SLPP secondary switch. These are strictly design terms and are not configuration parameters. The Rx thresholds are staggered between the primary and secondary switch. Therefore, the primary switch disables an uplink immediately upon a loop occurring. If this resolves the loop issue, then the edge closet still has connectivity back through the SLPP secondary switch. If the loop is not resolved, then the SLPP secondary switch disables the uplink and isolates the closet to protect the rest of the network from the loop.

As the number of VLANs running SLPP scale off of a specific uplink port, the Rx-threshold value may need to be increased to prevent complete isolation of the offending edge. The primary goal of SLPP is to protect the core at all costs. In certain loop conditions, what can occur is the secondary switch also detects the loop and SLPP Rx-threshold of the secondary switch is reached before the primary can stop the loop by taking its port down. Therefore, both switches eventually take their ports down and the edge is isolated. The larger the number of VLANs associated with the port, the more likely this can occur, especially for loop conditions that affect all VLANs.

The loop detection functionality of the device must not be used under normal operating conditions. Only use it if directed by the technical support personnel.

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

Spanning Tree and Protection against Isolated VLANs

Virtual Local Area Network (VLAN) isolation disrupts packet forwarding. The following figure illustrates the problem. Two VLANs (V1 and V2) connect four devices, and both VLANs are in the same spanning tree group. V2 includes three of the four devices, whereas V1 includes all four devices. After a spanning tree protocol detects a loop, it blocks the link with the highest link cost. In this case, the 100 Mbps link is blocked, which isolates a device in V2. To avoid this problem, either configure V2 on all four devices or use MSTP with a different Multiple Spanning Tree Instance (MSTI) for each VLAN.
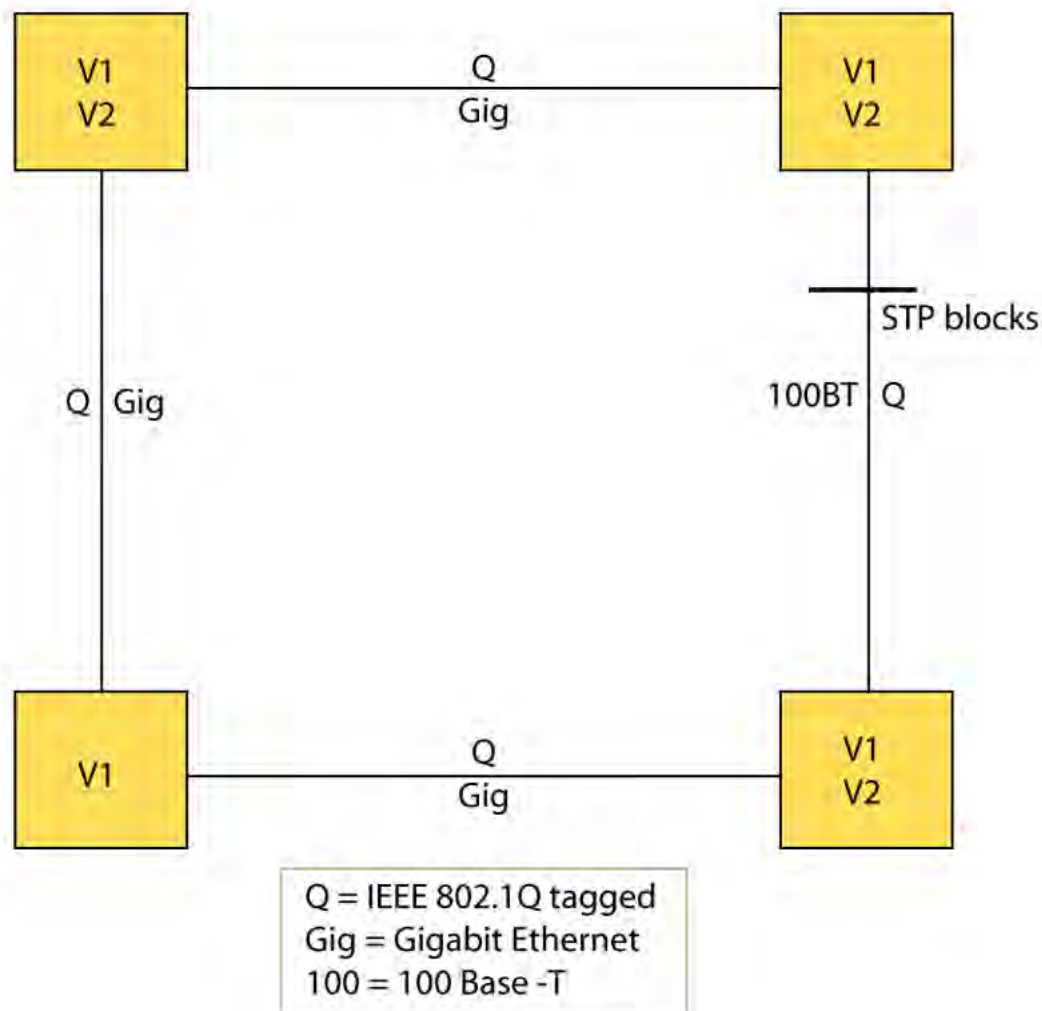
Figure 7: VLAN isolation

IGMP Layer 2 Querier

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

Overview

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

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

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

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

IGMP Snooping

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

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

IGMP Layer 2 Querier and IGMP interaction

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

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

- Querier
- Non-Querier

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

For more information about how to configure IGMP Layer 2 Querier, see Configuring IP Multicast Routing Protocols for VOSS.

Switched UNI Layer 3

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

You must associate the S-UNI I-SID to the platform VLAN. After you associate the platform VLAN with the I-SID, it becomes a CVLAN.

The switch performs MAC and ARP learning on the platform VLAN.

> ⊛ **Note:**
>
> You cannot add S-UNI ports or MLT to the S-UNI platform VLANs directly. Add the ports to the I-SID and assign the I-SID to the platform VLAN.

You can associate only port based VLAN with S-UNI I-SID.

VLAN configuration using CLI

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

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

Create a VLAN

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

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

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create a VLAN by specifying one of the following VLAN types:

   a. Create a VLAN by port:

   ```
   vlan create <2-4059> [name WORD<0-64>] type port-mstprstp <0-63>
   [color <0-32>]
   ```

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

   ```
   vlan create <2-4059> [name WORD<0-64>] type protocol-mstprstp
   <0-63> ipv6 [color <0-32>]
   ```

   c. Create an SPBM B-VLAN:

   ```
   vlan create <2-4059> [name WORD<0-64>] type spbm-bvlan [color
   <0-32>]
   ```

3. **(Optional)** Associate a CVLAN I-SID to the platform VLAN.

   ```
   vlan i-sid <1-4059> <1-16777215> [force]
   ```

4. Log on to the VLAN Interface Configuration mode for the VLAN ID:

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

5. Assign an IP address to a VLAN:

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

6. **(Optional)** Specify the MAC-offset value:

   ```
   ip address <A.B.C.D/X>|<A.B.C.D> <A.B.C.D> dvr-one-ip <MAC-offset>
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#vlan create 2 type port-mstprstp 0 color 4
Switch:1(config)#vlan i-sid 2 100
Switch:1(config)#interface vlan 2
Switch:1(config-if)#ip address 192.0.2.0/24 dvr-one-ip
```

Variable Definitions

The following table defines parameters for the **vlan create** command.

Variable	Value
<2-4059>	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.
name *WORD<0-64>*	Specifies the VLAN name. The name attribute is optional.
type port-mstprstp *<0-63> [color <0-32>]*	Creates a VLAN by port: • *<0-63>* is the STP instance ID from 0 to 63. • *color <0-32>* is the color of the VLAN in the range of 0 to 32. ✳ **Note:** MSTI instance 62 is reserved for SPBM if SPBM is enabled on the switch.
type pvlan-mstprstp *<0-63> [color <0-32>]*	Creates a private VLAN by port: • *<0-63>* is the STP instance ID from 0 to 63. • *color <0-32>* is the color of the VLAN in the range of 0 to 32.

Table continues…

Variable	Value
type protocol-mstprstp *<0–63>* ipv6	Creates a VLAN by protocol: • *<0–63>* is the STP instance ID. • color <0-32> is the color of the VLAN in the range of 0 to 32.
type spbm-bvlan	Creates a SPBM B-VLAN.

The following table defines parameters for 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.
dvr-one-ip	Specifies that the IP address will be used as the DvR gateway IP address and will be used by all other DvR Controllers for the DvR VLAN subnet.
<MAC-offset>	Specifies a number by which to offset the MAC address from the chassis MAC address. This ensures that each IP address has a different MAC address. If you omit this variable, a unique MAC offset is automatically generated. Different hardware platforms support different ranges. To see which range is available on the switch, use the CLI command completion Help.

The following table defines parameters for the `vlan i-sid` command.

Variable	Value
<1-4059>	Specifies the VLAN ID. Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
<0-16777215>	Specifies the service instance identifier (I-SID). You cannot use I-SID 0x00ffffff. The system reserves this I-SID to advertise the virtual BMAC in an SMLT dual-homing environment. This value is the same for the primary and secondary VLANs.
force	Specifies the software must replace the existing VLAN-to-I-SID mapping, if one exists.

Creating a Private VLAN

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create a private VLAN:

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

3. Specify a name for the VLAN:

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

4. Enter GigabitEthernet Interface Configuration mode:

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

   * **Note:**

   If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

5. Set the port type:

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

   * **Note:**

   If the port is a member of an MLT, the port inherits the private VLAN port type of the MLT. For more information about creating MLTs and LACPs, see, Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.

6. Exit to Global Configuration mode:

   ```
   exit
   ```

7. Enter VLAN Interface Configuration mode:

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

8. Add ports to the primary VLAN:

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

Example

```
Switch:1> enable

Switch:1# configure terminal

Switch:1(config)# vlan create 2 type pvlan-mstprstp 6 secondary 5

Switch:1(config)# interface gigabitethernet 1/36

Switch:1(config-if)# private-vlan isolated

Switch:1(config-if)# exit

Switch:1(config)# interface vlan 2

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

Variable Definitions

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

Variable	Value
<2-4059>	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.
name *WORD<0-64>*	Specifies the VLAN name. The name attribute is optional.
type pvlan-mstprstp *<0-63>*	Creates a private VLAN by port. The variable *<0-63>* is the STP instance ID from 0 to 63. ⊛ **Note:** MSTI instance 62 is reserved for SPBM if SPBM is enabled on the switch.
secondary*<2-4059>*	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.

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

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

✱ **Note:**

If there are other non-private VLANs using the defined port, the following message is displayed:
```
All non private VLANs using this interface will be removed once this
port becomes a member of a private VLAN. Ports with private-vlan type
of isolated or promiscuous may only contain private VLANs. Do you wish
to continue (y/n) ?
```

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

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

Assign an IP Address to a VLAN

Assign an IP address to a VLAN so that it supports routing operations.

Before you begin

• You must create the VLAN.

• Activate IP forwarding globally.

About this task

If an IP interface is configured without specifying the VRF instance, it maps to VRF 0 by default.

Use the vrf parameter to associate the VLAN with a VRF instance.

> ⓘ **Important:**
>
> The VRRP virtual IP address cannot be same as the local IP address of the port or VLAN on which VRRP is enabled.

Procedure

1. Enter VLAN Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface vlan <1-4059>
   ```

2. Assign an IP address to a VLAN:

   ```
   ip address <A.B.C.D/X>|<A.B.C.D> <A.B.C.D> dvr-one-ip name WORD
   <0-64>
   ```

3. **(Optional)** If required, associate the VLAN with a VRF:

   ```
   vrf WORD<1-16>
   ```

Example

```
Switch:1> enable
Switch:1# configure terminal
Switch:1(config)# interface vlan 2
Switch:1(config-if)# ip address 192.0.2.5 255.255.255.0 dvr-one-ip name Boston
```

Variable Definitions

The following table defines parameters for 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.
dvr-one-ip	Specifies that the IP address will be used as the DvR gateway IP address and will be used by all other DvR Controllers for the DvR VLAN subnet.
name *WORD <0-64>*	Specifies the name associated with the IP address on a VLAN. This parameter does not apply to all hardware platforms.

The following table defines parameters for the `vrf` command.

Variable	Value
WORD<0-16>	Specifies the VRF of the VLAN.

Performing a general VLAN action

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Perform a general VLAN action:

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

Example

Perform a general VLAN action:

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

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

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

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

Variable definitions

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

Table 12: Variable definitions

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

Table continues…

Variable	Value
	VLAN, and removes MAC addresses learned on those ports for this VLAN.
flushDynMemb	Configures action to flushDynMemb. This action removes port members not configured as static from the list of active port members of a policy-based VLAN, and removes MAC addresses learned on those ports for this VLAN.
triggerRipUpdate	Configures action to triggerRipUpdate.
all	Configures action to all and performs all preceding actions.

Configuring static MAC addresses for a VLAN

Configure the static MAC address parameters.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure a static MAC address of a VLAN:

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

Example

Configure a static MAC address of a VLAN:

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

Variable definitions

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

Table 13: Variable definitions

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also

Table continues…

Variable	Value
	reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
<0x00:0x00:0x00:0x00:0x00:0x00>	Indicates the MAC address.
{slot/port[/sub-port][-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Limit MAC Address Learning

Configure the MAC security feature to control traffic from specific MAC addresses. The total number of MAC addresses that you can configure are fixed. The switch supports a maximum of 32k MAC entries for non-SPBM configurations. For SPBM configurations, the switch supports a maximum of 16k MAC entries. You can enable this feature at 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, MAC learning stops on that port.

Procedure

1. Enter Interface Configuration mode:

   `enable`

   `configure terminal`

   `interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}` or `interface mlt` *<1-512>*

   ✴ **Note:**

   If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

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

   `mac-security [port {slot/port[/sub-port][-slot/port[/sub-port]] [,...]}] limit-learning enable [max-addrs` *<1-32000>*`]`

Example

Protect the FDB from hits by too many MAC addresses:

```
Switch:1(config)#interface gigabitethernet 1/1
Switch:1(config-if)#mac-security limit-learning enable
Switch:1(config-if)#mac-security limit-learning max-addrs 5000
```

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.
	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 *<1–32000>*	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.
port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
	Use this parameter to apply the change to multiple ports without changing CLI modes.

Configuring the forwarding database timeout globally

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enter the following command:

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

Variable definitions

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

Table 14: Variable definitions

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

Adding or removing ports in a VLAN

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

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   ⭐ **Note:**

   If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Add ports in a VLAN:

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

3. Remove ports in a VLAN:

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

Example

Add ports in a VLAN:

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

Remove ports in a VLAN:

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

Variable definitions

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

Table 15: Variable definitions

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
{slot/port[/sub-port][-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
portmember	Configures the port type as port member.

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` *<1-4059>* `<0x00:0x00:0x00:0x00:0x00:0x00>`

3. Remove a VLAN source MAC address:

   `no vlan srcmac` *<1-4059>* `<0x00:0x00:0x00:0x00:0x00:0x00>`

Example

Add a VLAN source MAC address:

`Switch(config)# vlan create 10 type srcmac-mstprstp 0`

`Switch(config)# vlan srcmac 10 0x00:0x00:0x00:0x00:0x00:0x11`

Configure 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 VOSS](#).

Before you begin

- For all modes, configure an IP address on the VLAN enabled with NLB.
- To switch between Unicast NLB and Multicast NLB, you must first disable the NLB support.

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 and Multicast modes.

Procedure

1. Enter VLAN Interface Configuration mode:

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

2. Enable NLB support on an interface:

   ```
   nlb-mode unicast
   ```

   Or,

   ```
   nlb-mode multicast
   ```

   To switch from one nlb-mode to another, you must first disable the NLB support, and then enter the new nlb-mode.

3. **(Optional)** Disable NLB support on an interface:

   ```
   no nlb-mode
   ```

Example

Configure unicast mode for VLAN 2, and then switch to multicast mode.

```
Switch:1(config)#interface vlan 2
Switch:1(config-if)#nlb-mode unicast
Switch:1(config-if)#no nlb-mode
Switch:1(config-if)#nlb-mode multicast
```

Configuring a tagged port to discard untagged frames

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

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   ⊛ **Note:**

   If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Configure a tagged port to discard untagged frames:

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

3. Discard a tagged frame on an untagged port:

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

4. Untag the default VLAN on a tagged port:

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

Example

Configure a tagged port to discard untagged frames:

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

Discard a tagged frame on an untagged port:

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

Untag the default VLAN on a tagged port:

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

Variable definitions

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

Table 16: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Configuring SLPP

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable SLPP:

   ```
   slpp enable
   ```

3. Configure the transmission interval:

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

4. Add a VLAN to the transmission list:

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

Example

Enable SLPP:

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

Configure the transmission interval to 5000 milliseconds:

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

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

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

Variable definitions

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

Table 17: Variable definitions

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

Job aid

The following table provides the recommended SLPP values.

Table 18: SLPP recommended values

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

Configuring SLPP packet-rx on a port

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

🛈 **Important:**

To provide protection against broadcast and multicast storms, it is recommended that you enable Rate Limiting for broadcast traffic and multicast traffic.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   > ⊛ **Note:**
   >
   > If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Configure SLPP on a port:

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

Example

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

Variable Definitions

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

Table 19: Variable definitions

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

Job aid

The following table provides the recommended SLPP values.

Table 20: SLPP recommended values

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

Configuring SLPP packet-tx on a VLAN

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

> 🛈 **Important:**
>
> To provide protection against broadcast and multicast storms, it is recommended that you enable Rate Limiting for broadcast traffic and multicast traffic.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   > ✶ **Note:**
   >
   > If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Enable SLPP:

   ```
   slpp enable
   ```

3. Configure the transmission interval:

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

4. Add a VLAN to the transmission list:

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

Example

Log on to the VLAN Interface Configuration mode:

`Switch(config)# interface vlan 2`

Enable SLPP:

`Switch(config-if)# slpp enable`

Configure the transmission interval to 500 milliseconds:

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

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

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

Variable definitions

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

Table 21: Variable definitions

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

Viewing SLPP information

Use SLPP information to view loop information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View SLPP information:

```
show slpp
```

Example

```
Switch# show slpp
```

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

Viewing SLPP information for a port

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

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. View SLPP information for a port:

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

3. Clear SLPP packet RX counters:

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

Example

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

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

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

Variable definitions

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

Table 22: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Configuring spoof detection

Configure spoof detection to prevent IP spoofing.

For more information about this feature, see

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

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

   ⊛ **Note:**

   If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-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:

```
Switch(config-if)# spoof-detect port 1/1 enable
```

Enable autorecovery on a port:

```
Switch(config-if)# auto-recover-port port 1/1 enable
```

Viewing VLAN information

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View VLAN information:

   `show vlan basic <1-4059>`

3. View advanced parameters:

   `show vlan advance <1-4059>`

Example

View VLAN information for VLAN 2:

`Switch:1> show vlan basic 2`

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

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

View VLAN information:

`Switch:1> show vlan basic`

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

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

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

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

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

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

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

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

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

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

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

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

14     VLAN-14          spbm-bvlan  62  none      N/A          N/A           0

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

View advanced parameters:

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

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

Variable definitions

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

Table 23: Variable definitions

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

Viewing private VLAN information

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View private VLAN information:

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

3. View private vlan port information:

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

Example

View VLAN information for private VLAN :

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

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

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

View port information for private VLAN:

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

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

Viewing brouter port information

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View brouter port information:

   ```
   show vlan brouter-port
   ```

Example

View brouter port information:

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

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

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

Viewing VLAN port member status

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View VLAN port member status:

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

Example

View VLAN port member status:

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

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

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


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

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


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

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

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


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

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

     1/38              1/38


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

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

Variable definitions

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

Variable	Value
null-vlan	Displays port members of the NULL VLAN. This is a place holder VLAN for ports that are not members of any port-based VLAN. When a port is removed from all port-based VLANs, it is added to the NULL VLAN as a port member. The NULL VLAN is an internal construct and cannot be deleted.
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port. If you do not specify a port, the command shows information for all the ports.
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. ✳ **Note:** 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

View VLAN source MAC addresses:

```
show vlan src-mac [<1-4059>]
```

Example

View VLAN source MAC addresses:

```
Switch(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
```

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. To enter User EXEC mode, log on to the switch.

2. View VLAN forwarding database information:

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

Example

View VLAN forwarding database information:

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

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

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

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

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

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

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

Variable definitions

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

Table 24: Variable definitions

Variable	Value
<1-4059>	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
mac <0x00:0x00:0x00:0x00:0x00:0x00>	Specifies the MAC address.
port {slot/port[-slot/port][,...]}	Specifies the port or port list.
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

View manual edit MAC addresses:

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

Example

View manual edit MAC addresses:

```
Switch(config)# show vlan manual-edit-mac

========================================================================
                        Manual Edit Mac
========================================================================
MAC ADDRESS          PORTS
------------------------------------------------------------------------
00:00:00:00:00:55  1/3
00:00:00:00:00:66  1/3

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

View 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 limit-learning:

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

Example

View port-level MAC security for limit-learning:

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

=====================================================================
                        Port limit-fdb-learning
=====================================================================
PORT  FDB      MAXMAC   MINMAC  LOG     PORT    CURMAC  MAC
NUM   PROTECT  COUNT    COUNT   TRAP    DOWN    COUNT   LEARN
---------------------------------------------------------------------
1/4   dis      1024     512     dis     dis     0       true
1/5   ena      5000     3000    dis     dis     0       true
```

View NLB-Mode Information

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View NLB port information:

   ```
   show interface vlan nlb-mode [<1-4059>]
   ```

Example

View NLB-mode information.

```
Switch:1#show interface vlan nlb-mode
=====================================================================
                        Vlan Nlb
=====================================================================
VLAN_ID NLB_ADMIN_MODE NLB_OPER_MODE PORT_LIST MLT_GROUPS
---------------------------------------------------------------------
2        unicast        disable
22       multicast      multicast  1/19-1/21   2 3
Total Entries: 2
```

Displaying C-VLAN and Switched UNI I-SID information

Use the following procedure to display C-VLAN and Switched UNI (S-UNI) I-SID information.

Procedure

1. To enter User EXEC mode, log on to the switch.

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

   `show vlan i-sid` *`<1-4059>`*

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

   `show i-sid <1-16777215>`

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

   `show isis spbm i-sid {all|config|discover} [vlan` *`<1-4059>`*`] [id <1-16777215>] [nick-name <x.xx.xx>]`

5. Display all elan I-SID:

   • `show i-sid elan`

6. Display I-SID configured on MLT:

   • `show mlt i-sid`

7. Display I-SID configured on port:

   • `show interfaces gigabitethernet i-sid`

Example

```
Switch:1>show isis spbm i-sid all
================================================================================
                               SPBM ISID INFO
================================================================================
ISID      SOURCE NAME  VLAN  SYSID           TYPE      HOST_NAME   ISID NAME
--------------------------------------------------------------------------------
16777000  f.84.35      4051  beb0.0000.8435  discover  BEB-8435    PIMGW-ISID
100       f.84.35      4052  beb0.0000.8435  discover  BEB-8435    ISID-100
16777000  0.01.48      4051  d884.66f9.4c84  config    Titan-48    PIMGW-ISID
100       f.84.35      4052  d884.66f9.4c84  config    Titan-48    ISID-100
--------------------------------------------------------------------------------
 Total number of SPBM ISID entries configured: 2
--------------------------------------------------------------------------------
 Total number of SPBM ISID entries discovered: 2
--------------------------------------------------------------------------------
 Total number of SPBM ISID entries: 4
--------------------------------------------------------------------------------

Switch:1>show i-sid elan

================================================================================
                               Isid Info
================================================================================
ISID      ISID                 PORT        MLT         ORIGIN      ISID
ID        TYPE       VLANID    INTERFACES  INTERFACES              NAME
--------------------------------------------------------------------------------
```

```
1        ELAN      N/A       -          -          CONFIG     ExtremeServer1
3        ELAN      N/A       -          -          CONFIG     ExtremeServer3
4        ELAN      N/A       -          -          CONFIG     ExtremeServer4
23       ELAN      N/A       -          -          CONFIG     ISID-23


c: customer vid    u: untagged-traffic

All 4 out of 4 Total Num of elan i-sids displayed
```

```
switch:1#show mlt i-sid
===============================================================================
                              MLT Isid Info
===============================================================================
           ISID                      ISID
MLTID IFINDEX ID       VLANID C-VID  TYPE       ORIGIN         BPDU
-------------------------------------------------------------------------------
10    6153    100      N/A    20     ELAN       CONFIG
-------------------------------------------------------------------------------

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

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

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

Variable Definitions

The following table defines parameters for the **show vlan i-sid** commands.

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

The following table defines parameters for the **show i-sid** commands.

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

The following table defines parameters for the **show isis** commands.

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

Enable DvR on a Layer 2 VSN (VLAN)

Before you begin

- Ensure that the VLAN on which to enable DvR exists and is associated with an I-SID.

About this task

On a Controller, DvR must be manually enabled at the Layer 2 VSN (VLAN) level.

Use this procedure to configure a gateway IPv4 address for a Layer 2 VSN (VLAN) subnet and then enable DvR on it. This address is pushed, along with other L3 configuration information, from the Controllers to the Leaf nodes within the domain, so that the Leaf nodes can create a gateway IP service for each DvR-enabled Layer 2 VSN.

✳️ **Note:**

Optionally, you can now use a single IP address in the subnet for every Controller by configuring the DvR VLAN IP to be the same as the DvR GW IP.

Procedure

1. Enter VLAN Interface Configuration mode:

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

2. Configure a gateway IPv4 address for the VLAN.

   ```
   dvr gw-ipv4 {A.B.C.D}
   ```

   🛈 **Important:**

   Ensure that you configure the same gateway IPv4 address on all Controllers in the domain that belong to a Layer 2 VSN (VLAN).

3. Enable DvR.

   ```
   dvr enable
   ```

   By default, DvR is disabled.

Example

Enable DvR on the Global Router VLAN.

```
Switch:1>en
Switch:1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config-if)#vlan create 200 type port-mstprstp 0
Switch:1(config-if)#vlan i-sid 200 20200
Switch:1(config-if)#interface vlan 200
Switch:1(config-if)#dvr gw-ipv4 192.0.2.1
Switch:1(config-if)#dvr enable
Switch:1(config-if)#ip address 192.0.2.2 255.255.0.0
```

Enable DvR on a VLAN associated to a VRF:

```
Switch:1>en
Switch:1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config-if)#vlan create 400 type port-mstprstp 0
Switch:1(config-if)#vlan i-sid 400 20200
Switch:1(config-if)#interface vlan 400
Switch:1(config-if)#vrf vrf500
Switch:1(config-if)#dvr gw-ipv4 198.51.100.1
Switch:1(config-if)#dvr enable
Switch:1(config-if)#ip address 198.51.100.2 255.255.0.0
```

Variable definitions

Use the data in the following table to use the `dvr gw-ipv4` command.

Variable	Value
{A.B.C.D}	Specifies the gateway IPv4 address for the VLAN.

Configure a Single IP Address for All DvR Controllers on a VLAN Subnet

✱ **Note:**

Product Notice: DvR One IP Enhancement is a demonstration feature on VOSS platforms. Demonstration features are provided for testing purposes. Demonstration features are for lab use only and are not for use in a production environment.

For information about platform support, see the [VOSS Feature Support Matrix](#).

Before you begin

• Ensure that the VLAN on which to enable DvR exists and is associated with an I-SID.

About this task

On a Controller, DvR must be manually enabled at the Layer 2 VSN (VLAN) level.

Use this procedure to configure a single IP address to be used for both the DvR GW IP and the VLAN IP in the DvR VLAN. This IP adddress represents the DvR GW IP address used by all DvR Controllers for the same DvR VLAN. When you configure a DvR VLAN in this way, the Controllers no longer have a unique VLAN IP address.

✱ **Note:**

Optionally, you can use two different IP address for the DvR VLAN and the DvR GW IP.

Procedure

1. Enter VLAN Interface Configuration mode:

   enable

   configure terminal

   interface vlan *<1-4059>*

2. Configure a single IP address for both the DvR GW IP and the VLAN IP in the DvR VLAN.

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

3. Enable DvR.

   `dvr enable`

   By default, DvR is disabled.

Example

Enable DvR.

```
Switch:1>en
Switch:1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config-if)#vlan create 200 type port-mstprstp 0
Switch:1(config-if)#vlan i-sid 200 20200
Switch:1(config-if)#interface vlan 200
Switch:1(config-if)#ip address 192.0.2.1 255.255.0.0 dvr-one-ip
Switch:1(config-if)#dvr enable
```

Variable Definitions

The following table defines parameters for 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.
dvr-one-ip	Specifies the IP address used for the DvR gateway IP address and the VLAN IP in the DvR VLAN.

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:

   We recommend that you enable tagging on the port before you configure UntagDefaultVlans.

9. Enter a default VLAN ID.

10. To enable spoof detect, select **SpoofDetect**.

11. In the Classification area, select the types of VLAN to enable.

12. In the **Classification** area, select the Private VLAN port type. See Creating a Private VLAN on page 75 for more information.

13. Click **Apply**.

14. Click **Close**.

VLAN field descriptions

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

Name	Description
PerformTagging	If checked, this port is a tagged (Trunk) Port. It can belong to multiple port-based VLANs and a VLAN tag is inserted in every frame it transmits. If it is not checked, the port is an untagged (Access) port. The default is disabled.
VlanIdList	Identifies which VLANs this port is assigned.
DiscardTaggedFrames	If selected, and the port is untagged (an access port), tagged frames received on the port are discarded by the forwarding process. If clear, tagged frames are processed normally. The default is disabled.
DiscardUntaggedFrames	If selected and the port is tagged (a trunk port), untagged frames received on the port are discarded by the forwarding process. If clear, untagged frames are processed normally. The default is disabled.
UntagDefaultVLAN	If selected, even if the port is tagged (a trunk port), frames forwarded to the default VLAN for the port are not tagged. The default is disabled.
UntaggedVlanIds	Identifies which VLANs this port is associated with as untagged.

Table continues…

Name	Description
DefaultVlanId	Specifies the VLAN ID assigned to untagged frames received on this trunk port that match no policy-based VLAN to which the port belongs.
SpoofDetect	Enables or disables spoof detection on the specified port.
Protocol	Enables protocol-based VLAN on the port. This feature is always enabled.
PrivateVlanPortType	Specifies the port type. If not specified, the port type defaults to None. • Isolated: Only private VLANs are permitted on isolated ports. • Promiscuous: Only private VLANs are permitted on promiscuous ports. • Trunk: The port is tagged.

Configuring the VLAN Feature on an Extreme Integrated Application Hosting Port

About this task

Perform this procedure to configure the VLAN feature on an Extreme Integrated Application Hosting (IAH) port.

Procedure

1. In the Navigation tree, expand the following folders: **Configuration** > **Edit** > **Insight Port**.

2. Select the IAH port you want to configure.

3. Select the **VLAN** tab.

4. Select **PerformTagging**, to enable tagging.

5. Select **DiscardTaggedFrames**, to discard tagged frames.

6. Select **DiscardUntaggedFrames**, to discard untagged frames.

7. Select **UntagDefaultVlan**, to enable the Untag Default VLAN feature.

   ❗ Important:

   You must enable tagging on the IAH port before you enable the Untagging Default VLANs feature.

8. In the **DefaultVlanId** field, enter a default VLAN ID.

9. Select **SpoofDetect**, to enable spoof detection.

10. In the **PrivateVlanPortType** field, select a type.

11. Click **Apply**.

VLAN Field Descriptions

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

Name	Description
PerformTagging	Enables tagging (trunking) on the Extreme Integrated Application Hosting (IAH) 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 IAH port is an untagged (Access) IAH port. The default value is different for each IAH port.
VlanIdList	Shows the VLAN ID to which the IAH port is assigned to.
DiscardTaggedFrames	Enables the functionality to discard tagged frames received on the IAH port by the forwarding process, for untagged (access) IAH port. The default is disabled.
DiscardUntaggedFrames	Enables the functionality to discard untagged frames received on the IAH port by the forwarding process, for tagged (trunk) IAH port. The default is disabled.
UntagDefaultVLAN	Enables the functinality to untag the frames forwarded to the default VLAN, even if the IAH port is tagged (trunk port). The default is disabled.
UntaggedVlanIds	Shows the untagged VLAN IDs associated with the IAH port.
DefaultVlanId	Specifies the VLAN ID assigned to untagged frames received on the IAH port that match no policy-based VLAN to which the EIAH port belongs.
SpoofDetect	Enables spoof detection on the specified IAH port.
PrivateVlanPortType	Specifies the following: • **trunk**: tagged IAH port. • **isolated**: Only private VLANs are permitted on isolated IAH ports. • **promiscuous**: Only private VLANs are permitted on promiscuous IAH ports. • **none**: default value.

Viewing existing VLANs

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

Procedure

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

2. Click **VLANs**.

3. View the configured VLANs in the **Basic** tab.

4. View the configured private VLANs in the **Private VLAN** tab.

Creating a port-based VLAN

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

- [Creating a protocol-based VLAN](#) on page 80
- [Creating an SPBM B-VLAN](#) on page 82

Procedure

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

2. Click **VLANs**.

3. In the **Basic** tab, click **Insert**.

4. In the **Id** box, enter an unused VLAN ID, or use the ID provided.

5. In the **Name** box, type the VLAN name, or use the name provided.

6. In the **Color Identifier** box, click the down arrow and choose a color from the list, or use the color provided.

7. In the **MstpInstance** box, click the down arrow and choose an msti instance from the list.

8. In the **Type** box, select **byPort**.

9. In the **PortMembers** box, click the **(...)** button.

10. Click on the ports to add as member ports.

    The ports that are selected are recessed, while the nonselected ports are not recessed. Port numbers that appear dimmed cannot be selected as VLAN port members.

11. Click **OK**.

12. Cick **Insert**.

Basic Field Descriptions

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

Name	Description
Id	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.
Name	Specifies the name of the VLAN.
IfIndex	Specifies the logical interface index assigned to the VLAN.
Color Identifier	Specifies a proprietary color scheme to associate a color with the VLAN. Color does not affect how frames are forwarded.
Type	Specifies the type of VLAN: • byPort • byProtocolId • spbm-bvlan • private
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. The sub-port only appears for channelized ports.
ActiveMembers	Specifies the slot/port of each VLAN member. The sub-port only appears for channelized ports.
StaticMembers	Specifies the slot/port of each static member of a policy-based VLAN. The sub-port only appears for channelized ports.
NotAllowToJoin	Specifies the slot/ports that are never allowed to become a member of the policy-based VLAN. The sub-port only appears for channelized ports.
ProtocolId	Specifies the network protocol for protocol-based VLANs. This value is taken from the Assigned Numbers of remote function call (RFC). If the VLAN type is port-based, none is displayed in the Basic tab ProtocolId field.

Table continues…

Name	Description
AgingTime	Specifies the timeout period, in seconds, to age out dynamic members of this VLAN. This field only applies to policy-based VLANs.
	The default is 600.

⊛ **Note:**

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

- Refresh your browser to reload EDM.

- Log out of EDM and log in again to restart EDM.

- Click **Refresh** in the VLAN **Basic** tab toolbar. If the old VLAN name appears in other tabs, click **Refresh** on those tabs as well.

Creating a Private VLAN

Before you begin

- To create a private VLAN, you must set the VLAN type to private and set the private VLAN port type.

- The ports you add to a private VLAN must have a port type of isolated, promiscuous, or trunk.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **VLAN**.

2. Click **VLANs**.

3. In the **Basic** tab, click **Insert**.

4. In the **Id** box, enter an unused VLAN ID, or use the ID provided.

5. In the **Name** box, type the VLAN name, or use the name provided.

6. In the **Color Identifier** box, click the down arrow and choose a color from the list, or use the color provided.

7. In the **MstpInstance** box, click the down arrow and choose an msti instance from the list.

8. In the **Type** box, select **private**.

9. In the **PortMembers** box, click the **(...)** button.

10. Click on the ports to add as member ports.

    The ports that are selected are recessed, while the non-selected ports are not recessed. Port numbers that appear dimmed cannot be selected as VLAN port members.

11. Click **OK**.

12. In the **Secondary Vlan** box, enter an unused VLAN ID.

13. Click **Insert**.

14. Collapse the **VLANs** tab.

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

    To set the port type for the private VLAN:

15. In the navigation pane, expand the following folders: **Configuration** > **VLAN**.

16. Click **VLANs**.

17. In the Classification area, select the **PrivateVlanPortType**.

18. Click **Apply**.

19. Click **Close**.

Basic Field Descriptions

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

Name	Description
Id	Specifies the VLAN ID in the range of 2 to 4059. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1. By default, the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998.
Name	Specifies the name of the VLAN.
IfIndex	Specifies the logical interface index assigned to the VLAN.
Color Identifier	Specifies a proprietary color scheme to associate a color with the VLAN. Color does not affect how frames are forwarded.
Type	Specifies the type of VLAN: • byPort • byProtocolId • spbm-bvlan • private
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.

Table continues…

Name	Description
PortMembers	Specifies the slot/port of each VLAN member. The sub-port only appears for channelized ports.
ActiveMembers	Specifies the slot/port of each VLAN member. The sub-port only appears for channelized ports.
StaticMembers	Specifies the slot/port of each static member of a policy-based VLAN. The sub-port only appears for channelized ports.
NotAllowToJoin	Specifies the slot/ports that are never allowed to become a member of the policy-based VLAN. The sub-port only appears for channelized ports.
ProtocolId	Specifies the network protocol for protocol-based VLANs. This value is taken from the Assigned Numbers of remote function call (RFC). If the VLAN type is port-based, none is displayed in the Basic tab ProtocolId field.
AgingTime	Specifies the timeout period, in seconds, to age out dynamic members of this VLAN. This field only applies to policy-based VLANs. The default is 600.

> ✱ **Note:**
>
> If you or another user changes the name of an existing VLAN using the VLAN **Basic** tab (or using CLI), the new name does not initially appear in EDM. To display the updated name, perform one of the following actions:
>
> - Refresh your browser to reload EDM.
> - Log out of EDM and log in again to restart EDM.
> - Click **Refresh** in the VLAN **Basic** tab toolbar. If the old VLAN name appears in other tabs, click **Refresh** on those tabs as well.

VLAN Field Descriptions

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

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

Viewing Private VLAN information

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

Procedure

1. In the navigation pane, expand the **Configuration** > **VLAN** folders.

2. Click **VLANs**.

3. Click **Private VLAN**.

Private VLAN field descriptions

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

Name	Description
Primary Vlan	Shows the VLAN ID for the primary VLAN.
Secondary Vlan	Shows the VLAN ID for the secondary VLAN.
Primary / Secondary I-sid	Shows the I-SID for the VLAN.

Configuring an IP address for a VLAN

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

About this task

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

Procedure

1. In the navigation pane, expand the **Configuration** > **VLAN** folders.

2. Click **VLANs**.

3. In the **Basic** tab, select the VLAN for which you are configuring an IP address.

4. Click **IP**.

5. Click **Insert**.

6. Configure the required parameters.

7. Click **Insert**.

IP Address field descriptions

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

Name	Description
Interface	Shows the interface to which this entry applies.
Ip Address	Specifies the IP address to associate with the VLAN.
Net Mask	Specifies the subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits configured to 1 and all the hosts bits configured to 0.
BcastAddrFormat	Shows the IP broadcast address format on this interface.
ReasmMaxSize	Shows the size of the largest IP datagram which this entity can reassemble from incoming IP fragmented datagrams received on this interface.
VlanId	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
BrouterPort	Indicates whether this entry corresponds to a brouter port, as oppose to a routable VLAN.
MacOffset	Specifies the MAC offset value. Routable VLANS are assigned MAC addresses arbitrarily or by offset. Their MAC addresses are: • 24 bits: Vendor ID • 12 bits: Chassis ID • 12 bits: 0xA00-0xFFF If you enter the MAC offset, the lowest 12 bits are 0xA00 plus the offset. If not, they are arbitrary.
VrfId	Associates the VLAN or brouter port with a VRF. VRF ID 0 is reserved for the administrative VRF.

Changing VLAN port membership

Modify VLAN port members to control access to the VLAN.

Procedure

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

2. Click **VLANs**.

3. Double-click the **PortMembers** number for the VLAN for which you want to modify port membership.

4. Click the port members you wish to add or remove.

5. Click **Ok**.

6. Click **Apply**.

   The VLAN port membership is changed.

Creating a protocol-based VLAN

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

Procedure

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

2. Click **VLANs**.

3. In the **Basic** tab, click **Insert**.

4. In the **Id** box, type the unique VLAN ID or use the ID provided.

5. In the **Name** box, type the VLAN name or use the name provided.

6. In the **Color Identifier** box, select the color or use the color provided.

   This color is used to visually distinguish the VLANs in a network.

7. In the **MstpInstance** box, click the down arrow and choose an MSTI instance from the list.

8. In the **Type** box, select **byProtocolId**.

   This activates additional fields needed to configure protocol-based VLANs.

9. To specify the VLAN port membership, click the button **(...)** for one of the following fields:

   Port Members

   OR

   StaticMembers

   OR

   NotAllowToJoin

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

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

    OR

    Green: Always members—static

    OR

    Red: Never members—not allowed to join

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

11. Click **Insert**.

Configure 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. Select **VLANs**.

3. In the **Basic** tab, select a source MAC address-based VLAN.

4. Select **Mac**.

5. To manually insert a MAC address, select **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. Select **Yes**.

11. Select **Close**.

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 a SPBM B-VLAN

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

> ⭐ **Note:**
>
> It is recommended that you always configure two B-VLANs in an SPBM dual-homing environment.

Procedure

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

2. Click **VLANs**.

3. In the **Basic** tab, click **Insert**.

4. In the **Id** box, enter an unused VLAN ID, or use the ID provided.

5. In the **Name** box, type the VLAN name, or use the name provided.

6. In the **Color Identifier** box, click the down arrow and choose a color from the list, or use the color provided.

7. In the **Type** box, select **spbm-bvlan**.

8. Cick **Insert**.

9. Collapse the **VLANs** tab.

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

Configuring advanced VLAN features

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

You can also configure a DvR Gateway IPv4 address on a VLAN, and enable DvR on it.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **VLAN**.

2. Click **VLANs**.

3. Click the **Advanced** tab.

4. Configure the parameters as required by double-clicking fields to make changes.

   You cannot make changes to fields that appear dim.

5. Click **Apply**.

Advanced Field Descriptions

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

Name	Description
Id	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
Name	Specifies the name of the VLAN.
IfIndex	Specifies the logical interface index assigned to the VLAN.
Type	Specifies the type of VLAN: • byPort • byProtocolId • spbm-bvlan • private
Isid	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.
Isid Name ⊛ **Note:** This field does not apply to all hardware platforms.	Specifies the name of the I-SID.
ProtocolId	Specifies the network protocol for protocol-based VLANs. If the VLAN type is not protocol-based, None is displayed in the Basic tab ProtocolId field.
AgingTime	Specifies the timeout period for dynamic VLAN membership. A potential VLAN port is made ACTIVE after it receives a packet that matches the VLAN; if no such packet is received for AgingTime seconds, the port is no longer active. The default is 600.
MacAddress	Specifies the MAC address assigned to the virtual router interface for this VLAN. This field is relevant only after the VLAN is configured for routing. This MAC address is used as the Source MAC in routed frames and ARP replies.

Table continues…

Name	Description
Vlan Operation Action	Performs an operation on the VLAN. The values are: • none • flushMacFdb: Configures action to flushMacFdb. This action removes the learned MAC addresses from the forwarding database for the selected VLAN. • flushArp: Configures action to flushArp. This action removes the ARP entries from the address table for the selected VLAN. • flushIp: Configures action to flushIp. This action removes the learned IP addresses from the forwarding table for the selected VLAN. • flushDynMemb: Configures action to flushDynMemb. This action removes port members not configured as static from the list of active port members of a policy-based VLAN and removes MAC addresses learned on those ports. • all: Configures action to all. This action performs all the supported actions; it does not perform the Snoop-related actions. The default is none.
Result	Specifies the result code after you perform an action.
NlbMode	Enables or disables Microsoft Network Load Balancing (NLB) operations on the VLAN. The default is disabled.
SpbMulticast	Enables or disables Multicast over Fabric Connect. The default is disabled.
SpbPimGatewayMulticast	Enables or disables SPB-PIM Gateway Multicast on a VLAN. The default is disabled.
RmonEnable	Enables or disables Remote Monitoring (RMON) on the interface. The default is disabled.
Ipv6FhsSnoopDhcpEnable	Enables or disables IPv6 dhcp snooping on a VLAN. The default is disabled.
Ipv6FhsNDInspectionEnable	Enables or disables neighbor discovery (ND) inspection on a VLAN. The default is disabled.
DvrEnable	Enables or disables DvR on a VLAN that is configured on the DvR Controller. The default is disabled.

Table continues…

Name	Description
	Note: You must enable DvR on every VLAN that is configured on a DvR Controller.
DvrGwIpv4Addr	Specifies the DvR gateway IPv4 address for a VLAN. **Important:** Ensure that you configure the same gateway IPv4 address on all Controllers in the DvR domain that belong to a VLAN.
DvrGwIpv4OneIp	Enables or disables the DvR One IP for a VLAN. The default is disabled (false).

Configure NLB Support

Use Microsoft Network Load Balancing (NLB) to share the workload among multiple clustering servers. For more information about software scaling capabilities, see Release Notes for VOSS.

Before you begin

Ensure that the VLAN exists and has an associated IP address.

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 and Multicast modes.
- Static multicast ARP entries are not supported for NLB Unicast or NLB Multicast.
- Multicast MAC flooding is not supported for NLB.
- ARP entries for NLB server IP addresses do not age out when there is still client traffic coming to the NLB servers, even after the NLB servers are no longer reachable.

Procedure

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

Configuring a port to accept tagged or untagged frames

Configure a port to accept tagged or untagged frames.

Procedure

1. In the Device Physical View tab, select a port.

2. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Port**.

3. Click **General**.

4. Click the **VLAN** tab.

5. To configure tagging on the port, select the **PerformTagging** check box.

   This setting applies to all VLANs associated with the port.

   > ✱ **Note:**
   >
   > 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 recommended SLPP values.

Table 25: SLPP recommended values

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

Configuring the SLPP by VLAN

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

Before you begin

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

Procedure

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

Insert VLANs Field Descriptions

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

Name	Description
VlanId	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
SlppEnable	Activates SLPP on the selected VLAN. The SLPP packet transmission and reception process is active only if you enable the SLPP operation. If you disable the SLPP operation, the following occurs: • the system sends no SLPP packets • the system discards received SLPP packets The default is enabled.

Configuring the SLPP by port

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

⊛ **Note:**

> To provide protection against broadcast and multicast storms, it is recommended 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.

Table continues…

Name	Description
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 recommended SLPP values.

Table 26: SLPP recommended values

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

Configure 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 pane, expand **Configuration** > **VLAN**.

2. Click **VLANs**.

3. Select the **Basic** tab.

4. Select a VLAN.

5. Click **IP**.

6. Click the **Direct Broadcast** tab.

7. Select **DirectBroadcastEnable**.

❗ **Important:**

> Configure multiple VLANs or IPs in the same subnet but in different systems simultaneously.

8. Click **Apply**.

Direct Broadcast field descriptions

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

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

Configuring the forwarding database timeout globally

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

Procedure

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

2. Click **VLANs**.

3. Click the **FdbAging** tab.

4. Type an interval, in seconds, for aging out dynamically learned forwarding information, or keep the default.

5. Click **Apply**.

FDB Aging field descriptions

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

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

Viewing VLAN forwarding database information

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

Procedure

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

2. Click **VLANs**.

3. In the VLANs tab, click the **Forwarding** tab.

Forwarding Field Descriptions

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

Name	Description
VlanId	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
Address	Specifies a unicast MAC address for which the VLAN has forwarding or filtering information.
Status	Specifies the status of the VLAN. The values are: • other • invalid • learned • self • mgmt
Port	Specifies either a value of zero (0) or the port number of the port on which a frame having the specified MAC address was seen. A value of **cpp** indicates a self-assigned MAC address.
BMac	Shows the backbone MAC address if the entry is learned from a Shortest Path Bridging MAC (SPBM) network.
Cvid	Specifies the customer VID.

Viewing the Forwarding Database for a Specific VLAN

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

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN**
2. Click **VLANs**.
3. Select a VLAN.
4. Click **Bridge**.
5. Click the **Forwarding** tab and the VLAN forwarding database information is displayed.

Forwarding Field Descriptions

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

Name	Description
VlanId	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
Address	Specifies a unicast MAC address for which the bridge has forwarding or filtering information.
Status	Specifies the status. Values include the following: • self—one of the bridge addresses • learned—a learned entry that is being used • mgmt—a static entry
Port	Specifies either a value of zero (0) or the port number of the port on which a frame having the specified MAC address was seen. A value of **cpp** indicates a self-assigned MAC address.
Cvid	Identifies the customer VID for this interface.

Clearing learned MAC addresses by VLAN

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

Procedure

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

2. Click **VLANs**.

3. Click the **Advanced** tab.

4. Double-click in the **VLAN Operation Action** field.

5. Choose **FlushMacFdb** from the list.

6. Click **Apply**.

Clearing learned MAC addresses for all VLANs by port

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

Procedure

1. In the Device Physical View tab, select a port.

2. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Port**.

3. Click **General**.

4. In the Interface tab **Action** box, select **FlushMacFdb**.

5. Click **Apply**.

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

6. Click **Close**.

Configuring static forwarding

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

🛈 **Important:**

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

Procedure

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

2. Click **VLANs**.

3. Select the **Basic** tab.

4. Select a VLAN.

5. Click **Bridge**.

6. In the Bridge, VLAN tab, click the **Static** tab.

7. Click **Insert**.

8. In the **MacAddress** box, enter a forwarding destination MAC address.

9. In the **Port** box, click the ellipsis button **(...)**.

10. Select the port on which the frame is received.

11. Click **Ok**.

12. Click **Insert**.

Static field descriptions

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

Name	Description
MacAddress	Specifies the destination MAC address in a frame to which the forwarding information for this entry applies. This object can take the value of a unicast address.
Port	Specifies the port number of the port on which the frame is received.
VlanId	Specifies the VLAN ID in the range of 1 to 4059. By default, VLAN IDs 1 to 4059 are configurable and the system reserves VLAN IDs 4060 to 4094 for internal use. On switches that support the vrf-scaling and spbm-config-mode boot configuration flags, if you enable these flags, the system also reserves VLAN IDs 3500 to 3998. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.
Status	Specifies the status of the VLAN.

Configure 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, MAC learning stops at that port.

Procedure

1. On the Device Physical View tab, select one or more ports.

2. In the navigation pane, expand the **Configuration** > **Edit** > **Port** folders.

3. Select **General**.

4. Select the **Limit-Learning** tab.

5. Configure the parameters as required.

6. Select **Apply**.

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.
CurrentMacCount	Shows the number of entries currently in the MAC table for the port.
Enable	Enables or disables limit learning for the port. The default is disable.
MacLearning	Shows if MAC learning is enabled or disabled for the port.

Chapter 4: Spanning Tree configuration

This chapter provides concepts and procedures to configure the Spanning Tree features supported on the switch.

Spanning Tree Fundamentals

Table 27: Spanning Tree Protocol product support

Feature	Product	Release introduced
For configuration details, see Configuring VLANs, Spanning Tree, and NLB for VOSS.		
Spanning Tree Protocol (STP): • Multiple STP (MSTP) • Rapid STP (RSTP)	VSP 4450 Series	VSP 4000 4.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 4.2.1
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VSP 8200 4.0
	VSP 8400 Series	VOSS 4.2
	VSP 8600 Series	VSP 8600 4.5
	XA1400 Series	VOSS 8.0.50

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

Spanning Tree

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

✳ **Note:**

Spanning Tree is disabled on all Switched UNI (S-UNI) ports. The ports will move into forwarding state as soon as the physical port or VLACP or LACP comes up on the port. If the platform VLAN is associated to the S-UNI Service Instance Identifier (I-SID), then the S-UNI

ports added to the platform VLAN will become the member of MSTP instances associated with the platform VLAN. To enable SLPP on the S-UNI ports, the platform VLAN must be associated with the S-UNI I-SID.

Spanning Tree Groups

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

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

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

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

The protocol considers bridge priority first. If more than one bridge has the same priority, then the protocol must consider the bridge ID. The bridge with the lowest ID becomes the root bridge. For MSTP, this bridge is called the Common and Internal Spanning Tree (CIST) Root because it is the root of the entire physical network.

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

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

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

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

STGs and VLANs

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

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

BPDU handling on S-UNI port/MLT

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

- When you configure a platform VLAN:
  - BPDUs are forwarded to the CPU by default.
  - For both the ingress and egress ports, BPDUs are not flooded in the S-UNI I-SID associated with the platform VLAN.

  ⊛ **Note:**

  If the platform VLAN is configured for the S-UNI port, you cannot enable BDPU forwarding.

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

BPDU Guard

Table 28: Bridge Protocol Data Unit (BPDU) Guard product support

Feature	Product	Release introduced
For configuration details, see Configuring VLANs, Spanning Tree, and NLB for VOSS.		
Bridge Protocol Data Unit (BPDU) Guard	VSP 4450 Series	VOSS 6.0
	VSP 4900 Series	VOSS 8.1
	VSP 7200 Series	VOSS 6.0
	VSP 7400 Series	VOSS 8.0
	VSP 8200 Series	VOSS 6.0
	VSP 8400 Series	VOSS 6.0
	VSP 8600 Series	VSP 8600 6.2
	XA1400 Series	VOSS 8.0.50

The switch supports Bridge Protocol Data Unit (BPDU) Guard 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.

To ensure the correct operation of Spanning Tree in the network, BPDU Guard protects the stability of the Root Bridge by dropping stray, unexpected, or unwanted BPDU packets entering a port, and immediately shutting down those ports for a specified time period. BPDU Guard is normally enabled on access ports connecting to end user devices such as servers that are not expected to operate Spanning Tree.

Use BPDU Guard 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 Guard 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 Guard on a port and the port receives a BPDU, the following actions occur:

1. The guard disables the port.

2. The switch generates an SNMP trap and alarm, and the following log message:

   ```
   BPDU Guard - Port <slot/port> is being shutdown by BPDU Guard,
   timeout <time_seconds>
   ```

3. The port timer begins.

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

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

BPDU Guard is enabled at the interface level. You can configure the BPDU Guard timer for each port, for 10 to 65535 seconds. If you set the port timer to zero, it will not expire.

Rapid Spanning Tree Protocol and Multiple Spanning Tree Protocol

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

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

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

- reduces convergence time after a topology change (from 30 seconds to less than 1 or 2 seconds)

- eliminates unnecessary flushing of the MAC database and the flooding of traffic to the network

- creates backward compatibility with classic 802.1d switches
- creates support for 64 instances of spanning tree in MSTP mode

The following sections relate to RSTP and MSTP:

RSTP interoperability with STP

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.

You must be aware of the following recommendations before you implement MSTP or RSTP:

- The default mode is MSTP. A special boot configuration flag identifies the mode.
- You can lose your configuration if you change the spanning tree mode from MSTP to RSTP and the configuration file contains VLANs configured with MSTI greater than 0. RSTP only supports VLANs configured with the default instance 0.
- For best interoperability results, contact your vendor representative.

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 29: 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 path cost values that support a wide range of link speeds. The following table lists the recommended path cost values.

Table 30: Recommended path cost values

Link speed	Recommended value
Less than or equal to 100 Kbps	200 000 000
1 Mbps	20 000 000
10 Mbps	2 000 000
100 Mbps	200 000
1 Gbps	20 000
10 Gbps	2000
100 Gbps	200
1 Tbps	20
10 Tbps	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).
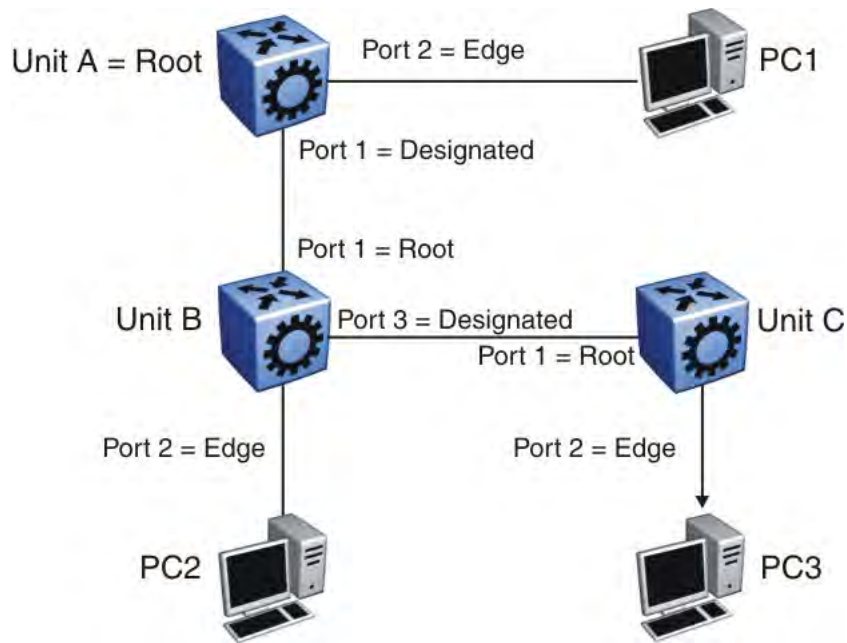
Figure 8: RSTP negotiation process

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 switchil recan exchange BPDUs during the negotiation process, and on the number of switches in the network.

Spanning Tree configuration using CLI

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

❗ **Important:**

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

Configuring Spanning Tree

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the STP mode:

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

Example

Configure the STP mode:

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

Variable definitions

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

Table 31: Variable definitions

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

Configuring BPDU Guard

Configure BPDU Guard 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[/sub-port][-slot/port[/sub-
port]][,...]}
```

> **⊛ Note:**
>
> If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Enable BPDU Guard for the port:

```
spanning-tree bpduguard enable
```

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

```
spanning-tree bpduguard timeout <0, 10-65535>
```

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

```
spanning-tree bpduguard port {slot/port[/sub-port][-slot/port[/
subport]][,...]} enable
```

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

```
spanning-tree bpduguard port {slot/port[/sub-port][-slot/port[/
subport]][,...]} timeout <0-65535>
```

6. Verify the configuration:

```
show spanning-tree bpduguard [GigabitEthernet {slot/port[/sub-port]
[-slot/port[/subport]][,...]}] [{slot/port[/sub-port][-slot/port[/
subport]][,...]}]
```

Example

Enable BPDU Guard on port 1/8, and specify a timer value of 200 seconds. Verify the configuration.

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#interface gigabitEthernet 1/8
Switch:1(config-if)#spanning-tree bpduguard enable
Switch:1(config-if)#spanning-tree bpduguard timeout 200
Switch:1(config-if)#show spanning-tree bpduguard 1/8


============================================================
                            Bpdu Guard
============================================================
Port      PORT           PORT               TIMER   BPDUGUARD
NUM MLTID ADMIN_STATE    OPER_STATE TIMEOUT COUNT   ADMIN_STATE
------------------------------------------------------------
1/8       Up             Up         200     0       Enabled
```

Variable definitions

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

Variable	Value
enable	Enables BPDU Guard on the port. The default is disabled.
port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
timeout *<0, 10-65535>*	Specifies the value to use for port-state recovery. After a BPDU guard 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, the expiry is infinity. |

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

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Configuring Rapid Spanning Tree Protocol

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure RSTP:

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

Example

Configure RSTP:

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

Variable definitions

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

Table 32: Variable definitions

Variable	Value
forward-time <400-3000>	Configures the RSTP forward delay for the bridge in hundredths of a second.
group-stp enable	Enables or disables RSTP for a specific STG. Enter the no form of the command to disable RSTP for the STG (`no spanning-tree rstp group-stp enable`).
hello-time <100-1000>	Assigns the RSTP hello time delay for the bridge in hundredths of a second.
max-age <600-4000>	Assigns the RSTP maximum age time for the bridge in hundredths of a second.
pathcost-type {bits16|bits32}	Assigns the RSTP default pathcost version. The default is 32 bits.
priority <0-61440>	Assigns the RSTP bridge priority.
tx-holdcount <1-10>	Assigns the RSTP transmit hold count from 1 to 10. The default value is 6.
version {rstp/stp-compatible}	Sets the version to RSTP or STP compatible.

Configuring Rapid Spanning Tree Protocol for a port

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

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

> ✱ **Note:**
>
> If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Configure RSTP:

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

Example

Configure RSTP:

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

Variable definitions

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

Table 33: Variable definitions

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

Table continues…

Variable	Value
	required to change this port back to RSTP mode. This process is called Port Protocol Migration.
stp enable	Configures STP for the port.

Configuring the Rapid Spanning Tree Protocol version

Perform this procedure to specify the RSTP mode.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure Rapid Spanning Tree Protocol version:

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

Example

Configure Rapid Spanning Tree Protocol version:

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

Variable definitions

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

Table 34: Variable definitions

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

Viewing the global RSTP configuration information

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View global RSTP configuration information:

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

Example

View global RSTP configuration information:

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

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

Viewing RSTP statistics

Perform this procedure to view RSTP statistics.

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View RSTP statistics:

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

Example

View RSTP statistics:

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

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

Viewing the RSTP status

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View the RSTP status:

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

Example

View the RSTP status:

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

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

Viewing the RSTP Configuration Information

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View RSTP configuration information:

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

   > ✱ **Note:**
   >
   > If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Example

View RSTP configuration information:

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

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

Variable definitions

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

Table 35: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Viewing the RSTP Status for a Port

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View the RSTP status for a port:

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

⭐ **Note:**

If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Example

View the RSTP status for a port:

```
Switch:1> show spanning-tree rstp port status 1/2

================================================================================
                            RSTP Port Status
                         (Port Priority Vector)
================================================================================
Port Number                    : 1/2
Port Designated Root           : 80:00:00:24:7f:9f:60:00
Port Designated Cost           : 0
Port Designated Bridge         : 80:00:00:24:7f:9f:60:00
Port Designated Port           : 80:c1
```

Variable definitions

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

Table 36: Variable definitions

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Viewing RSTP information for a selected port

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the RSTP information for a selected port:

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

Example

View the RSTP information for a selected port:

```
Switch:1# show spanning-tree rstp port statistics 1/4

========================================================================
                        RSTP Port Statistics
========================================================================
Port Number                      : 1/4
Number of Fwd Transitions        : 0
Rx RST BPDUs Count               : 0
Rx Config BPDU Count             : 0
Rx TCN BPDU Count                : 0
Tx RST BPDUs Count               : 9
Tx Config BPDU Count             : 0
Tx TCN BPDU Count                : 0
Invalid RST BPDUs Rx Count       : 0
Invalid Config BPDU Rx Count     : 0
Invalid TCN BPDU Rx Count        : 0
Protocol Migration Count         : 0
```

Variable definitions

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

Variable	Value
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Viewing the RSTP role

View the RSTP role to display the RSTP information.

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View the RSTP role:

   show spanning-tree rstp port role [*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]

Example

View the RSTP role:

```
Switch:1> show spanning-tree rstp port role 1/3
================================================================================
                           RSTP Port Roles and States
================================================================================
Port-Index   Port-Role     Port-State    PortSTPStatus   PortOperStatus
--------------------------------------------------------------------------------
1/3          Designated    Forwarding    Enabled         Enabled
```

Variable definitions

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

Variable	Value
{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Viewing spanning tree configuration

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View spanning tree configuration information:

   ```
   show spanning-tree config
   ```

3. View spanning tree status information:

   ```
   show spanning-tree status
   ```

Example

View spanning tree configuration information:

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

```
================================================================================
                            Spanning Tree Config
================================================================================
            BRIDGE  BRIDGE     FORWARD
ID    PRIORITY MAX_AGE HELLO_TIME DELAY    STATE
--------------------------------------------------------------------------------
0     32768    20      0          15       Enabled
1     32768    20      0          15       Enabled

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

Total number of Spanning Tree IDs :  2
```

View spanning tree status information:

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

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

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

Total number of Spanning Tree IDs :  2
```

Configuring Multiple Spanning Tree Protocol

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure MSTP:

   ```
   spanning-tree mstp
   ```

Example

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

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

Variable Definitions

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

Table 37: Variable definitions

Variable	Value
forward-time <400-3000>	Configures the MSTP forward delay for the bridge from 400 to 3000 hundredths of a second.
max-age <600-4000>	Assigns the MSTP maximum age time for the bridge from 600 to 4000 one hundredths of a second.
max-hop <100-4000>	Assigns the MSTP bridge maximum hop count. The range is 100 to 4000 one hundredths of a second. The original MIB erroneously designated the value in hundredths of a second, when it should have been in hops. The replacement MIB kept the range at 100-4000 to remain backwards compatible. To convert this value to hops, divide by 100 so 100-4000 equals 1-40 hops.
msti <1-63> priority <0–65535>	Assigns the MSTP MSTI instance parameter.
pathcost-type {bits16|bits32}	Assigns the MSTP default pathcost type to either 16 bits or 32 bits. The default is 32 bits.
priority <0-61440>	Assigns the MSTP bridge priority in a range of 0 to 61440 in steps of 4096.

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 switch in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with STP. MSTP spanning tree groups are not the same as STP spanning tree groups. Using a switch 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

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure MSTP MSTI:

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

Example

Configure MSTP MSTI:

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

Variable Definitions

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

Table 38: Variable definitions

Variable	Value
<1-63>	Specifies the instance ID.
<0–65535>	Specifies the priority value. Enter values in increments of 4096: • 4096 • 8192 • 12288 • 16384 • 20480 • 24576 • 28672 • 32768 • 36864 • 40960 • 45056 • 49152 • 53248 • 57344 • 61440

Configuring Ethernet MSTP

Configure Ethernet MSTP on a port to enable this feature.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable

   configure terminal

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

> ⊛ **Note:**
>
> If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Configure Ethernet MSTP:

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

Example

Configure Ethernet MSTP:

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

Variable definitions

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

Table 39: Variable definitions

Variable	Value
cost *<1–200000000>*	Configures the path cost for a port. Valid values are 1 to 200000000
edge-port *<false|true>*	Enables or disables the port as an edge port.
force-port-state enable	Enables STP.
hello-time *<100–1000>*	Configures the hello-time for a port.
msti *<1–63>*	Configures the port MSTP MSTI.
p2p *{auto|force-false|force-true}*	Enables or disables point-to-point for a port.
{slot/port[/sub-port]}	Identifies a single slot and port. If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
priority *<0–240>*	Configures priority for the port.
protocol-migration *{false|true}*	If you chose true, the option initiates protocol migration for a port. If you chose false, the option terminates protocol migration for a port.
	An MSTP-compatible port transmits and receives only RSTP BPDUs. If an MSTP port receives an STP BPDU, it becomes an STP port. User intervention is required to change this port back to MSTP mode. This process is called Port Protocol Migration.

Table continues…

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

Configuring Ethernet MSTP MSTI

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

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

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

   ⭐ **Note:**

   If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Configure Ethernet MSTP MSTI:

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

Example

Configure Ethernet MSTP MSTI:

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

Variable definitions

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

Table 40: Variable definitions

Variable	Value
<1–63>	Specifies the instance ID.
cost <1–200000000>	Configures the path cost for the port
force-port-state enable	Enables MSTI learning for the port.

Table continues…

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If the platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
priority <0–240>	Configures the priority for the port. Enter the priority value (0–240) as increments of 16.

Viewing MSTP configurations

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View the MSTP configurations:

   `show spanning-tree mstp config`

Example

View the MSTP configurations:

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

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

Viewing MSTP status

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View the MSTP status:

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

Example

View the MSTP status:

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

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

Viewing MSTP Port Information

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. View the MSTP port information:

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

> ⊛ **Note:**
>
> If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Example

View the MSTP port information:

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

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

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

Viewing MSTP MSTI Information

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. Show MSTI information:

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

   ⊛ **Note:**

   If your platform supports channelization and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Example

Show MSTI information:

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

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

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

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

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

Variable Definitions

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

Table 41: Variable definitions

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

Viewing MSTP statistics

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

Procedure

1. To enter User EXEC mode, log on to the switch.

2. Show MSTP statistics:

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

Example

Show MSTP statistics:

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

================================================================================
                          MSTP Bridge Statistics
================================================================================
Mstp UP Count                    : 1
Mstp Down Count                  : 0
Region Config Change Count       : 4
Time Since Topology Change       : 0 seconds
Topology Change Count            : 0
New Root Bridge Count            : 1
```

Configuring tc-receive-alarm-threshold

About this task

You can establish a threshold rate for receiving TC/TCN packets by configuring values for count and interval. If the threshold rate is exceeded, you receive a warning message. Use the following procedure to configure values for **tc-receive-alarm-threshold count** and **tc-receive-alarm-threshold interval**.

Procedure

1. Enter Global Configuration mode:

   enable

   configure terminal

2. Configure a value for count:

   spanning-tree tc-receive-alarm-threshold count <1-1000>

3. Configure a value for interval:

   spanning-tree tc-receive-alarm-threshold interval <1-15>

Example

Configure count and interval values:

```
Switch:1>enable
Switch:1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch:1(config)#spanning-tree tc-receive-alarm-threshold count 3
Switch:1(config)#spanning-tree tc-receive-alarm-threshold interval 2
```

Display the alarm threshold configuration:

```
Switch:1#show spanning-tree tc-receive-alarm-threshold

================================================================================
            Spanning Tree TC/TCN Rx Alarm Threshold Configuration
================================================================================
Interval                : 2 minutes
Count                   : 3
```

Variable definitions

Use the data in the following table to use the `tc-receive-alarm-threshold` command.

Variable	Value
count <1-1000>	Specifies the number of packets used to establish the threshold rate. The default is 2.
interval <1-15>	Specifies the time interval (in minutes) used to establish the threshold rate. The default is 1.

Displaying the tc-receive-alarm-threshold configuration

About this task

You can configure a threshold rate for receiving TC/TCN packets. If the threshold is exceeded, you receive a warning message. Use the following procedure to display the tc-receive-alarm-threshold configuration.

Procedure

1. To enter User EXEC mode, log on to the switch.

2. Display the tc-receive-alarm-threshold configuration:

```
show spanning-tree tc-receive-alarm-threshold
```

Example

```
Switch:1(config)#show spanning-tree tc-receive-alarm-threshold

================================================================================
               Spanning Tree TC/TCN Rx Alarm Threshold Configuration
================================================================================
Interval                 : 1 minutes
Count                    : 2
```

Spanning Tree configuration using EDM

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

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

Configuring the Spanning Tree mode

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

> **Important:**
>
> After you change the mode, restart the system for the changes to take effect.

Procedure

1. In the navigation pane, expand the **Configuration** > **VLAN** > **Spanning Tree** folders.

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.

Globals field descriptions

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

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

Restarting the switch

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

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit**.

2. Click **Chassis**.

3. In the System tab, locate the **ActionGroup1** box.

4. Select **saveRuntimeConfig** .

5. Click **Apply**.

6. In the **ActionGroup4** box, select **softReset** .

7. Click **Apply**.

Configure BPDU Guard

Configure BPDU Guard 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 Guard** tab appears as a table-based tab. For more information about how to use a table-based tab, see Configuring User Interfaces and Operating Systems for VOSS.

Procedure

1. In the Device Physical View tab, select a port.

2. In the navigation pane, expand the following folders: **Configuration** > **Edit** > **Port**.

3. Click **General**.

4. Click the **Interface** tab.

5. Select **BpduGuardAdminEnabled** to enable BPDU Guard for the port.

6. **(Optional)** Type a value in **BpduGuardTimeout** to configure the timer for port-state recovery

7. Click **Apply**.

Interface Field Descriptions

Use the data in the following table to use the Interface tab.

Name	Description
Index	Displays the index of the port, written in the slot/port[/sub-port] format.
Name	Configures the name of the port.
Descr	Displays the description of the port. A textual string containing information about the interface.
Type	Displays the type of connector plugged in the port.
Mtu	Displays the Maximum Transmission Unit (MTU) for the port. The size of the largest datagram which can be sent or received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.
PhysAddress	Displays the physical address of the port. The address of the interface at the protocol layer immediately `below' the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.
VendorDescr	Displays the vendor of the connector plugged in the port.
DisplayFormat	Identifies the slot and port numbers (slot/port). If the port is channelized, the format also includes the sub-port in the format slot/port/sub-port
AdminStatus	Configures the port as enabled (up) or disabled (down) or testing. The testing state indicates that no operational packets can be passed.
OperStatus	Displays the current status of the port. The status includes enabled (up) or disabled (down) or testing. The testing state indicates that no operational packets can be passed.
LicenseControlStatus ✴ **Note:** Exception: only supported on VSP 7200 Series.	Shows the port license status.
ShutdownReason	Indicates the reason for a port state change.
LastChange	Displays the timestamp of the last change.
LinkTrap	Enable or disable link trapping.
AutoNegotiate	Enables or disables Auto-Negotiation for this port.

Table continues…

Name	Description
	The default varies depending on the platform: • VSP 4000 Series - Enabled • VSP 4900 Series - Enabled • VSP 7200 Series - Disabled • VSP 7400 Series - Enabled • VSP 8200 Series - Enabled • VSP 8400 Series - Enabled • VSP 8600 Series - Enabled (except 10 Gbps SFP+ ports) • XA1400 Series - Enabled (except 10 Gbps SFP+ ports)
AutoNegAd	Specifies the port speed and duplex abilities to advertise during link negotiation. Supported speeds and duplex modes vary, depending on your hardware. The abilities specified in this object are only used when auto-negotiation is enabled on the port. If all bits in this object are disabled, and auto-negotiation is enabled on the port, then the physical link process on the port will be disabled (if hardware supports this ability). Any change to this configuration restarts the auto-negotiation process, which has the same effect as physically unplugging and reattaching the cable attached to the port. If you select **default**, all capabilities supported by the hardware are advertised.
AdminDuplex	Configures the administrative duplex setting for the port.
OperDuplex	Indicates the operational duplex setting for the port.
AdminSpeed	Configures the administrative speed for the port. 🛈 **Important:** If Auto-Negotiation is disabled and you change the administrative speed on a port that results in a configuration mismatch in speed between two ports, VSP 4450 Series and VSP 4900 Series switches may show an incorrect operational status of "up" for the mismatched ports.
OperSpeed	Indicates the operational speed for the port.

Table continues…

Name	Description
QoSLevel	Selects the Quality of Service (QoS) level for this port. The default is level1.
DiffServ	Enables the Differentiated Service feature for this port. The default is disabled.
Layer3Trust	Configures if the system should trust Layer 3 packets coming from access links or core links only. The default is core.
Layer2Override8021p	Specifies whether Layer 2 802.1p override is enabled (selected) or disabled (cleared) on the port. The default is disabled (clear).
MltId	Shows the MLT ID associated with this port. The default is 0.
Locked	Shows if the port is locked. The default is disabled.
UnknownMacDiscard	Discards packets that have an unknown source MAC address, and prevents other ports from sending packets with that same MAC address as the destination MAC address. The default is disabled.
DirectBroadcastEnable	Specifies if this interface forwards direct broadcast traffic.
OperRouting	Shows the routing status of the port.
HighSecureEnable	Enables or disables the high secure feature for this port.
RmonEnable	Enables or disables Remote Monitoring (RMON) on the interface. The default is disabled.
FlexUniEnable	Enables Flex UNI on the port. The default is disabled.
IngressRateLimit ⊛ **Note:** Exception: only supported on VSP 4900 Series, VSP 7200 Series, VSP 8200 Series, VSP 8400 Series, and XA1400 Series.	Limits the traffic rate accepted by the specified ingress port.
IngressRatePeak	Configures the peak rate in Kbps. The default is 0.
IngressRateSvc	Configures the service rate in Kbps. The default is 0.
EgressRateLimitState	Enables or disables egress port-based shaping to bind the maximum rate at which traffic leaves the port. The default is disabled.
EgressRateLimit	Specifies the egress rate limit in Kbps. Different hardware platforms support different egress rate limits, depending on the port with the highest speed available on the platform. You cannot configure the egress shaper rate to exceed the port capability.

Table continues…

Name	Description
⊛ Note: Exception: only supported on VSP 4000 Series, VSP 4900 Series, VSP 7200 Series, VSP 8200 Series, and VSP 8400 Series.	If you configure this value to 0, shaping is disabled on the port.
TxFlowControl **⊛ Note:** Exception: only supported on VSP 4000 Series, VSP 4900 Series, VSP 7200 Series, VSP 7400 Series, VSP 8200 Series, VSP 8400 Series, and XA1400 Series.	Configures if the port sends pause frames. By default, an interface does not send pause frames. You must also enable the flow control feature globally before an interface can send pause frames.
TxFlowControlOperState	Shows the operational state of flow control.
BpduGuardTimerCount	Shows the time, starting at 0, since the port became disabled. When the BpduGuardTimerCount reaches the BpduGuardTimeout value, the port is enabled. Displays in 1/100 seconds.
BpduGuardTimeout	Specifies the value to use for port-state recovery. After a BPDU guard disables a port, the port remains in the disabled state until this timer expires. You can configure a value of 0 or to 65535. The default is 120 seconds. If you configure the value to 0, the expiry is infinity.
BpduGuardAdminEnabled	Enables BPDU Guard on the port. The default is disabled.
ForwardErrorCorrection	Configures one of the following options for Forward Error Correction (FEC) on the port: • CL 91 • CL 108 • CL 74 • disable • auto The disable option disables this configuration on the port.
ForwardErrorCorrectionApplicability	Displays whether FEC is applicable on the interface.
OperAutoNegotiate	Shows the operational state of Auto-Negotiation.
OperForwardErrorCorrection	Shows the negotiated operational FEC clause. If the value is off, the port supports FEC and is up but not configured for FEC. If the value is notApplicable, the port does not support FEC. If the

Table continues…

Name	Description
	value is unknown, the port supports FEC but is down.
IsPortShared	Indicates whether the port is combo or not. • portShared—Combo port. • portNotShared—Not a combo port.
PortActiveComponent	Specifies whether the copper port is active or fabric port is active if port is a combo port. • fixed port—Copper port is active. • gbic port—Fabric port is active.
Action	Performs one of the following actions on the port • none - none of the following actions • flushMacFdb - flush the MAC forwarding table • flushArp - flush the ARP table • flushIp - flush the IP route table • flushAll - flush all tables • triggerRipUpdate — manually triggers a RIP update The default is none.
Result	Displays the result of the selected action. The default is none.

Configuring RSTP global parameters

Perform this procedure to configure the RSTP global parameters.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.

2. Click **RSTP**.

3. Configure the parameters as required.

4. Click **Apply**.

Globals field descriptions

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

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

Table continues…

Name	Description
	state. The value determines how long the port stays in each of the listening and learning states, which precede the forwarding state. This value is also used after a topology change is detected, and is underway, to age all dynamic entries in the forwarding database.
RstpUpCount	Specifies the number of times the RSTP module is enabled. A trap is generated on the occurrence of this event.
RstpDownCount	Specifies the number of times the RSTP module is disabled. A trap is generated on the occurrence of this event.
NewRootIdCount	Specifies the number of times this bridge detects a root identifier change. A trap is generated on the occurrence of this event.
TimeSinceTopology Change	Specifies the time (in hundredths of a second) since the TcWhile Timer for any port in this bridge was nonzero for Common Spanning Tree.
TopChanges	Specifies the number of times that there was at least one nonzero TcWhile Timer on this bridge for Common Spanning Tree.

Configuring RSTP ports

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

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.

2. Click **RSTP**.

3. Click the **RSTP Ports** tab.

4. Use the fields in the **RSTP Ports** tab to configure the RSTP ports.

5. Click **Apply**.

RSTP Ports field descriptions

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

Name	Description
Port	Specifies a unique value, greater than zero, indicating the port number.

Table continues…

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

Viewing RSTP port status

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

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.

2. Click **RSTP**.

3. In the RSTP tab, click the **RSTP Status** tab.

RSTP Status field descriptions

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

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

Configuring MSTP global parameters

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

Before you begin

- The system must be in MSTP mode.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.

2. Click **MSTP**.

3. Click the **Globals** tab.

4. Configure MSTP as required.

5. Click **Apply**.

Globals field descriptions

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

Name	Description
PathCostDefaultType	Specifies the version of the spanning tree default path costs to be used by this bridge. A value of 8021d1998 denotes the use of the 16-bit default path costs from IEEE 802.1d-1998. A value of stp8021t2001 denotes the use of the 32-bit default path costs from IEEE 802.1t.
TxHoldCount	Specifies the value used by the port transmit state to limit the maximum transmission rate. The default is 3.
MaxHopCount	Assigns the MSTP bridge maximum hop count. The range is 100 to 4000 one hundredths of a second.
	The original MIB erroneously designated the value in hundredths of a second, when it should have been in hops. The replacement MIB kept the range at 100-4000 to remain backwards compatible. To convert this value to hops, divide by 100 so 100-4000 equals 1-40 hops.
NoOfInstancesSupported	Indicates the maximum number of spanning tree instances supported.
MstpUpCount	The number of times the MSTP module is enabled. A trap is generated on the occurrence of this event.
MstpDownCount	The number of times the MSTP module is disabled. A trap is generated on the occurrence of this event.
ForceProtocolVersion	Specifies the version of Spanning Tree Protocol that the bridge currently runs. stpCompatible indicates that the Spanning Tree Protocol as specified in IEEE 802.1d is in use; rstp indicates that the Rapid Spanning Tree Protocol as specified in IEEE 802.1w is in use; and mstp indicates that the multiple spanning tree protocol as specified in IEEE 802.1s is in use.
	Although STP and MSTP are variations of the same spanning tree protocol, they communicate information differently. A switch in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with STP. MSTP spanning tree groups are not the same as STP spanning tree groups. Using a switch in MSTP mode with a chassis in STP mode can create a loop in the network.
	The default is MSTP.
BrgAddress	Specifies the MAC address used by this bridge if it must be referred to in a unique fashion. It is recommended that this should be the numerically smallest MAC address of all ports that belong to this

Table continues…

Name	Description
	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.
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

Table continues…

Name	Description
	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 tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.

2. Click **MSTP**.

3. Click the **CIST Port** tab.

> ✳ **Note:**
>
> The MSTP, CIST Port tab contains information for each port that is common to all bridge and spanning tree instances.

4. Use the fields in the **CIST Port** box to configure the MSTP CIST port.

5. Click **Apply**.

CIST Port field descriptions

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

Name	Description
Port	Specifies the port number of the port for which this entry contains spanning tree information.
PathCost	Specifies the contribution of this port to the path cost of paths towards the CIST root that includes this port.
Priority	Specifies the four most significant bits of the port identifier of the spanning tree instance which are modified by setting the CistPortPriority value. The values that are configured for port priority must be in steps of 16.
	Although port priority values can range from 0 to 255, only the following values are used: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
	The default is 128.
DesignatedRoot	Specifies the unique bridge identifier of the bridge recorded as the CIST root in the configuration BPDUs transmitted.
DesignatedCost	Specifies the path cost of the designated port of the segment that connects to this port.
DesignatedBridge	Specifies the unique bridge identifier of the bridge which that port considers to be the designated bridge for the ports segment.
DesignatedPort	Specifies the port identifier of the port on the designated bridge for this port segment.
RegionalRoot	Specifies the unique bridge identifier of the bridge recorded as the CIST regional root identifier in the configuration BPDUs transmitted.
RegionalPathCost	Specifies the contribution of this port to the path cost of paths towards the CIST regional root that include this port.
ProtocolMigration	Indicates the protocol migration state of this port. If you chose true, the option initiates protocol migration

Table continues…

Name	Description
	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.
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.

Table continues…

Name	Description
	Although STP and MSTP are variations of the same spanning tree protocol, they communicate information differently. A switch in MSTI mode cannot recognize the spanning tree groups running on a chassis configured with STP. MSTP spanning tree groups are not the same as STP spanning tree groups. Using a switch in MSTP mode with another chassis in STP mode can create a loop in the network.
EffectivePortState	Specifies the effective operational state of the port for CIST. This is true only if the port is operationally up at the interface and protocol levels for CIST. This is configured to false for all other conditions.
State	Specifies the current state of the port as defined by the common spanning tree protocol. It can be disabled, discarding, learning, or forwarding.
ForcePortState	Specifies the current state of the port. You can change the port to either Disabled or Enabled for the base spanning tree instance.
SelectedPortRole	Specifies the selected port role of the port for this spanning tree instance.
CurrentPortRole	Specifies the current port role of the port for this spanning tree instance.

Configuring MSTI bridges for MSTP

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

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.

2. Click **MSTP**.

3. Click the **MSTI Bridges** tab.

   ✱ **Note:**

   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.
InstanceUpCount	Specifies the number of times a new spanning tree instance is created. A trap is generated on the occurrence of this event.
InstanceDownCount	Specifies the number of times a spanning tree instance is deleted. A trap is generated on the occurrence of this event.

Configuring MSTI ports for MSTP

Perform the following procedure to configure MSTI ports for MSTP.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **VLAN** > **Spanning Tree**.

2. Click **MSTP**.

3. Click the **MSTI Port** tab.

> ✳ **Note:**
>
> 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 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.

Table continues…

Name	Description
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

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.

command line interface (CLI)
A textual user interface. When you use CLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.

common and internal spanning tree (CIST)
The single spanning tree calculated by the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP) to ensure that all LANs in a bridged Local Area Network (LAN) are simply and fully connected.

common spanning tree (CST)
The single spanning tree calculated by STP, RSTP, and MSTP to connect multiple spanning tree (MST) regions.

Enterprise Device Manager (EDM)
A web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.

forwarding database (FDB)
A database that maps a port for every MAC address. If a packet is sent to a specific MAC address, the switch refers to the forwarding database for the corresponding port number and sends the data packet through that port.

Institute of Electrical and Electronics Engineers (IEEE)
An international professional society that issues standards and is a member of the American National Standards Institute, the International Standards Institute, and the International Standards Organization.

Internet Control Message Protocol (ICMP)
A collection of error conditions and control messages exchanged by IP modules in both hosts and gateways.

Layer 2
Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.

Local Area Network (LAN)
A data communications system that lies within a limited spatial area, uses a specific user group and topology, and can connect to a public switched telecommunications network (but is not one).

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

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