JUNIPER NETWORKS

Junos® OS

Spanning-Tree Protocols Feature Guide

Release
16.2

Modified: 2016-11-15

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS Spanning-Tree Protocols Feature Guide
16.2

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- MX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

Table 1 on page xiii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xiii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/

- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

CHAPTER 1

Understanding Spanning-Tree Protocols

Understanding Spanning Tree Protocol Used for Eliminating Bridge Loops in Ethernet LANs

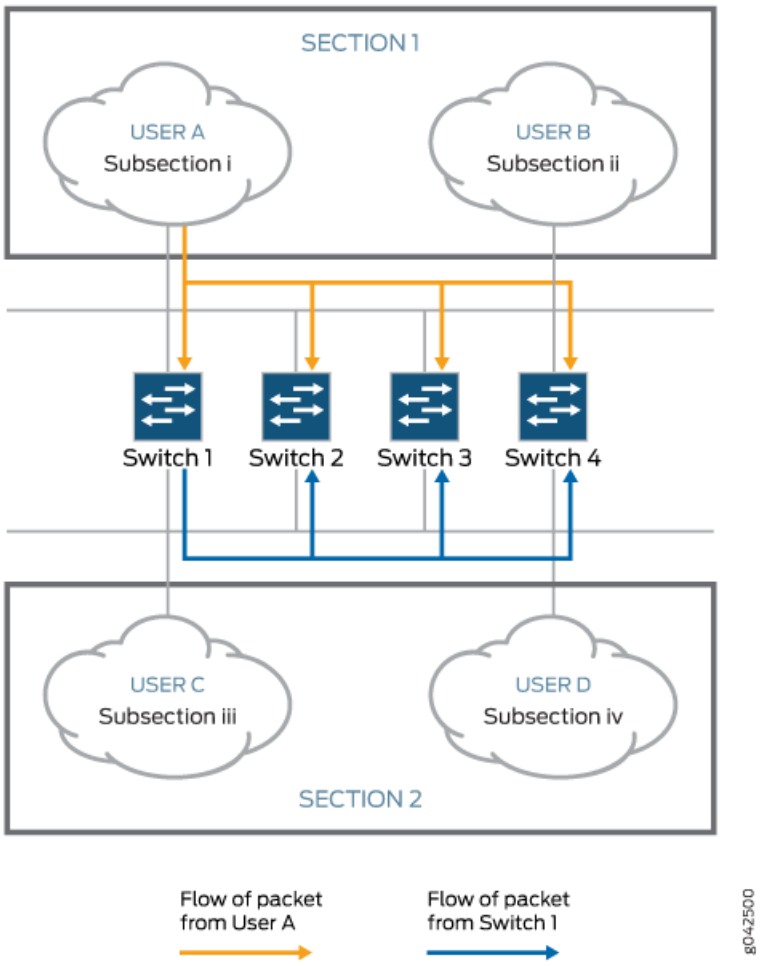
The Spanning Tree Protocol (STP) is a network protocol that is used to eliminate bridge loops in Ethernet LANs. STP prevents network loops and associated network outage by blocking redundant links or paths. The redundant paths can be used to keep the network operational if the primary link fails.

The sections describe bridge loops and how STP helps eliminate them.

Understanding Bridge Loops

To understand bridge loops, consider a scenario in which four switches (or bridges) are connected to four different subsections (Subsection i, ii, iii, and iv) where each subsection is a collection of network nodes (see Figure 1 on page 18). For simplicity, Subsection i and Subsection ii are combined to form Section 1. Similarly, Subsection iii and Subsection iv are combined to form Section 2.

Figure 1: Formation of Bridge Loops



When the switches are powered on, the bridge tables are empty. If User A in Subsection i tries to send a single packet Packet 1 to User D in Subsection iv, all the switches, which are in listening mode, receive the packet. The switches make an entry in their respective bridging tables, as shown in the following table:

Bridge 1 ID | Port Facing Direction	Bridge 2 ID | Port Facing Direction	Bridge 3 ID | Port Facing Direction	Bridge 4 ID | Port Facing Direction
Packet 1 | Section 1	Packet 1 | Section 1	Packet 1 | Section 1	Packet 1 | Section 1

At this point, the switches do not know where Subsection iv is, and the packet is forwarded to all the ports except the source port (which results in flooding of the packet). In this example, after Subsection 1 sends the packet, the switches receive the packet on the ports facing Section 1. As a result, they start forwarding the packet through the ports facing Section 2. Which switch gets the first chance to send out the packet depends on

the network configuration. In this example, suppose Switch 1 transmits the packet first. Because it received the packet from Section 1, it floods the packet toward Section 2. Similarly, Switches 2, 3, and 4, which are also in listening mode, receive the same packet from Switch 1 (originally sent from Section 1) on the ports facing Section 2. They readily update their bridging tables with incorrect information, as shown in the following table:

Bridge 1 ID | Port Facing Direction	Bridge 2 ID | Port Facing Direction	Bridge 3 ID | Port Facing Direction	Bridge 4 ID | Port Facing Direction
Packet 1 | Section 1	Packet 1 | Section 2	Packet 1 | Section 2	Packet 1 | Section 2

Thus, a loop is created as the same packet is received both from Section 1 and Section 2. As illustrated in Figure 1 on page 18, Switch 1 has information that the packet came from Subsection i in Section 1, whereas all other switches have incorrect information that the same packet came from Section 2.

The entire process is repeated when Switch 2 gets the chance to transmit the original packet. Switch 2 receives the original packet from Section 1 and transmits the same packet to Section 2. Eventually, Switch 1, which still has no idea where Subsection iv is, updates its bridging table, as shown in the following table:

Bridge 1 ID | Port Facing Direction	Bridge 2 ID | Port Facing Direction	Bridge 3 ID | Port Facing Direction	Bridge 4 ID | Port Facing Direction
Packet 1 | Section 2	Packet 1 | Section 2	Packet 1 | Section 2	Packet 1 | Section 2

In complex networks, this process can quickly lead to huge packet transmission cycles as the same packet is sent repeatedly.

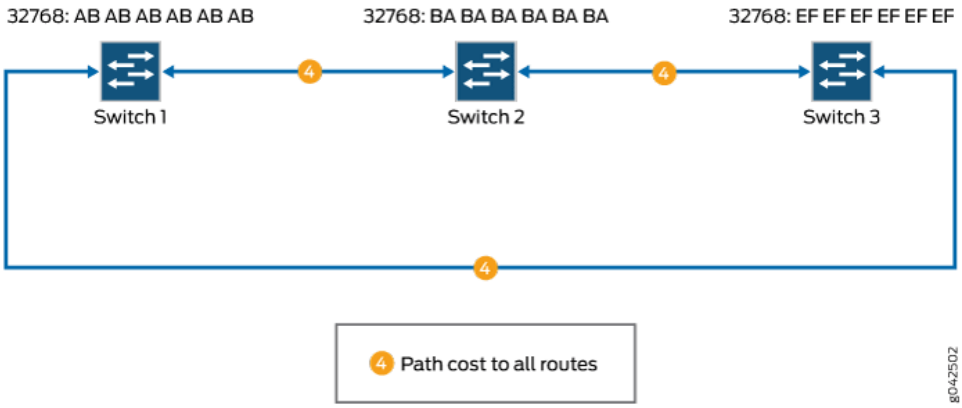
How STP Helps Eliminate Loops

Spanning Tree Protocol helps eliminate loops in a network by turning off additional routes that can create a loop. The blocked routes are enabled automatically if the primary path gets deactivated.

To understand the steps followed by STP in eliminating bridge loops, consider the following example where three switches are connected to form a simple network (see Figure 2 on page 20). To maintain redundancy, more than one path exists between each device. The switches communicate with each other by using Bridge Protocol Data Units (BPDUs) sent every 2 seconds.

NOTE: BPDUs are frames that consist of bridge ID, the bridge port where it originates, the priority of the bridge port, cost of the path and so on. BPDUs are sent as multicast MAC address 01:80:c2:00:00:00. BPDUs can be of three types: configuration BPDUs, topology change notification (TCN) BPDUs, and topology change acknowledgment (TCA) BPDUs.

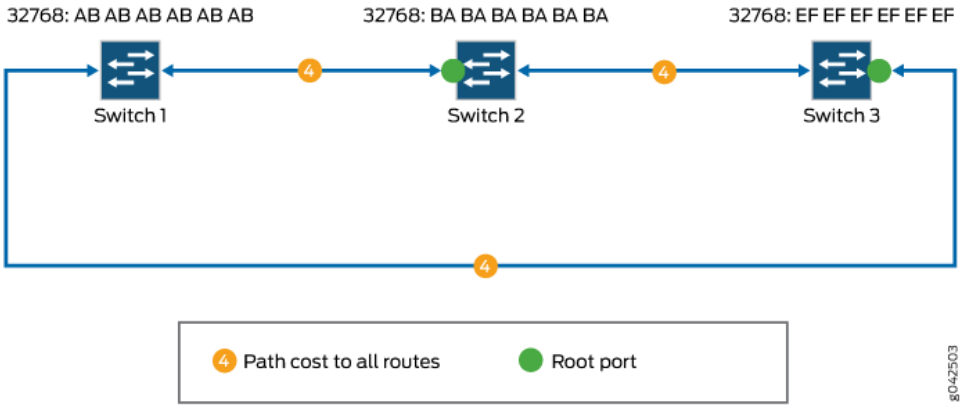
Figure 2: Simple Network with Redundant Links



To eliminate network loops, STP performs the following steps in this sample network:

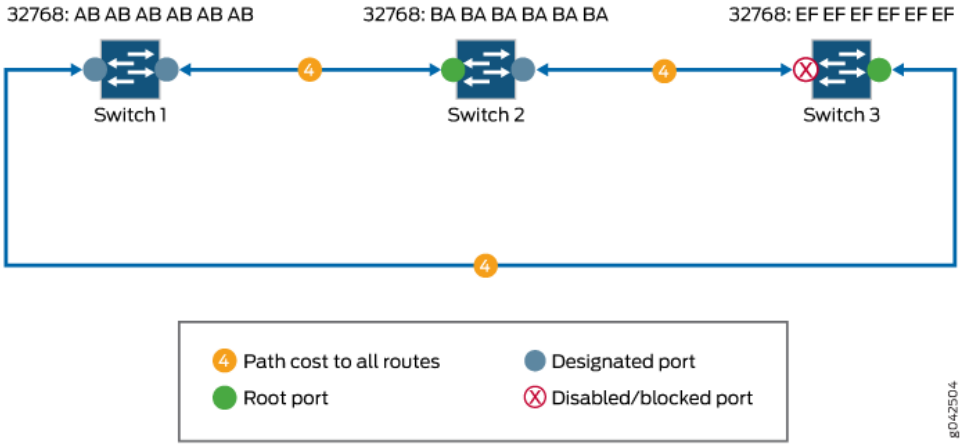
1. *Elects a root bridge (or switch).* To elect a root switch, STP uses the bridge ID. The bridge ID is 8 bytes in length and consists of two parts. The first part is 2 bytes of information known as bridge priority. The default bridge priority is 32,768. In this example, the default value is used for all the switches. The remaining 6 bytes consist of the MAC address of the switch. In this example, Switch1 is elected as the root switch because it has the lowest MAC address.
2. *Elects the root ports.* Typically, root ports use the least-cost paths from one switch to the other. In this example, assume that all paths have similar costs. Therefore, the root port for Switch 2 is the port that receives packets through the direct path from Switch 1 (cost 4), because the other path is through Switch 3 (cost 4 + 4) as shown in Figure 3 on page 20. Similarly, for Switch 3, the root port is the one that uses the direct path from Switch 1.

Figure 3: Electing Root Ports



3. *Selects the designated ports.* Designated ports are the only ports that can receive and forward frames on switches other than the root switch. They are generally the ports that use the least-cost paths. In Figure 4 on page 21, the designated ports are marked.

Figure 4: Selecting Designated Ports and Blocking Redundant Paths



Because there is more than one path involved in the network and the root ports and designated ports are identified, STP can block the path between Switch 2 and Switch 3 temporarily, eliminating any Layer 2 loops.

Types of Spanning-Tree Protocols Supported

In a Layer 2 environment, you can configure various spanning-tree protocol versions to create a loop-free topology in Layer 2 networks.

A spanning-tree protocol is a Layer 2 control protocol (L2CP) that calculates the best path through a switched network containing redundant paths. A spanning-tree protocol uses bridge protocol data unit (BPDU) data frames to exchange information with other switches. A spanning-tree protocol uses the information provided by the BPDUs to elect a root bridge, identify root ports for each switch, identify designated ports for each physical LAN segment, and prune specific redundant links to create a loop-free tree topology. The resulting tree topology provides a single active Layer 2 data path between any two end stations.

NOTE: In discussions of spanning-tree protocols, the terms *bridge* and *switch* are often used interchangeably.

The Juniper Networks MX Series 3D Universal Edge Routers and EX Series switches support STP, RSTP, MSTP, and VSTP.

- The original Spanning Tree Protocol (STP) is defined in the IEEE 802.1D 1998 specification. A newer version called Rapid Spanning Tree Protocol (RSTP) was originally defined in the IEEE 802.1w draft specification and later incorporated into the IEEE 802.1D-2004 specification. A recent version called Multiple Spanning Tree Protocol (MSTP) was originally defined in the IEEE 802.1s draft specification and later incorporated into the IEEE 802.1Q-2003 specification. The VLAN Spanning Tree Protocol (VSTP) is compatible with the Per-VLAN Spanning Tree Plus (PVST+) and Rapid-PVST+ protocols supported on Cisco Systems routers and switches.
- RSTP provides faster reconvergence time than the original STP by identifying certain links as point to point and by using protocol handshake messages rather than fixed timeouts. When a point-to-point link fails, the alternate link can transition to the forwarding state without waiting for any protocol timers to expire.
- MSTP provides the capability to logically divide a Layer 2 network into regions. Every region has a unique identifier and can contain multiple instances of spanning trees. All regions are bound together using a Common Instance Spanning Tree (CIST), which is responsible for creating a loop-free topology *across* regions, whereas the Multiple Spanning-Tree Instance (MSTI) controls topology *within* regions. MSTP uses RSTP as a converging algorithm and is fully interoperable with earlier versions of STP.
- VSTP maintains a separate spanning-tree instance for each VLAN. Different VLANs can use different spanning-tree paths. When different VLANs use different spanning-tree paths, the CPU processing resources being consumed increase as more VLANs are configured. VSTP BPDU packets are tagged with the corresponding VLAN identifier and are transmitted to the multicast destination media access control (MAC) address **01-00-0c-cc-cc-cd** with a protocol type of **0x010b**. VSTP BPDUs are tunneled by pure IEEE 802.1q bridges.

Understanding BPDUs Used for Exchanging Information Among Bridges

In a Layer 2 bridge environment, spanning-tree protocols use data frames called Bridge Protocol Data Units (BPDUs) to exchange information among bridges.

Spanning-tree protocols on peer systems exchange BPDUs, which contain information about port roles, bridge IDs, and root path costs. On each MX Series router or EX Series switch, the spanning-tree protocol uses this information to elect a root bridge, identify root ports for each switch, identify designated ports for each physical LAN segment, and prune specific redundant links to create a loop-free tree topology. The resulting tree topology provides a single active Layer 2 data path between any two end stations.

NOTE: In discussions of spanning-tree protocols, the terms *bridge* and *switch* are often used interchangeably.

The transmission of BPDUs is controlled by the Layer 2 Control Protocol process (l2cpd) on MX Series 3D Universal Edge Routers.

The transmission of periodic packets on behalf of the l2cpd process is carried out by periodic packet management (PPM), which, by default, is configured to run on the Packet Forwarding Engine. The ppmd process on the Packet Forwarding Engine ensures that the BPDUs are transmitted even when the l2cpd process control plane is unavailable, and keeps the remote adjacencies alive during a unified in-service software upgrade (unified ISSU). However, if you want the distributed PPM (ppmd) process to run on the Routing Engine instead of the Packet Forwarding Engine, you can disable the ppmd process on the Packet Forwarding Engine. For more information, see the *Junos OS High Availability Library for Routing Devices*.

On MX Series routers or EX Series switches with redundant Routing Engines (two Routing Engines that are installed in the same router), you can configure nonstop bridging. Nonstop bridging enables the router to switch from a primary Routing Engine to a backup Routing Engine without losing Layer 2 Control Protocol (L2CP) information. Nonstop bridging uses the same infrastructure as graceful Routing Engine switchover (GRES) to preserve interface and kernel information. However, nonstop bridging also saves L2CP information by running the l2cpd process on the backup Routing Engine.

NOTE: **To use nonstop bridging, you must first enable GRES.**

Nonstop bridging is supported for the following Layer 2 control protocols:

- Spanning-Tree Protocol (STP)
- Rapid Spanning-Tree Protocol (RSTP)
- Multiple Spanning-Tree Protocol (MSTP)

For more information about GRES and nonstop bridging, see the *Junos OS High Availability Library for Routing Devices*.

Related Documentation

- Understanding Loop Protection for Spanning-Tree Instance Interfaces on page 66
- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69
- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57

Forward Delay Before Ports Transition to Forwarding State

The forwarding delay timer specifies the length of time a spanning-tree protocol bridge port remains in the listening and learning states before transitioning to the forwarding state. Setting the interval too short could cause unnecessary spanning-tree reconvergence. Before changing this parameter, you should have a thorough understanding of spanning-tree protocols.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring VLAN Spanning Tree Protocol on page 36

- forward-delay on page 108

CHAPTER 2

Configuring Spanning-Tree Protocols

Spanning-Tree Instance Interface

STP and RSTP are limited to a single instance on any physical interface. Use the **interface** statement to configure which interfaces participate in the STP or RSTP instance.

MSTP supports multiple instances on a single physical interface. Use the **interface** statement to configure which logical interfaces participate in MSTP.

For VSTP, interfaces can be configured at the global level or at the VLAN level. Interfaces configured at the global VSTP level will be enabled for all the configured VLANs. If an interface is configured at both the global and VLAN levels, the configuration at the VLAN level overrides the global configuration.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring VLAN Spanning Tree Protocol on page 36
- **cost on page 103**
- **edge on page 105**
- **interface (Spanning Tree) on page 110**
- **mode on page 113**
- **priority on page 117**

Spanning-Tree Instance Interface Priority

The root port is the interface on the nonroot bridge with the lowest path cost to the root bridge. When multiple interfaces have the same path cost to the root bridge, the interface with the lowest interface priority is selected as the root port.

If the interface priority is not configured and multiple interfaces have the same path cost to the root bridge, the interface with the lowest interface identifier is selected as the root port.

If the interface priority is configured under the MSTP protocol, this becomes the default value for all interfaces. If the interface priority is configured under the MSTI interface, the value overrides the default for that interface.

If the interface priority is configured at both the VSTP global and VLAN levels, the configuration at the VLAN level overrides the global configuration.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring VLAN Spanning Tree Protocol on page 36
- **interface (Spanning Tree) on page 110**
- **priority on page 117**

Spanning-Tree Instance Interface Cost

The path cost used to calculate the root path cost from any given LAN segment is determined by the total cost of each link in the path. By default, the link cost is determined by the speed of the link. The interface cost can be configured to override the default cost and control which bridge is the designated bridge and which port is the designated port. In MSTP the CIST external path cost is determined by the link speed and the number of hops.

If the interface cost is not configured, the cost is determined by the speed of the interface. For example, a 100-Mbps link has a default path cost of 19, a 1000-Mbps link has a default path cost of 4, and a 10-Gbps link has a default path cost of 2.

If the interface cost is configured under MSTP, this becomes the default value for all interfaces. If the interface cost is configured under the MSTI interface, the value overrides the default for that interface.

If the interface cost is configured at both the VSTP global and VLAN levels, the configuration at the VLAN level overrides the global configuration.

The interface cost should be set the same for all interfaces connected to the same LAN segment.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring VLAN Spanning Tree Protocol on page 36
- **cost on page 103**
- **interface (Spanning Tree) on page 110**

Spanning-Tree Instance Interface Point-to-Point Link Mode

The interface mode allows RSTP, MSTP, and VSTP to converge faster than the original STP on point-to-point links. The protocol does not need to wait for timers on point-to-point links. Configure interfaces that have a point-to-point link to another Layer 2 bridge as **p2p**. This parameter is ignored if the STP is configured to run the original spanning-tree version.

If the interface mode is configured at both the VSTP global and VLAN levels, the configuration at the VLAN level overrides the global configuration.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring VLAN Spanning Tree Protocol on page 36
- **mode on page 113**
- **interface (Spanning Tree) on page 110**

Spanning-Tree Protocol Trace Options

In order to trace spanning-tree protocol operations, you can set spanning-tree protocol-specific trace options in the spanning-tree protocol configuration.

For general information about tracing and global tracing options, see the statement summary for the global **traceoptions** statement in the *Junos OS Routing Protocols Library*.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring VLAN Spanning Tree Protocol on page 36
- Example: Tracing Spanning-Tree Protocol Operations on page 91
- **traceoptions (Spanning Tree) on page 122**

Configuring Rapid Spanning Tree Protocol

You can configure Rapid Spanning Tree Protocol (RSTP) under the following hierarchy levels:

- **[edit *logical-systems logical-system-name* protocols]**
- **[edit *logical-systems logical-system-name routing-instances routing-instance-name* protocols]**
- **[edit protocols]**
- **[edit *routing-instances routing-instance-name* protocols]**

The routing instance type can be either **virtual-switch** or **layer2-control**.

To configure the Rapid Spanning Tree Protocol:

1. Enable RSTP as the version of spanning-tree protocol to be configured:

   ```
   [edit]
   user@host@ edit ... protocols (STP Type) rstp
   ```

2. (Optional) For compatibility with older bridges that do not support RSTP, you can force RSTP to run as the original IEEE 802.1D Spanning Tree Protocol (STP) version:

   ```
   [edit ... protocols rstp]
   user@host# set force-version stp
   ```

   NOTE: If RSTP has been forced to run as the original STP version, you can revert back to RSTP by first removing the **force-version** statement from the configuration and then entering the clear spanning-tree protocol-migration configuration mode command.

3. (Optional) Enable provider bridge participation in the RSTP instance:

   ```
   [edit ... protocols rstp]
   ```

```
user@host# set bpdu-destination-mac-address provider-bridge-group
```

4. (Optional) Specify the extended system identifier used in identifiers bridges that participate in RSTP:

   ```
   [edit ... protocols rstp]
   user@host# set extended-system-id identifier
   ```

5. Configure the interfaces that participate in the RSTP instance.

   a. Enable configuration of the interface:

      ```
      [edit ... protocols rstp]
      user@host# edit interface interface-name
      ```

   b. Configure the interface priority:

      ```
      [edit ... protocols rstp interface interface-name]
      user@host# set priority interface-priority
      ```

   c. (Optional) By default, the interface link cost is determined by the link speed. You can configure the interface link cost to control which bridge is the designated bridge and which port is the designated port:

      ```
      [edit ... protocols rstp interface interface-name]
      user@host# set cost interface-link-cost
      ```

   d. Configure the interface link mode to identify point-to-point links:

      ```
      [edit ... protocols rstp interface interface-name]
      user@host# set mode (p2p | shared)
      ```

      Specify **p2p** if the link is point to point. Specify **shared** if the link is a shared media.

   e. (Optional) Configure the interface as an edge port:

      ```
      [edit ... protocols rstp interface interface-name]
      user@host# set edge
      ```

      Edge ports do not expect to receive bridge protocol data unit (BPDU) packets. If a BPDU packet is received for an edge port, the port becomes a non-edge port

   You can also enable BPDU root protection for all spanning-tree protocol instances on the interface. BPDU root protect ensures the port is the spanning-tree designated port. If the port receives superior BPDU packets, root protect moves this port to a root-prevented spanning-tree state. For configuration details, see "Checking the Status of Spanning-Tree Instance Interfaces" on page 87.

6. Configure the bridge priority:

   ```
   [edit ... protocols rstp]
   user@host# set bridge-priority bridge-priority
   ```

   For more information, see "Bridge Priority for Election of Root Bridge and Designated Bridge" on page 51.

7. Configure hello BPDU timers.

   a. Configure the maximum expected arrival time of hello BPDUs:

      ```
      [edit ... protocols rstp]
      user@host# set max-age seconds
      ```

   b. Configure the time interval at which the root bridge transmits configuration BPDUs:

      ```
      [edit ... protocols rstp]
      user@host# set hello-time seconds
      ```

8. (Optional) By default, the bridge port remains in the listening and learning states for 15 seconds before transitioning to the forwarding state. You can specify a delay from **4** through **20** seconds instead:

   ```
   [edit ... protocols rstp]
   user@host# set forward-delay seconds
   ```

9. Verify the RSTP configuration:

   ```
   [edit]
   ... { # Optional logical system and/or routing instance
     protocols (STP Type) {
       rstp {
         force-version stp; # Optional.
         bpdu-destination-mac-address provider-bridge-group; # Optional
         extended-system-id identifier; # Optional.
         interface interface-name {
           priority interface-priority;
           cost interface-link-cost; # Optional.
           mode (p2p | shared);
           edge; # Optional.
         }
         bridge-priority bridge-priority;
         max-age seconds;
         hello-time seconds;
         forward-delay seconds; # Optional.
       }
     }
   }
   ```

Related Documentation

- RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 53
- Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 52
- Provider Bridge Participation in RSTP or MSTP Instances on page 51
- System Identifier for Bridges in STP or RSTP Instances on page 51

Configuring Multiple Spanning Tree Protocol

You can configure the Multiple Spanning Tree Protocol (MSTP) under the following hierarchy levels:

- [edit *logical-systems logical-system-name* protocols]
- [edit *logical-systems logical-system-name routing-instances routing-instance-name* protocols]
- [edit protocols]
- [edit *routing-instances routing-instance-name* protocols]

The routing instance type can be either virtual-switch or layer2-control.

To configure the Multiple Spanning Tree Protocol:

1. Enable MSTP as the version of spanning-tree protocol to be configured:

   ```
   [edit]
   user@host@ edit ... protocols (STP Type) mstp
   ```

2. (Optional) Enable provider bridge participation in the MSTP instance:

   ```
   [edit ... protocols mstp]
   user@host# set bpdu-destination-mac-address provider-bridge-group
   ```

3. Configure the interfaces that participate in the MSTP instance.

   a. Enable configuration of the interface:

      ```
      [edit ... protocols mstp]
      user@host# edit interface interface-name
      ```

   b. Configure the interface priority:

      ```
      [edit ... protocols mstp interface interface-name]
      user@host# set priority interface-priority
      ```

   c. (Optional) By default, the interface link cost is determined by the link speed. You can configure the interface link cost to control which bridge is the designated bridge and which port is the designated port:

      ```
      [edit ... protocols mstp interface interface-name]
      user@host# set cost interface-link-cost
      ```

   d. Configure the interface link mode to identify point-to-point links:

      ```
      [edit ... protocols mstp interface interface-name]
      user@host# set mode (p2p | shared)
      ```

      Specify **p2p** if the link is point to point. Specify **shared** if the link is a shared media.

   e. (Optional) Configure the interface as an edge port:

      ```
      [edit ... protocols mstp interface interface-name]
      user@host# set edge
      ```

      Edge ports do not expect to receive bridge protocol data unit (BPDU) packets. If a BPDU packet is received for an edge port, the port becomes a non-edge port

   You can also enable BPDU root protection for all spanning-tree protocol instances on the interface. BPDU root protect ensures the port is the spanning-tree designated port. If the port receives superior BPDU packets, root protect moves this port to a root-prevented spanning-tree state. For configuration details, see "Checking the Status of Spanning-Tree Instance Interfaces" on page 87.

4. Configure the bridge priority:

   ```
   [edit ... protocols mstp]
   user@host# set bridge-priority bridge-priority
   ```

   For more information, see "Bridge Priority for Election of Root Bridge and Designated Bridge" on page 51.

5. Configure hello BPDU timers.

   a. Configure the maximum expected arrival time of hello BPDUs:

      ```
      [edit ... protocols mstp]
      user@host# set max-age seconds
      ```

   b. Configure the time interval at which the root bridge transmits configuration BPDUs:

      ```
      [edit ... protocols mstp]
      user@host# set hello-time seconds
      ```

6. (Optional) By default, the bridge port remains in the listening and learning states for 15 seconds before transitioning to the forwarding state. You can specify a delay from **4** through **20** seconds instead:

   ```
   [edit ... protocols mstp]
   ```



```
user@host# set forward-delay seconds
```

7. Configure MSTP-specific options.

   a. Configure the MSTP region configuration name:

   ```
   [edit ... protocols mstp]
   user@host# set configuration-name configuration-name
   ```

   b. Configure the MSTP revision level:

   ```
   [edit ... protocols mstp]
   user@host# set revision-level revision-level
   ```

   c. Configure the maximum number of hops a BPDU can be forwarded in the MSTP region:

   ```
   [edit ... protocols mstp]
   user@host# set max-hops hops
   ```

8. Verify the MSTP configuration:

```
[edit]
... { # Optional logical system and/or routing instance
  protocols (STP Type) {
    mstp {
      bpdu-destination-mac-address provider-bridge-group; # Optional
      interface interface-name {
        priority interface-priority;
        cost interface-link-cost; # Optional.
        mode (p2p | shared);
        edge; # Optional.
      }
      bridge-priority bridge-priority;
      max-age seconds;
      hello-time seconds;
      forward-delay seconds; # Optional.
      configuration-name configuration-name; # MST region configuration name.
      revision-level revision-level; # MST revision number.
      max-hops hops; # MST maximum hops.
    }
  }
}
```

Related Documentation

- Configuring MST Instances on a Physical Interface on page 34
- Disabling MSTP on page 35

Configuring MST Instances on a Physical Interface

You can configure a Multiple Spanning Tree Instance (MSTI) under the following hierarchy levels:

- **[edit** ***logical-systems logical-system-name*** protocols mstp**]**
- **[edit** ***logical-systems logical-system-name routing-instances routing-instance-name*** protocols mstp**]**
- **[edit** protocols mstp**]**
- **[edit** ***routing-instances routing-instance-name*** protocols mstp**]**

The routing instance type can be either **virtual-switch** or **layer2-control**.

Before you begin, configure Multiple Spanning-Tree Protocol. For configuration details, see "Configuring MSTP" on page 31.

1. Enable configuration of an MST instance:

   ```
   [edit]
   user@host# edit ... protocols mstp msti msti-id
   ```

   The *msti-id* value must be from **1** through **64**.

2. Configure the interfaces that participate in the MST instance.

   a. Enable configuration of the interface:

      ```
      [edit ... protocols mstp msti msti-id]
      user@host# edit interface interface-name
      ```

   b. Configure the interface priority:

      ```
      [edit ... protocols mstp msti msti-id interface interface-name]
      user@host# set priority interface-priority
      ```

   c. (Optional) By default, the interface link cost is determined by the link speed. You can configure the interface link cost to control which bridge is the designated bridge and which port is the designated port:

      ```
      [edit ... protocols mstp msti msti-id interface interface-name]
      user@host# set cost interface-link-cost
      ```

   d. (Optional) Configure the interface as an edge port:

      ```
      [edit ... protocols mstp msti msti-id interface interface-name]
      user@host# set edge
      ```

      Edge ports do not expect to receive bridge protocol data unit (BPDU) packets. If a BPDU packet is received for an edge port, the port becomes a non-edge port

3. Configure the bridge priority:

   ```
   [edit ... protocols mstp msti msti-id]
   user@host# set bridge-priority bridge-priority
   ```

   For more information, see "Bridge Priority for Election of Root Bridge and Designated Bridge" on page 51.

4. (Optional) An MSTI can map to a range of VLANs just as a logical port can map to a range of VLANs. The MSTP VLAN specifies the VLAN or VLAN range to which this MSTI is mapped. The vlan-id is configured under the logical interface. Configure the VLAN or VLAN range of the MSTI instance:

   ```
   [edit]
   user@host#  set vlan (vlan-id | vlan-id-range)
   ```

5. Verify the MST interface configuration.

   ```
   [edit]
   protocols {
     mstp {
       ...basic-mstp-configuration...
       msti msti-id { # Instance identifier 1 – 64.
         bridge-priority priority;
         vlan vlan-id; # Optional
         interface interface-name {
           cost cost;
           edge;
           priority interface-priority;
         }
       }
     }
   }
   ```

Related Documentation

- Configuring Multiple Spanning Tree Protocol on page 31
- Disabling MSTP on page 35

Disabling MSTP

To disable the entire MSTP instance:

- Include the **disable** statement. You can include this statement at the following hierarchy levels:
  - **[edit *logical-systems logical-system-name* protocols mstp]**
  - **[edit *logical-systems logical-system-name routing-instances routing-instance-name* protocols mstp]**
  - **[edit protocols mstp]**
  - **[edit *routing-instances routing-instance-name* protocols mstp]**

Related Documentation

- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring MST Instances on a Physical Interface on page 34

Configuring VLAN Spanning Tree Protocol

You can configure the VLAN Spanning Tree Protocol (VSTP) under the following hierarchy levels:

NOTE: This task supports the Enhanced Layer 2 Software (ELS) configuration style.

- **[edit logical-systems** *logical-system-name* protocols**]**
- **[edit logical-systems** *logical-system-name* **routing-instances** *routing-instance-name* protocols**]**
- **[edit** protocols**]**
- **[edit routing-instances** *routing-instance-name* protocols**]**

The routing instance type can be either **virtual-switch** or **layer2-control**.

To configure the VLAN Spanning Tree Protocol:

1. Enable VSTP as the version of spanning-tree protocol to be configured:

   ```
   [edit]
   user@host@ edit ... protocols (STP Type) vstp
   ```

2. (Optional) For compatibility with older bridges that do not support VSTP, you can run force VSTP to run as the original IEEE 802.1D Spanning Tree Protocol (STP) version:

   ```
   [edit ... protocols vstp]
   user@host# set force-version stp
   ```

NOTE: If VSTP has been forced to run as the original STP version, you can revert back to VSTP by first removing the **force-version** statement from the configuration and then entering the clear spanning-tree protocol-migration configuration mode command.

3. Configure the interfaces that participate in the VSTP instance.

   a. Enable configuration of the interface:

      ```
      [edit ... protocols vstp]
      user@host# edit interface interface-name
      ```

   b. Configure the interface priority:

      ```
      [edit ... protocols vstp interface interface-name]
      user@host# set priority interface-priority
      ```

   c. (Optional) By default, the interface link cost is determined by the link speed. You can configure the interface link cost to control which bridge is the designated bridge and which port is the designated port:

      ```
      [edit ... protocols vstp interface interface-name]
      user@host# set cost interface-link-cost
      ```

   d. Configure the interface link mode to identify point-to-point links:

      ```
      [edit ... protocols vstp interface interface-name]
      user@host# set mode (p2p | shared)
      ```

      Specify **p2p** if the link is point to point. Specify **shared** if the link is a shared media.

   e. (Optional) Configure the interface as an edge port:

      ```
      [edit ... protocols vstp interface interface-name]
      user@host# set edge
      ```

      Edge ports do not expect to receive bridge protocol data unit (BPDU) packets. If a BPDU packet is received for an edge port, the port becomes a non-edge port

   You can also enable BPDU root protection for all spanning-tree protocol instances on the interface. BPDU root protect ensures the port is the spanning-tree designated port. If the port receives superior BPDU packets, root protect moves this port to a root-prevented spanning-tree state. For configuration details, see "Checking the Status of Spanning-Tree Instance Interfaces" on page 87.

4. Enable configuration of a VLAN instance:

   ```
   [edit ... protocols vstp]
   user@host# edit vlan vlan-id
   ```

5. Configure the bridge priority:

   ```
   [edit ... protocols vstp vlan vlan-id]
   user@host# set bridge-priority bridge-priority
   ```

   For more information, see "Bridge Priority for Election of Root Bridge and Designated Bridge" on page 51.

6. Configure hello BPDU timers.

   a. Configure the maximum expected arrival time of hello BPDUs:

      ```
      [edit ... protocols vstp vlan vlan-id]
      user@host# set max-age seconds
      ```

   b. Configure the time interval at which the root bridge transmits configuration BPDUs:

      ```
      [edit ... protocols vstp vlan vlan-id]
      user@host# set hello-time seconds
      ```

7. (Optional) By default, the bridge port remains in the listening and learning states for 15 seconds before transitioning to the forwarding state. You can specify a delay from **4** through **20** seconds instead:

   ```
   [edit ... protocols vstp vlan vlan-id]
   user@host# set forward-delay seconds
   ```

8. Configure the interfaces that participate in the VSTP instance.

   a. Enable configuration of the interface:

      ```
      [edit ... protocols vstp vlan vlan-id]
      user@host# edit interface interface-name
      ```

   b. Configure the interface priority:

      ```
      [edit ... protocols vstp vlan vlan-id interface interface-name]
      user@host# set priority interface-priority
      ```

   c. (Optional) By default, the interface link cost is determined by the link speed. You can configure the interface link cost to control which bridge is the designated bridge and which port is the designated port:

      ```
      [edit ... protocols vstp vlan vlan-id interface interface-name]
      user@host# set cost interface-link-cost
      ```

   d. Configure the interface link mode to identify point-to-point links:

      ```
      [edit ... protocols vstp vlan vlan-id interface interface-name]
      user@host# set mode (p2p | shared)
      ```

      Specify **p2p** if the link is point to point. Specify **shared** if the link is a shared media.

   e. (Optional) Configure the interface as an edge port:

      ```
      [edit ... protocols vstp vlan vlan-id interface interface-name]
      user@host# set edge
      ```

      Edge ports do not expect to receive bridge protocol data unit (BPDU) packets. If a BPDU packet is received for an edge port, the port becomes a non-edge port.

   You can also enable BPDU root protection for all spanning-tree protocol instances on the interface. BPDU root protect ensures the port is the spanning-tree designated port. If the port receives superior BPDU packets, root protect moves this port to a root-prevented spanning-tree state. For configuration details, see "Checking the Status of Spanning-Tree Instance Interfaces" on page 87.

9. Verify the VSTP configuration:

   ```
   [edit]
   ... { # Optional logical system and/or routing instance
     protocols (STP Type) {
       vstp {
   ```



```
        force-version stp; # Optional.
        interface interface-name {
          priority interface-priority;
          cost interface-link-cost; # Optional.
          mode (p2p | shared);
          edge; # Optional.
        }
        vlan vlan-id {
          bridge-priority bridge-priority;
          max-age seconds;
          hello-time seconds;
          forward-delay seconds; # Optional.
          interface interface-name {
            priority interface-priority;
            cost interface-link-cost; # Optional.
            mode (p2p | shared);
            edge; # Optional.
          }
        }
      }
    }
  }
```

Related Documentation

- RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 53
- Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 52
- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71
- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 72

VSTP on a Trunk Port with Tagged Traffic Overview

In 802.1ad provider bridge networks (stacked VLANs), single-tagged access ports and double-tagged trunk ports can co-exist in a single spanning tree context. In this mode, the VLAN Spanning Tree Protocol (VSTP) can send and receive untagged Rapid Spanning Tree Protocol (RSTP) bridge protocol data units (BPDUs) on Gigabit Ethernet (ge), 10 -Gigabit Ethernet (xe), and aggregated Ethernet (ae) interfaces. The untagged RSTP BPDUs interoperate with tagged VSTP BPDUs sent over the double-tagged trunk ports.

Double-tagging can be useful for Internet service providers, allowing them to use VLANs internally while mixing traffic from clients that are already VLAN-tagged.

Related Documentation

- access-trunk on page 96
- Example: Configuring VSTP on a Trunk Port with Tagged Traffic on page 39

Example: Configuring VSTP on a Trunk Port with Tagged Traffic

This example shows how to configure the VSTP to send and receive standard untagged Rapid Spanning Tree Protocol (RSTP) bridge protocol data units (BPDUs) on access

trunks that interoperate with tagged VSTP BPDUs sent over the double-tagged trunk ports.

Requirements

This example uses the following hardware and software components:

- Two CE devices (MX Series routers with DPCE or MPC cards)
- Two PE devices (MX Series routers with DPCE or MPC cards)
- Junos OS Release 12.3 or later running on the PE devices

Overview

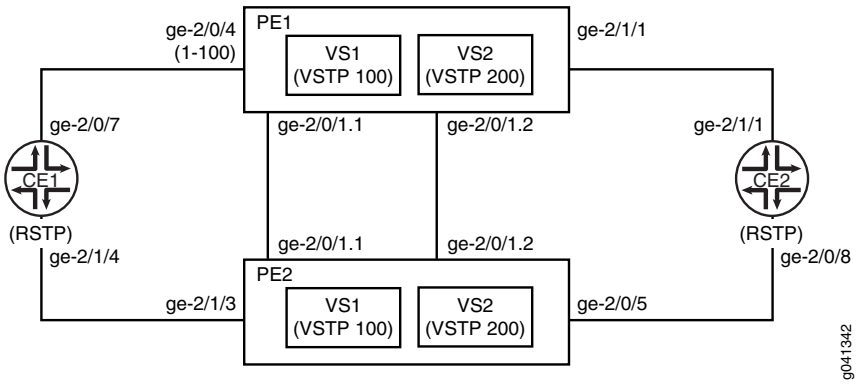
This example shows how to configure VSTP on a trunk port with tagged traffic.

Topology

Figure 5 on page 40 shows a sample topology in which two customer edge (CE) bridges are dual-homed to two provider edge (PE) devices. All of the PE-CE links are single-tagged trunks using C-VLANs 1-100. The core link between Devices PE1 and PE2 is a double-tagged trunk that carries traffic from both CE devices, using S-VLANs 100 and 200 to distinguish the CE traffic.

Two VSTP instances are created on the PE devices, one for each S-VLAN. The CE devices run the standard RSTP. The PE devices run VSTP on the core link while sending standard untagged RSTP BPDUs toward the CE devices.

Figure 5: Topology for VSTP Configured on a Trunk Port with Tagged Traffic



Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

Device PE1

```
set interfaces ge-2/0/1 flexible-vlan-tagging
set interfaces ge-2/0/1 encapsulation flexible-ethernet-services
set interfaces ge-2/0/1 unit 1 vlan-id 100
set interfaces ge-2/0/1 unit 1 family bridge interface-mode trunk
set interfaces ge-2/0/1 unit 1 family bridge inner-vlan-id-list 1-100
set interfaces ge-2/0/1 unit 2 vlan-id 200
set interfaces ge-2/0/1 unit 2 family bridge interface-mode trunk
set interfaces ge-2/0/1 unit 2 family bridge inner-vlan-id-list 1-100
set interfaces ge-2/0/4 encapsulation ethernet-vpls
set interfaces ge-2/0/4 unit 0 description to_CE1
set interfaces ge-2/0/4 unit 0 family bridge interface-mode trunk
set interfaces ge-2/0/4 unit 0 family bridge vlan-id-list 1-100
set interfaces ge-2/1/1 unit 0 description to_CE2
set interfaces ge-2/1/1 unit 0 family bridge interface-mode trunk
set interfaces ge-2/1/1 unit 0 family bridge vlan-id-list 1-100
set routing-instances vs1 instance-type virtual-switch
set routing-instances vs1 interface ge-2/0/1.1
set routing-instances vs1 interface ge-2/0/4.0
set routing-instances vs1 protocols vstp vlan 100 interface ge-2/0/1
set routing-instances vs1 protocols vstp vlan 100 interface ge-2/0/4 access-trunk
set routing-instances vs1 bridge-domains bd vlan-id-list 1-100
set routing-instances vs2 instance-type virtual-switch
set routing-instances vs2 interface ge-2/0/1.2
set routing-instances vs2 interface ge-2/1/1.0
set routing-instances vs2 protocols vstp vlan 200 interface ge-2/0/1
set routing-instances vs2 protocols vstp vlan 200 interface ge-2/1/1 access-trunk
set routing-instances vs2 bridge-domains bd vlan-id-list 1-100
```

Device PE2

```
set interfaces ge-2/0/1 flexible-vlan-tagging
set interfaces ge-2/0/1 encapsulation flexible-ethernet-services
set interfaces ge-2/0/1 unit 1 vlan-id 100
set interfaces ge-2/0/1 unit 1 family bridge interface-mode trunk
set interfaces ge-2/0/1 unit 1 family bridge inner-vlan-id-list 1-100
set interfaces ge-2/0/1 unit 2 vlan-id 200
set interfaces ge-2/0/1 unit 2 family bridge interface-mode trunk
set interfaces ge-2/0/1 unit 2 family bridge inner-vlan-id-list 1-100
set interfaces ge-2/1/3 description to_CE1
set interfaces ge-2/1/3 unit 0 family bridge interface-mode trunk
set interfaces ge-2/1/3 unit 0 family bridge vlan-id-list 1-100
set interfaces ge-2/0/5 description to_CE2
set interfaces ge-2/0/5 unit 0 family bridge interface-mode trunk
set interfaces ge-2/0/5 unit 0 family bridge vlan-id-list 1-100
set routing-instances vs1 instance-type virtual-switch
set routing-instances vs1 interface ge-2/0/1.1
set routing-instances vs1 interface ge-2/1/3.0
set routing-instances vs1 protocols vstp vlan 100 interface ge-2/0/1
set routing-instances vs1 protocols vstp vlan 100 interface ge-2/1/3 access-trunk
set routing-instances vs1 bridge-domains bd vlan-id-list 1-100
```

```
set routing-instances vs2 instance-type virtual-switch
set routing-instances vs2 interface ge-2/0/1.2
set routing-instances vs2 interface ge-2/0/5.0
set routing-instances vs2 protocols vstp vlan 200 interface ge-2/0/1
set routing-instances vs2 protocols vstp vlan 200 interface ge-2/0/5 access-trunk
set routing-instances vs2 bridge-domains bd vlan-id-list 1-100
```

Device CE1

```
set interfaces ge-2/0/7 unit 0 description to_PE1
set interfaces ge-2/0/7 unit 0 family bridge interface-mode trunk
set interfaces ge-2/0/7 unit 0 family bridge vlan-id-list 1-100
set interfaces ge-2/1/4 unit 0 description to_PE2
set interfaces ge-2/1/4 unit 0 family bridge interface-mode trunk
set interfaces ge-2/1/4 unit 0 family bridge vlan-id-list 1-100
set protocols rstp interface ge-2/0/7
set protocols rstp interface ge-2/1/4
set bridge-domains bd vlan-id-list 1-100
```

Device CE2

```
set interfaces ge-2/0/8 unit 0 description to_PE2
set interfaces ge-2/0/8 unit 0 family bridge interface-mode trunk
set interfaces ge-2/0/8 unit 0 family bridge vlan-id-list 1-100
set interfaces ge-2/1/1 unit 0 description to_PE1
set interfaces ge-2/1/1 unit 0 family bridge interface-mode trunk
set interfaces ge-2/1/1 unit 0 family bridge vlan-id-list 1-100
set protocols rstp interface ge-2/0/8
set protocols rstp interface ge-2/1/1
set bridge-domains bd vlan-id-list 1-100
```

Configuring PE1, PE2, CE1, and CE2

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Device PE1:

1. Configure the network interfaces.

```
[edit interfaces]
user@PE1# set ge-2/0/1 flexible-vlan-tagging
user@PE1# set ge-2/0/1 encapsulation flexible-ethernet-services
user@PE1# set ge-2/0/1 unit 1 vlan-id 100
user@PE1# set ge-2/0/1 unit 1 family bridge interface-mode trunk
user@PE1# set ge-2/0/1 unit 1 family bridge inner-vlan-id-list 1-100
user@PE1# set ge-2/0/1 unit 2 vlan-id 200
user@PE1# set ge-2/0/1 unit 2 family bridge interface-mode trunk
user@PE1# set ge-2/0/1 unit 2 family bridge inner-vlan-id-list 1-100

user@PE1# set ge-2/0/4 encapsulation ethernet-vpls
user@PE1#set ge-2/0/4 unit 0 description to_CE1
user@PE1# set ge-2/0/4 unit 0 family bridge interface-mode trunk
user@PE1#set ge-2/0/4 unit 0 family bridge vlan-id-list 1-100

user@PE1# set ge-2/1/1 unit 0 description to_CE2
user@PE1# set ge-2/1/1 unit 0 family bridge interface-mode trunk
user@PE1# set ge-2/1/1 unit 0 family bridge vlan-id-list 1-100
```

2. Configure the routing instances.

```
[edit routing-instances]
user@PE1# set vs1 instance-type virtual-switch
user@PE1# set vs1 interface ge-2/0/1.1
user@PE1# set vs1 interface ge-2/0/4.0
user@PE1# set vs1 protocols vstp vlan 100 interface ge-2/0/1
user@PE1# set vs1 protocols vstp vlan 100 interface ge-2/0/4 access-trunk
user@PE1# set vs1 bridge-domains bd vlan-id-list 1-100

user@PE1# set vs2 instance-type virtual-switch
user@PE1# set vs2 interface ge-2/0/1.2
user@PE1# set vs2 interface ge-2/1/1.0
user@PE1# set vs2 protocols vstp vlan 200 interface ge-2/0/1
user@PE1# set vs2 protocols vstp vlan 200 interface ge-2/1/1 access-trunk
user@PE1# set vs2 bridge-domains bd vlan-id-list 1-100
```

Step-by-Step Procedure

To configure Device PE2:

1. Configure the interfaces.

```
[edit interfaces]
user@PE2# set ge-2/0/1 flexible-vlan-tagging
user@PE2# set ge-2/0/1 encapsulation flexible-ethernet-services
user@PE2# set ge-2/0/1 unit 1 vlan-id 100
user@PE2# set ge-2/0/1 unit 1 family bridge interface-mode trunk
user@PE2# set ge-2/0/1 unit 1 family bridge inner-vlan-id-list 1-100
user@PE2# set ge-2/0/1 unit 2 vlan-id 200
user@PE2# set ge-2/0/1 unit 2 family bridge interface-mode trunk
user@PE2# set ge-2/0/1 unit 2 family bridge inner-vlan-id-list 1-100

user@PE2# set ge-2/1/3 description to_CE1
user@PE2# set ge-2/1/3 unit 0 family bridge interface-mode trunk
user@PE2# set ge-2/1/3 unit 0 family bridge vlan-id-list 1-100

user@PE2# set ge-2/0/5 description to_CE2
user@PE2# set ge-2/0/5 unit 0 family bridge interface-mode trunk
user@PE2# set ge-2/0/5 unit 0 family bridge vlan-id-list 1-100
```

2. Configure the routing instances.

```
[edit routing-instances]
user@PE2# set vs1 instance-type virtual-switch
user@PE2# set vs1 interface ge-2/0/1.1
user@PE2# set vs1 interface ge-2/1/3.0
user@PE2# set vs1 protocols vstp vlan 100 interface ge-2/0/1
user@PE2# set vs1 protocols vstp vlan 100 interface ge-2/1/3 access-trunk
user@PE2# set vs1 bridge-domains bd vlan-id-list 1-100

user@PE2# set vs2 instance-type virtual-switch
user@PE2# set vs2 interface ge-2/0/1.2
user@PE2# set vs2 interface ge-2/0/5.0
user@PE2# set vs2 protocols vstp vlan 200 interface ge-2/0/1
user@PE2# set vs2 protocols vstp vlan 200 interface ge-2/0/5 access-trunk
user@PE2# set vs2 bridge-domains bd vlan-id-list 1-100
```

Step-by-Step Procedure

To configure CE1:

1. Configure the interfaces.

```
[edit interfaces]
user@CE1# set ge-2/0/7 unit 0 description to_PE1
user@CE1# set ge-2/0/7 unit 0 family bridge interface-mode trunk
user@CE1# set ge-2/0/7 unit 0 family bridge vlan-id-list 1-100

user@CE1# set ge-2/1/4 unit 0 description to_PE2
user@CE1# set ge-2/1/4 unit 0 family bridge interface-mode trunk
user@CE1# set ge-2/1/4 unit 0 family bridge vlan-id-list 1-100
```

2. Configure the protocols.

```
[edit protocols]
user@CE1# set rstp interface ge-2/0/7
user@CE1# set rstp interface ge-2/1/4
```

3. Configure the bridge domain.

```
[edit bridge-domains]
user@CE1# set bd vlan-id-list 1-100
```

Step-by-Step Procedure

To configure CE2:

1. Configure the interfaces.

```
[edit interfaces]
user@CE2# set ge-2/0/8 unit 0 description to_PE2
user@CE2# set ge-2/0/8 unit 0 family bridge interface-mode trunk
user@CE2# set ge-2/0/8 unit 0 family bridge vlan-id-list 1-100

user@CE2# set ge-2/1/1 unit 0 description to_PE1
user@CE2# set ge-2/1/1 unit 0 family bridge interface-mode trunk
user@CE2# set ge-2/1/1 unit 0 family bridge vlan-id-list 1-100
```

2. Configure the protocols.

```
[edit protocols]
user@CE2# set rstp interface ge-2/0/8
user@CE2# set rstp interface ge-2/1/1
```

3. Configure the bridge domain.

```
[edit bridge-domains]
user@CE2# set bd vlan-id-list 1-100
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show routing-instances**, **show protocols**, and **show bridge-domains** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

Device PE1

```
user@PE1# show interfaces
ge-2/0/1 {
   flexible-vlan-tagging;
```

```
    encapsulation flexible-ethernet-services;
    unit 1 {
      vlan-id 100;
      family bridge {
        interface-mode trunk;
        inner-vlan-id-list 1-100;
      }
    }
    unit 2 {
      vlan-id 200;
      family bridge {
        interface-mode trunk;
        inner-vlan-id-list 1-100;
      }
    }
}
ge-2/0/4 {
    encapsulation ethernet-vpls;
    unit 0 {
      description to_CE1;
      family bridge {
        interface-mode trunk;
        vlan-id-list 1-100;
      }
    }
}
ge-2/1/1 {
    unit 0 {
      description to_CE2;
      family bridge {
        interface-mode trunk;
        vlan-id-list 1-100;
      }
    }
}

user@PE1# show routing-instances
vs1 {
    instance-type virtual-switch;
    interface ge-2/0/1.1;
    interface ge-2/0/4.0;
    protocols {
      vstp {
        vlan 100 {
          interface ge-2/0/1;
          interface ge-2/0/4 {
            access-trunk;
          }
        }
      }
    }
    bridge-domains {
      bd {
        vlan-id-list 1-100;
      }
    }
```

```
    }
    vs2 {
      instance-type virtual-switch;
      interface ge-2/0/1.2;
      interface ge-2/0/1.0;
      protocols {
        vstp {
          vlan 200 {
            interface ge-2/0/1;
            interface ge-2/1/1 {
              access-trunk;
            }
          }
        }
      }
      bridge-domains {
        bd {
          vlan-id-list 1-100;
        }
      }
    }
```

Device PE2

```
user@PE2# show interfaces
ge-2/0/1 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    vlan-id 100;
    family bridge {
      interface-mode trunk;
      inner-vlan-id-list 1-100;
    }
  }
  unit 2 {
    vlan-id 200;
    family bridge {
      interface-mode trunk;
      inner-vlan-id-list 1-100;
    }
  }
}
ge-2/0/5 {
  description to_CE2;
  unit 0 {
    family bridge {
      interface-mode trunk;
      vlan-id-list 1-100;
    }
  }
}
ge-2/1/3 {
  description to_CE1;
  unit 0 {
    family bridge {
      interface-mode trunk;
      vlan-id-list 1-100;
```

```
    }
  }
}

user@PE2# show routing-instances
vs1 {
  instance-type virtual-switch;
  interface ge-2/0/1.1;
  interface ge-2/1/3.0;
  protocols {
    vstp {
      vlan 100 {
        interface ge-2/0/1;
        interface ge-2/1/3 {
          access-trunk;
        }
      }
    }
  }
  bridge-domains {
    bd {
      vlan-id-list 1-100;
    }
  }
}
vs2 {
  instance-type virtual-switch;
  interface ge-2/0/1.2;
  interface ge-2/0/5.0;
  protocols {
    vstp {
      vlan 200 {
        interface ge-2/0/1;
        interface ge-2/0/5 {
          access-trunk;
        }
      }
    }
  }
  bridge-domains {
    bd {
      vlan-id-list 1-100;
    }
  }
}
```

Device CE1

```
user@CE1# show interfaces
ge-2/0/7 {
  unit 0 {
    description to_PE1;
    family bridge {
      interface-mode trunk;
      vlan-id-list 1-100;
    }
  }
}
```

```
ge-2/1/4 {
  unit 0 {
    description to_PE2;
    family bridge {
      interface-mode trunk;
      vlan-id-list 1-100;
    }
  }
}

user@CE1# show protocols
rstp {
  interface ge-2/0/7;
  interface ge-2/1/4;
}

user@CE1# show bridge-domains
bd {
  vlan-id-list 1-100;
}
```

Device CE2

```
user@CE2 show interfaces
ge-2/0/8 {
  unit 0 {
    description to_PE2;
    family bridge {
      interface-mode trunk;
      vlan-id-list 1-100;
    }
  }
}
ge-2/1/1 {
  unit 0 {
    description to_PE1;
    family bridge {
      interface-mode trunk;
      vlan-id-list 1-100;
    }
  }
}

user@CE2# show protocols
rstp {
  interface ge-2/0/8;
  interface ge-2/1/1;
}

user@CE2# show bridge-domains
bd {
  vlan-id-list 1-100;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying That the Interfaces Are Operational

Purpose Verify that the interfaces are operational.

Action From operational mode, enter the **show spanning-tree interface routing-instance** command.

```
user@PE1> show spanning-tree interface routing-instance vs1
Spanning tree interface parameters for VLAN 100

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID        bridge ID          Cost
ge-2/0/1       128:82       128:82  32868.0021590f37d0     20000  FWD    DESG
ge-2/0/4       128:85       128:85  32868.0021590f37d0     20000  FWD    DESG
```

Meaning The output shows the status of the interfaces configured for VLAN 100.

Verifying the STP Bridge Parameters of the Routing Instances

Purpose Verify the STP bridge parameters configured for the routing instances.

Action From operational mode, enter the **show spanning-tree bridge routing-instance** command.

```
user@PE1> show spanning-tree bridge routing-instance vs1
STP bridge parameters
Routing instance name               : vs1
Enabled protocol                    : RSTP

STP bridge parameters for VLAN 100
  Root ID                           : 32868.00:21:59:0f:37:d0
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Message age                       : 0
  Number of topology changes        : 2
  Time since last topology change   : 687 seconds
  Local parameters
    Bridge ID                       : 32868.00:21:59:0f:37:d0
    Extended system ID              : 100
```

Meaning The output shows the status of the STP bridge parameters for routing instance vs1.

Displaying STP Statistics for the Configured Bridge

Purpose Display spanning-tree statistics for the configured bridge.

Action From operational mode, enter the **show spanning-tree statistics bridge** command.

```
user@PE1> show spanning-tree statistics bridge
STP Context  : default
STP Instance : 0
Number of Root Bridge Changes: 0
Number of Root Port Changes:   0

STP Context  : x/default
STP Instance : 0
Number of Root Bridge Changes: 0
Number of Root Port Changes:   0

STP Context  : vs1
STP Instance : 0
Number of Root Bridge Changes: 2           Last Changed: Thu Sep 20 15:12:18
2012
Number of Root Port Changes:   1           Last Changed: Thu Sep 20 15:01:13
2012
Recent TC  Received:  ge-2/0/1.1           Received    : Thu Sep 20 15:01:17
2012

STP Context  : vs2
STP Instance : 0
Number of Root Bridge Changes: 2           Last Changed: Thu Sep 20 15:10:25
2012
Number of Root Port Changes:   2           Last Changed: Thu Sep 20 15:10:25
2012
Recent TC  Received:  ge-2/1/1.0           Received    : Thu Sep 20 15:10:47
2012

STP Context  : CE1/default
STP Instance : 0
Number of Root Bridge Changes: 0
Number of Root Port Changes:   0
Recent TC  Received:  ge-2/1/4.0           Received    : Thu Sep 20 15:12:15
2012
```

Meaning The command output shows spanning-tree statistics for the configured bridge.

Related Documentation

- access-trunk on page 96
- VSTP on a Trunk Port with Tagged Traffic Overview on page 39

Provider Bridge Participation in RSTP or MSTP Instances

A provider network can bridge the customer STP BPDU packets between customer sites by default. At the same time, the provider network can prevent forwarding loops by running a spanning-tree protocol in the provider network. On an MX Series router running Rapid Spanning-Tree Protocol (RSTP) or Multiple Spanning-Tree Protocol (MSTP) in a provider network, you can enable provider bridge participation in the RSTP or MSTP instance.

The IEEE 802.1ad specification reserves the group MAC address value of **01:80:c2:00:00:08** to designate the *provider bridge group*. On an MX Series router for which you have enabled provider bridge participation in the RSTP or MSTP instance, the router exchanges BPDU packets with the provider bridge group as follows:

- Transmitted BPDU packets contain the destination MAC address **01:80:c2:00:00:08**.
- Received BPDU packets with the destination MAC address **01:80:c2:00:00:08** are accepted and passed to the Routing Engine.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- **bpdu-destination-mac-address on page 98**

System Identifier for Bridges in STP or RSTP Instances

The extended system identifier is used to specify different bridge identifiers for different STP or RSTP routing instances.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28
- **extended-system-id on page 106**

Bridge Priority for Election of Root Bridge and Designated Bridge

Use the bridge priority to control which bridge is elected as the root bridge and also to control which bridge is elected the root bridge when the initial root bridge fails.

The root bridge for each spanning-tree protocol instance is determined by the bridge ID. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge. The bridge with the lowest bridge ID is elected as the root bridge. If the bridge priorities are equal or if the bridge priority is not configured, the bridge with the lowest MAC address is elected the root bridge.

The bridge priority can also be used to determine which bridge becomes the designated bridge for a LAN segment. If two bridges have the same path cost to the root bridge, the bridge with the lowest bridge ID becomes the designated bridge.

The bridge priority can be set only in increments of 4096.

Consider a sample scenario in which a dual-homed customer edge (CE) router is connected to two other provider edge (PE) routers, which function as the VPLS PE routers, with MTSP enabled on all these routers, and with the CE router operating as the root bridge. Integrated Routing and Bridging (IRB) interface is configured for the VPLS routing instances on the routers. In such a network, the MAC addresses that are learned in the VPLS domain continuously move between the LSI or virtual tunnel (VT) interfaces and the VPLS interfaces on both the PE routers. To avoid the continuous movement of the MAC addresses, you must configure root protection by including the **no-root-port** statement at the **[edit routing-instances *routing-instance-name* protocols mstp interface *interface-name*]** hierarchy level and configure the bridge priority as zero by including the **bridge priority 0** statement at the **[edit routing-instances *routing-instance-name* protocols mstp]** hierarchy level on the PE routers. This configuration on the PE routers is required to prevent the CE-side facing interfaces from becoming the root bridge.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring VLAN Spanning Tree Protocol on page 36
- **bridge-priority on page 101**

Reverting to RSTP or VSTP from Forced IEEE 802.1D STP

On MX Series routers and EX Series and QFX Series switches on which Rapid Spanning Tree Protocol (RSTP) or VLAN Spanning Tree Protocol (VSTP) has been forced to run as the original IEEE 802.1D Spanning Tree Protocol (STP) version, you can revert back to RSTP or VSTP.

To revert from the forced instance of the original IEEE 802.1D STP version to the originally configured RSTP or VSTP version:

1. Remove the **force-version** statement from the following RSTP or VSTP configuration:

   ```
   user@host# delete protocols rstp force-version stp
   user@host# delete protocols vstp force-version stp
   ```

   Include this statement at the following hierarchy levels:

   - **[edit logical-systems *routing-instance-name* protocols rstp]**
   - **[edit protocols rstp]**
   - **[edit protocols vstp]**
   - **[edit routing-instances *routing-instance-name* protocols rstp]**
   - **[edit routing-instances *routing-instance-name* protocols vstp]**

2. Revert the forced IEEE 802.1D STP to run as the configured RSTP or VSTP:

   ```
   user@host# clear spanning-tree protocol-migration <interface interface-name>
     <routing-instance routing-instance-name>
   ```

   To revert the STP protocol globally, issue the statement without options (**clear spanning-tree protocol-migration**).

To revert the STP protocol for the specified interface only, specify the **interface *interface-name*** option.

To revert the STP protocol for a particular routing instance only, specify the **routing-instance *routing-instance-name*** option.

Related Documentation

- RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 53
- *Configuring RSTP (CLI Procedure)*
- *Configuring VLAN Spanning Tree Protocol*

RSTP or VSTP Forced to Run as IEEE 802.1D STP

On MX Series routers and EX Series and QFX Series switches in a Layer 2 environment, you can force the configured Rapid Spanning Tree Protocol (RSTP) or VLAN Spanning Tree Protocol (VSTP) to run as the original IEEE 802.1D Spanning Tree Protocol (STP) version. Configure original IEEE_802.1D STP for compatibility with older bridges that do not support RSTP or VSTP.

Keep the following limitations in mind when RSTP or VSTP are forced to run as the original STP version:

- If you configure an instance interface as an edge port, the configuration statement is ignored.
- If you configure point-to-point link mode for an instance interface, the configuration statement is ignored.

Related Documentation

- *Configuring RSTP (CLI Procedure)*
- *Configuring VLAN Spanning Tree Protocol*
- Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 52
- force-version on page 107

Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure)

NOTE: This procedure uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. For ELS details, see *Getting Started with Enhanced Layer 2 Software*.

On EX Series switches running Rapid Spanning Tree Protocol (RSTP) (the default) or VLAN Spanning Tree Protocol (VSTP), you can force the original IEEE 802.1D Spanning Tree Protocol (STP) version to run in place of RSTP or VSTP. Configure the **force-version stp** statement for compatibility with older bridges that do not support RSTP or VSTP.

To force the spanning-tree protocol version to be the original IEEE 802.1D STP:

1. Enable IEEE 802.1D STP:

```
[edit protocols]
user@switch# set (rstp | vstp) force-version stp
```

NOTE: After using the **force-version** statement to enable xSTP globally, apply the **force-version** statement for specific Layer 2 ports.

Related Documentation

- RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 53
- Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 52

Configuring a Spanning-Tree Instance Interface as an Edge Port for Faster Convergence

RSTP, MSTP, and VSTP instance interfaces configured as *edge ports* enable the protocol to converge faster than the original IEEE 802.1D STP version. Edge ports transition directly to the forwarding state, and so the protocol does not need to wait for BPDUs to be received on edge ports.

The Junos OS supports automatic detection of edge ports as described in the RSTP standard. Layer 2 bridges do not expect to receive BPDUs for edge ports. If a BPDU is received for an edge port, the port becomes a non-edge port.

Keep the following guidelines in mind when configuring spanning-tree instance interfaces as edge ports:

- Do not configure a spanning-tree instance interface as an edge port if it is connected to any Layer 2 bridge. An instance interface connected to Layer 2 bridges but configured as an edge port can cause physical loops.
- if the spanning-tree protocol is configured to run the original IEEE 802.1D spanning-tree version, the edge-port option (if configured) is ignored.
- If edge ports are configured at both the VSTP global and VLAN levels, the configuration at the VLAN level overrides the global configuration.

Related Documentation

- Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on page 61
- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring VLAN Spanning Tree Protocol on page 36
- **edge on page 105**
- **interface (Spanning Tree) on page 110**
- *Configuring RSTP (CLI Procedure)*
- *Configuring VLAN Spanning Tree Protocol*

- *Configuring MSTP*

Configuring a Virtual Switch Routing Instance

On MX Series routers only, use the **virtual-switch** routing instance type to isolate a LAN segment with its spanning-tree instance and to separate its VLAN ID space. A bridge domain consists of a set of ports that share the same flooding or broadcast characteristics. Each virtual switch represents a Layer 2 network. You can optionally configure a virtual switch to support Integrated Routing and Bridging (IRB), which facilitates simultaneous Layer 2 bridging and Layer 3 IP routing on the same interface. You can also configure Layer 2 control protocols to provide loop resolution. Protocols supported include the Spanning-Tree Protocol (STP), Rapid Spanning-Tree Protocols (RSTP), Multiple Spanning-Tree Protocol (MSTP), and VLAN Spanning-Tree Protocol (VSTP).

To create a routing instance for a virtual switch, include at least the following statements in the configuration:

```
[edit]
routing-instances {
  routing-instance-name
    instance-type virtual-switch;
    bridge-domains {
      bridge-domain-name {
        domain-type bridge;
        interface interface-name;
        vlan-id (all | none | number);
        vlan-tags outer number inner number;
      }
    }
    protocols {
      (rstp | mstp | vstp) {
        ...stp-configuration ...
      }
    }
  }
}
```

For more information about configuring virtual switches, see *Configuring a Layer 2 Virtual Switch* .

Related Documentation

- *Routing Instances Overview*
- *Layer 2 Routing Instance Types*
- *Configuring a VPLS Routing Instance*
- *Configuring a Layer 2 Control Protocol Routing Instance*

CHAPTER 3

Configuring BPDU Protection, Loop Protection, and Root Protection for Spanning-Tree Protocols

Understanding BPDU Protection for Spanning-Tree Instance Interfaces

By default, if a bridge protocol data unit (BPDU) data frame is received on a blocked interface, the system will disable the interface and stop forwarding frames out the interface until the interface is explicitly cleared.

The Spanning Tree Protocol (STP) family is designed to break possible loops in a Layer 2 bridged network. Loop prevention avoids damaging broadcast storms that can potentially render the network useless. STP processes on bridges exchange BPDUs to determine the LAN topology, decide the root bridge, stop forwarding on some ports, and so on.

However, a misbehaving user application or device can interfere with the operation of the STP protocols and cause network problems.

On the MX Series routers or EX Series switches only, you can configure BPDU protection to ignore BPDUs received on interfaces where none should be expected (for example, a LAN interface on a network edge with no other bridges present). If a BPDU is received on a blocked interface, the interface is disabled and stops forwarding frames. By default, all BPDUs are accepted and processed on all interfaces.

You can configure BPDU protection on interfaces with the following encapsulation types:

- **ethernet-bridge**
- **ethernet-vpls**
- **extended-vlan-bridge**
- **vlan-vpls**
- **extended-vlan-vpls**

You can configure BPDU protection on individual interfaces or on all the edge ports of the bridge.

Related Documentation

- Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 60
- Configuring BPDU Protection on All Edge Ports on page 61
- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69
- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71

Maximum Age for Awaiting Arrival of Hello BPDUs

The maximum age timer specifies the maximum expected arrival time of hello BPDUs. If the maximum age timer expires, the bridge detects that the link to the root bridge has failed and initiates a topology reconvergence. The maximum age timer should be longer than the configured hello timer.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring VLAN Spanning Tree Protocol on page 36
- **max-age on page 111**

Hello Time for Root Bridge to Transmit Hello BPDUs

The hello timer specifies the time interval at which the root bridge transmits configuration BPDUs.

Related Documentation
- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring VLAN Spanning Tree Protocol on page 36
- hello-time on page 109

BPDU Protection for Individual Spanning-Tree Instance Interfaces

To configure BPDU protection on one or more spanning-tree instance interfaces, include the **bpdu-block** statement:

```
bpdu-block {
  interface interface-name;
  disable-timeout seconds;
}
```

NOTE: If you also include the optional **disable-timeout** *seconds* statement, *blocked interfaces* are automatically cleared after the specified time interval unless the interval is **0**.

Related Documentation
- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69
- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57
- Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 60

BPDU Protection on All Edge Ports of the Bridge

To configure edge port blocking for a particular STP family member, include the **bpdu-block-on-edge** statement for **mstp**, **rstp**, or **vstp**:

```
bpdu-block-on-edge;
interface interface-name;
```

NOTE: In contrast to BPDU protection configured on individual spanning-tree instance interfaces, BPDU protection configured on all edge ports of an entire spanning-tree protocol *disables designated edge ports* and does not enable them again.

Related Documentation
- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69
- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57
- Configuring BPDU Protection on All Edge Ports on page 61

Configuring BPDU Protection for Spanning-Tree Instance Interfaces

On MX Series routers and EX Series switches, you can configure BPDU protection to ignore BPDU received on interfaces where none should be expected. If a BPDU is received on a blocked interface, the interface is disabled and stops forwarding frames. By default, all BPDUs are accepted and processed on all interfaces.

To configure BPDU protection for individual spanning-tree instance interfaces:

1. Enable BPDU protection on a specific spanning-tree instance interface:

   ```
   [edit]
   user@host# edit protocols layer2-control bpdu-block
   user@host# set interface interface (aex | (ge-fpc/pic/port | xe-fpc/pic/port)
   ```

   If a BPDU is received on the interface, the system will disable the interface and stop forwarding frames out the interface until the bridging process is restarted.

2. (Optional) Configure the amount of time the system waits before *automatically* unblocking this interface after it has received a BPDU:

   ```
   [edit protocols layer2-contorl bpdu-block interface interface-name]
   user@host# set disable-timeout seconds
   ```

   The range of the *seconds* option value is from 10 through 3600 seconds (one hour). A *seconds* option value of **0** is allowed, but this results in the default behavior (the interface is blocked until the interface is cleared).

3. Verify the configuration of BPDU blocking for individual interfaces:

   ```
   [edit]
   interfaces {
     ge-fpc/pic/port { # VLAN encapsulation on Gigabit Ethernet.
       encapsulation (ethernet-bridge | extended-vlan-bridge | extended-vlan-vpls |
         vlan-vpls);
     }
     xe-fpc/pic/port { # VLAN encapsulation on 10-Gigabit Ethernet.
       encapsulation (ethernet-bridge | extended-vlan-bridge | extended-vlan-vpls |
         vlan-vpls);
     }
     ae-X { # VLAN encapsulation
       encapsulation (ethernet-vpls vlan-vpls); # on aggregated Ethernet.
       ...
     }
     ae-X { # Extended VLAN encapsulation
       vlan-tagging; # on aggregated Ethernet.
       encapsulation extended-vlan-vpls;
       unit logical-unit-number {
         vlan-id number;
         ......
       }
       ......
     }
   }
   protocols
     layer2-control {
       bpdu-block
   ```

```
        interface interface-name;
        disable-timeout seconds;
    }
}
```

Related Documentation

- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69
- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57
- BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 59

Configuring BPDU Protection on All Edge Ports

On MX Series routers and EX Series switches, you can configure BPDU protection to ignore BPDU received on interfaces where none should be expected. If a BPDU is received on a blocked interface, the interface is disabled and stops forwarding frames. By default, all BPDUs are accepted and processed on all interfaces.

To configure BPDU protection for all edge ports for a particular spanning-tree protocol:

1. Enable edge port blocking for a particular spanning-tree protocol:

```
[edit]
user@host# set protocols (STP Type) (mstp | rstp | vstp) bpdu-block-on-edge
```

2. Verify BPDU protection for edge ports:

```
[edit]
protocols (STP Type) {
    (mstp | rstp | vstp) {
        bpdu-block-on-edge;
    }
}
```

Related Documentation

- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69
- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57
- BPDU Protection on All Edge Ports of the Bridge on page 59

Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations

MX Series routers provide Layer 2 loop prevention through the Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). All spanning-tree protocols use a special type of frame called a bridge protocol data unit (BPDU) to communicate. Other devices—PC bridging applications, for example also use BPDUs and generate their own BPDUs. These different BPDUs are not compatible. When BPDUs generated by spanning-tree protocols are transmitted to a device that uses another type of BPDU, they can cause problems on the device. Similarly, if routers

within a spanning-tree topology receive BPDUs from other devices, network outages can occur because of STP miscalculations.

This example configures BPDU protection on MX Series routers that use RSTP. The upstream configuration is done on the edge interfaces, where outside BPDUs are often received from other devices.

Requirements

This example uses the following hardware and software components:

- Two MX Series routers in an RSTP topology
- Junos OS Release 13.1 or later

Before you configure the interfaces on Router 2 for BPDU protection, be sure you have:

- RSTP enabled on the routers.

Overview

The MX Series routers, being in an RSTP topology, support a loop-free network through the exchange of BPDUs. Receipt of outside BPDUs in an STP, RSTP, or MSTP topology, however, can lead to network outages by triggering an STP misconfiguration. To prevent such outages, enable BPDU protection on STP interfaces that could receive outside BPDUs. If an outside BPDU is received on a BPDU-protected interface, the interface shuts down to prevent the outside BPDU from accessing the STP interface.

Figure 6 on page 63 shows the topology for this example. In this example, Router 1 and Router 2 are configured for RSTP and create a loop-free topology. The interfaces on Router 2 are edge access ports which frequently receive outside BPDUs generated by PC applications.

This example configures interface ge-0/0/5.0 and interface ge-0/0/6.0 as edge ports on Router 2, and then configures BPDU protection on those ports. With BPDU protection enabled, these interfaces shut down when they encounter an outside BPDU sent by the PCs connected to Router 2.

Topology

Figure 6: BPDU Protection Topology

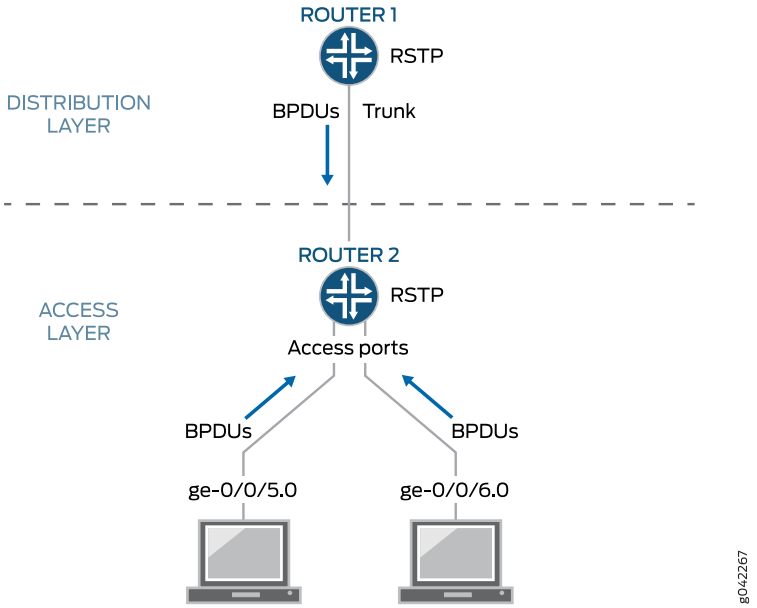


Table 3 on page 63 describes the components that are configured for BPDU protection.

Table 3: Components of the Topology for Configuring BPDU Protection on MX Series Routers

Property	Settings
Router 1 (Distribution Layer)	Router 1 is connected to Router 2 on a trunk interface.
Router 2 (Access Layer)	Router 2 has these access ports that require BPDU protection: • ge-0/0/5.0 • ge-0/0/6.0

This configuration example uses RSTP topology. You also can configure BPDU protection for STP or MSTP topologies at the [**edit protocols (mstp | rstp | vstp)**] hierarchy level.

Configuration

CLI Quick Configuration

To quickly configure RSTP on the two Router 2 interfaces and configure BPDU protection on all edge ports on Router 2, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level:

Router 2

```
set protocols rstp interface ge-0/0/5.0 edge
set protocols rstp interface ge-0/0/6.0 edge
set protocols rstp bpdu-block-on-edge
```

Configuring Router 2

Step-by-Step Procedure

To configure RSTP on the two Router 2 interfaces, and then configure BPDU protection:

1. Configure RSTP on interface ge-0/0/5.0 and interface ge-0/0/6.0, and configure them as edge ports.

   ```
   [edit protocols rstp]
   user@Router2# set interface ge-0/0/5.0 edge
   user@Router2# set interface ge-0/0/6.0 edge
   ```

2. Configure BPDU protection on all edge ports on this router.

   ```
   [edit protocols rstp]
   user@Router2# set bpdu-block-on-edge
   ```

Results

From configuration mode, confirm your configuration by entering the **show configuration protocols rstp** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@Router2> show configuration protocols rstp
interface ge-0/0/5.0 {
   edge;
}
interface ge-0/0/6.0 {
   edge;
}
bpdu-block-on-edge;
```

Verification

Verify that the configuration is working properly.

- Displaying the Interface State Before BPDU Protection Is Triggered on page 64
- Verifying That BPDU Protection Is Working Correctly on page 65

Displaying the Interface State Before BPDU Protection Is Triggered

Purpose

Before BPDUs can be received from PCs connected to interface ge-0/0/5.0 and interface ge-0/0/6.0, confirm the interface state.

Action Use the operational mode command **show spanning-tree instance**.

```
user@Router2> show spanning-tree interface

Spanning tree interface parameters for instance 0

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID        bridge ID          Cost
ge-0/0/0.0     128:513      128:513  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/1.0     128:514      128:514  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/2.0     128:515      128:515  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/3.0     128:516      128:516  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/4.0     128:517      128:517  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/5.0     128:518      128:518  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/6.0     128:519      128:519  32768.0019e2503f00     20000  FWD    DESG
[output truncated]
```

Meaning The output from the **show spanning-tree interface** command shows that interface ge-0/0/5.0 and interface ge-0/0/6.0 are ports in a forwarding state.

Verifying That BPDU Protection Is Working Correctly

Purpose In this example, the PCs connected to Router 2 start sending BPDUs to interface ge-0/0/5.0 and interface ge-0/0/6.0. Verify that BPDU protection is working on the interfaces.

Action Use the operational mode command **show spanning-tree interface**.

```
user@Router2> show spanning-tree interface

Spanning tree interface parameters for instance 0

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID        bridge ID          Cost
ge-0/0/0.0     128:513      128:513  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/1.0     128:514      128:514  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/2.0     128:515      128:515  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/3.0     128:516      128:516  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/4.0     128:517      128:517  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/5.0     128:518      128:518  32768.0019e2503f00     20000  BLK    DIS
(Bpdu-Incon)
ge-0/0/6.0     128:519      128:519  32768.0019e2503f00     20000  BLK    DIS
(Bpdu-Incon)
ge-0/0/7.0     128:520        128:1  16384.00aabbcc0348     20000  FWD    ROOT
ge-0/0/8.0     128:521      128:521  32768.0019e2503f00     20000  FWD    DESG
[output truncated]
```

Meaning When BPDUs are sent from the PCs to interface ge-0/0/5.0 and interface ge-0/0/6.0 on Router 2, the output from the operational mode command **show spanning-tree interface** shows that the interfaces have transitioned to a BPDU inconsistent state. The BPDU inconsistent state causes the interfaces to shut down.

Disabling the BPDU protection configuration on an interface does not automatically re-enable the interface. However, if the **disable-timeout** statement has been included in the BPDU configuration, the interface does return to service after the timer expires.

Otherwise, you must use the operational mode command **clear error bpdu interface** ***interface-name*** to unblock and re-enable the interface.

If the PCs connected to Router 2 send BPDUs to the interfaces again, BPDU protection is triggered once more, and the interfaces transition back to the BPDU inconsistent state, causing them to shut down. In such cases, you need to find and repair the misconfiguration on the PCs that are sending BPDUs to Router 2.

Related Documentation

- Configuring a Spanning-Tree Instance Interface as an Edge Port for Faster Convergence on page 54

Example: Blocking BPDUs on Aggregated Ethernet Interface for 600 Seconds

The following example, when used with a full bridge configuration with aggregated Ethernet, blocks BPDUs on aggregated interface **ae0** for 10 minutes (600 seconds) before enabling the interface again:

```
[edit protocols layer2-control]
bpdu-block {
  interface ae0;
  disable-timeout 600;
}
```

Related Documentation

- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69
- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57
- BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 59
- BPDU Protection on All Edge Ports of the Bridge on page 59
- Checking the Status of Spanning-Tree Instance Interfaces on page 87
- Clearing the Blocked Status of a Spanning-Tree Instance Interface on page 88

Understanding Loop Protection for Spanning-Tree Instance Interfaces

Spanning-tree protocol loop protection enhances the normal checks that spanning-tree protocols perform on interfaces. Loop protection performs a specified action when BPDUs are not received on a nondesignated port interface. You can choose to block the interface or issue an alarm when bridge protocol data units (BPDUs) are not received on the port.

The spanning-tree protocol family is responsible for breaking loops in a network of bridges with redundant links. However, hardware failures can create forwarding loops (STP loops) and cause major network outages. Spanning-tree protocols break loops by blocking ports (interfaces). However, errors occur when a blocked port transitions erroneously to a forwarding state.

Ideally, a spanning-tree protocol bridge port remains blocked as long as a superior alternate path to the root bridge exists for a connected LAN segment. This designated port is determined by receiving superior BPDUs from a peer on that port. When other

ports no longer receive BPDUs, the spanning-tree protocol considers the topology to be loop free. However, if a blocked or alternate port moves into a forwarding state, this creates a loop.

By default (that is, without spanning-tree protocol loop protection configured), an interface that stops receiving BPDUs will assume the designated port role and possibly result in a spanning-tree protocol loop.

By default, a spanning-tree protocol interface that stops receiving bridge protocol data unit (BPDU) data frames will transition to the designated port (forwarding) state, creating a potential loop. To prevent a spanning-tree instance interface from interpreting a lack of received BPDUs as a "false positive" condition for assuming the designated port role, you can configure one of the following loop protection options:

- Configure the router to raise an alarm condition if the spanning-tree instance interface has not received BPDUs during the timeout interval.
- Configure the router to block the spanning-tree instance interface if the interface has not received BPDUs during the timeout interval.

NOTE: Spanning-tree instance interface loop protection is enabled for all spanning-tree instances on the interface, but blocks or alarms only those instances that stop receiving BPDUs.

You can configure spanning-tree protocol loop protection to improve the stability of Layer 2 networks. We recommend you configure loop protection only on non-designated interfaces such as the root or alternate interfaces. Otherwise, if you configure loop protection on both sides of a designated link, then certain STP configuration events (such as setting the root bridge priority to an inferior value in a topology with many loops) can cause both interfaces to transition to blocking mode.

You configure spanning-tree protocol loop protection to prevent selected interfaces from interpreting the lack of received BPDUs as a "false positive" condition for making the interface the designated port.

Related Documentation

- Configuring Loop Protection for a Spanning-Tree Instance Interface on page 68
- Example: Enabling Loop Protection for Spanning-Tree Protocols on page 67

Example: Enabling Loop Protection for Spanning-Tree Protocols

This example blocks and logs the non-designated RSTP port **ge-1/2/0** after the BPDU timeout interval expires:

```
[edit]
protocols {
   rstp {
      interface ge-1/2/0 {
         bpdu-timeout-action block;
      }
```

```
    }
}
```

NOTE: This is not a complete configuration. You must also fully configure RSTP, including the ge-1/2/0 interface.

Related Documentation

- *Loop Protection for a Spanning-Tree Instance Interface*
- Understanding Loop Protection for Spanning-Tree Instance Interfaces on page 66

Configuring Loop Protection for a Spanning-Tree Instance Interface

Before you begin, you must fully configure the spanning-tree protocol, including instance interfaces. You can configure RSTP, MSTP, or VSTP at the following hierarchy levels:

- **[edit protocols]**
- **[edit routing-instances *routing-instance-name* protocols]**

To configure enhanced loop protection:

1. Include the **bpdu-timeout-action** statement with either the **block** or **log** option for the spanning-tree protocol interface.

   - For the STP or RSTP instance on a physical interface:

     ```
     [edit]
     protocols {
       rstp {
         interface interface-name {
           bpdu-timeout-action (log | block);
         }
       }
     }
     ```

   - For all MSTP instances on a physical interface:

     ```
     [edit]
     protocols {
       mstp {
         interface interface-name {
           bpdu-timeout-action (log | block);
         }
       }
     }
     ```

   - For all VSTP instances on a physical interface configured at the global level or a the VLAN level:

     ```
     [edit]
     protocols {
       vstp {
         interface interface-name {
           bpdu-timeout-action (log | block);
     ```

```
    }
    vlan vlan-id {
      interface interface-name {
        bpdu-timeout-action (log | block);
      }
    }
  }
}
```

2. To display the spanning-tree protocol loop protection characteristics on an interface, use the **show spanning-tree interface** operational command.

Related Documentation

- Understanding Loop Protection for Spanning-Tree Instance Interfaces on page 66
- *Loop Protection for a Spanning-Tree Instance Interface*
- Example: Enabling Loop Protection for Spanning-Tree Protocols on page 67

Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network

Root protect helps to enforce the root bridge placement in a Layer 2 switched network. Enable root protect on interfaces that should not receive superior bridge protocol data units (BPDUs) from the root bridge. Typically, these ports are spanning tree protocol-designated ports on an administrative boundary. Enabling root protect ensures the port remains a spanning-tree designated port.

When root protect is enabled on an interface, it is enabled for all spanning-tree protocol instances on that interface. The interface is blocked only for those instances that receive superior BPDUs.

By default, root protect is disabled.

If the bridge receives superior BPDUs on a port that has root protect enabled, that port transitions to a root-prevented STP state and the interface is blocked. This prevents a bridge that should not be the root bridge from being elected the root bridge.

After the bridge stops receiving superior BPDUs on the port with root protect enabled and the received BPDUs time out, that port transitions back to the STP-designated port state.

Related Documentation

- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69
- Enabling Root Protection for a Spanning-Tree Instance Interface on page 70

Enabling Root Protection for a Spanning-Tree Instance Interface

To enable root protect for a spanning-tree instance interface:

1. Enable configuration of the spanning-tree protocol:

   ```
   [edit]
   user@host# edit protocols (mstp | rstp | vstp <vlan vlan-id>)
   ```

2. Enable configuration of the spanning-tree instance interface:

   ```
   [edit ... protocols (mstp | rstp | vstp <vlan vlan-id>)]
   user@host# edit interface interface-name
   ```

3. Enable root protection on the interface:

   ```
   [edit ... protocols (mstp | rstp | vstp <vlan vlan-id>) interface interface-name]
   user@host# set no-root-port
   ```

4. Verify the configuration of root protect for the spanning-tree instance interface:

   ```
   [edit ... protocols (mstp | rstp | vstp <vlan vlan-id>) interface interface-name]
   user@host# top
   user@host# show ... protocols

   ...
   (mstp | rstp | vstp <vlan vlan-id>) {
     interface interface-name {
       no-root-port;
     }
   }
   ```

NOTE: This is not a complete configuration.

Related Documentation

- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69

CHAPTER 4

Configuring Root Protection in a VPLS Multihoming Environment

Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure

Redundancy is built into many networks through the use of alternate links and paths, which often take the shape of rings.

In the case of multiple hosts attached to customer edge (CE) routers and provider edge (PE) routers to secure virtual private LAN service (VPLS), this practice is often called *multihoming*:

- Multiple hosts attach to CE routers, which are attached to each other as well as to the PE routers that access the VPLS network cloud. Any single link between the edge routers can fail without impacting the hosts' access to the VPLS services.
- This Layer 2 ring connects to the multiprotocol link switching (MPLS) infrastructure through two PE routers. Link breaks on the ring are protected by running a version of the spanning-tree protocol with the root-protect option enabled.

The virtual private network (VPN) protocols at Layer 3, however, are not aware of the blocking state that results from this root protection setup (rings or loops are not permitted at Layer 2 because the Layer 2 protocols will not function properly).

However, to keep the Layer 2 ring functioning in a multihomed environment with link failures, the spanning-tree protocol running on the MX Series routers requires the following additional configuration:

- The VPN protocols have to act on the blocking and unblocking of interfaces by the spanning-tree protocol. Specifically, media access control (MAC) flush messages need to be sent by the blocking PE router to LDP peers in order to flush the MAC addresses learned when other interface ports were blocked.
- Also, if an active PE router with VPLS root protection bridging enabled loses VPLS connectivity, root protection requires that the bridge switch to the other PE router to maintain connectivity. The spanning-tree protocol needs to be aware of the status of the VPLS connectivity on the PE router. If the MAC address cache is not flushed when the topology changes, frames could be sent to the wrong device.

You can control the actions taken by the MX Series router when the topology changes in a multihomed Layer 2 ring VPLS environment using *VPLS root protection*.

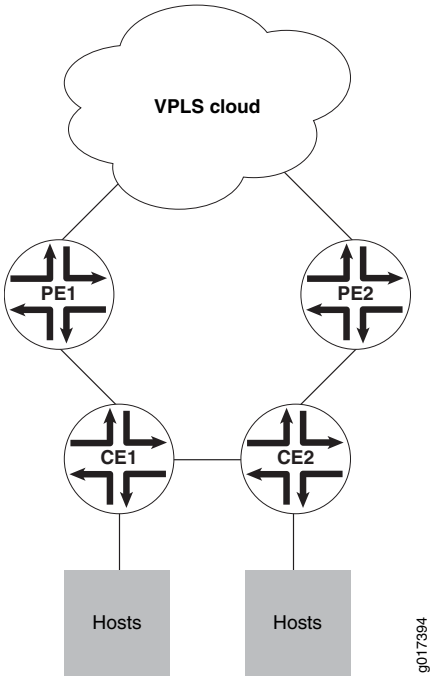
Related Documentation

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 72
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 77
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 78
- Example: Configuring VPLS Root Topology Change Actions on page 76

Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology

Figure 7 on page 73 shows hosts connected to CE routers and to a VPLS network through two PE routers. The CE routers are also connected, forming a kind of ring structure.

Figure 7: VPLS Multihoming Configuration



The two PE routers have their own links to a VPLS network service, but are not directly connected to each other. All four edge routers run some type of spanning-tree protocol with root protection enabled, and only one PE interface will be in the forwarding state, the other being blocked.

Assume this forwarding interface is through PE1. If the link between CE1 and CE2 fails, then the blocking PE2 interface must detect a root protection switch and move to the forwarding state. All of the MAC addresses learned by CE2 that connect to the VPLS network service through PE1 need to be flushed. In the same way, when the link between CE1 and CE2 is restored, PE2 again detects the root protection switch and begins blocking again. Now all of the MAC addresses learned by CE2 that connect through PE2 need to be flushed. All of this is controlled by configuring VPLS root protection topology change actions on the CE routers.

Also, at a global level, each type of spanning-tree protocol will have a priority hold time associated with it. This is the number of seconds, in the range from 1 through 255 seconds, that the system waits to switch to the primary priority when the first core domain comes up. The default is 2 seconds. This allows the maximum number of core domains to come up, and some might be slower than others.

Related Documentation

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 77
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 78
- Example: Configuring VPLS Root Topology Change Actions on page 76

VPLS Multihoming: Priority of the Backup Bridge

When an MX Series router in a VPLS multihomed Layer 2 ring is running a spanning-tree protocol with root protection enabled, you can modify the default actions taken by the MX Series router when the topology changes. To do this, configure the VPLS root protection topology change actions.

The default value of the backup bridge is **32,768**. You can set the backup bridge priority to a value from **0** through **61440**, in increments of 4096.

To change the default value, you can use the following statement:

```
backup-bridge-priority vpls-ring-backup-bridge-priority
```

You can include the statement at the **[edit protocols (mstp | rstp | vstp)]** hierarchy level (to control global spanning-tree protocol behavior) or at the **[edit protocols vstp vlan *vlan-id*]** hierarchy level (to control a particular VLAN).

NOTE: **VPLS root topology change actions are configured independently of VPLS, the spanning-tree protocol, or the spanning-tree protocol root protect option.**

Related Documentation

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71
- VPLS Multihoming: Hold Time Before Switching to Primary Priority on page 74
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 77
- Example: Configuring VPLS Root Topology Change Actions on page 76

VPLS Multihoming: Hold Time Before Switching to Primary Priority

When an MX Series router or an EX Series switch in a VPLS multihomed Layer 2 ring is running a spanning-tree protocol with root protection enabled, you can modify the default actions taken by the router or switch when the topology changes. To do this, configure the VPLS root protection topology change actions.

The default number of seconds to hold before switching to the primary priority when the first core domain comes up is 2 seconds.

To change the default value, you can use the following statement:

```
priority-hold-time seconds
```

You can include the statement at the **[edit protocols (mstp | rstp | vstp)]** hierarchy level (to control global spanning-tree protocol behavior) or at the **[edit protocols vstp vlan *vlan-id*]** hierarchy level (to control a particular VLAN).

NOTE: VPLS root topology change actions are configured independently of VPLS, the spanning-tree protocol, or the spanning-tree protocol root protect option.

Related Documentation

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71
- VPLS Multihoming: Priority of the Backup Bridge on page 74
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 77
- Example: Configuring VPLS Root Topology Change Actions on page 76

VPLS Multihoming: System Identifier for Bridges in the Ring

The system identifier for bridges in the ring is not configured by default.

To configure a system identifier for bridges in the ring, you can use the following statement:

system-id ***system-id-value*** *bridge-host-ip-address(es)*

You can include the statement at the **[edit protocols (mstp | rstp | vstp)]** hierarchy level (to control global spanning-tree protocol behavior) or at the **[edit protocols vstp vlan *vlan-id*]** hierarchy level (to control a particular VLAN).

NOTE: VPLS root topology change actions are configured independently of VPLS, the spanning-tree protocol, or the spanning-tree protocol root protect option.

Related Documentation

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71
- VPLS Multihoming: Priority of the Backup Bridge on page 74
- VPLS Multihoming: Hold Time Before Switching to Primary Priority on page 74
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 77
- Example: Configuring VPLS Root Topology Change Actions on page 76

VPLS Multihoming: Bridge Flush of MAC Cache on Topology Change

When an MX Series router or an EX Series switch in a VPLS multihomed Layer 2 ring is running a spanning-tree protocol with root protection enabled, you can modify the default actions taken by the router or switch when the topology changes. To do this, configure the VPLS root protection topology change actions.

By default, if root protect is enabled and then the topology changes, the bridges do not flush the media access control (MAC) address cache of the MAC addresses learned when other interface ports were blocked.

To change the default behavior, you can use the following statement:

vpls-flush-on-topology-change

You can include the statement at the **[edit protocols (mstp | rstp | vstp)]** hierarchy level (to control global spanning-tree protocol behavior) or at the **[edit protocols vstp vlan *vlan-id*]** hierarchy level (to control a particular VLAN).

Specifically, MAC flush messages are sent from the blocked PE to LDP peers based on the mapping of system identifier to IP addresses as specified using the system-id statement.

NOTE: VPLS root topology change actions are configured independently of VPLS, the spanning-tree protocol, or the spanning-tree protocol root protect option.

Related Documentation

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 77
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 78
- Example: Configuring VPLS Root Topology Change Actions on page 76

Example: Configuring VPLS Root Topology Change Actions

This example configures a bridge priority of **36k**, a backup bridge priority of **44k**, a priority hold time value of **60** seconds, a system identifier of **000203:040506** for IP address **10.1.1.1/32**, and sets the bridge to flush the MAC cache on a topology change for MSTP only.

```
[edit]
protocols {
   mstp {
      bridge-priority 36k;
      backup-bridge-priority 44k;
      priority-hold-time 60;
```

```
        system-id 000203:040506 {
          10.1.1.1/32;
        }
        vpls-flush-on-topology-change;
      }
    }
```

NOTE: This is not a complete configuration.

Related Documentation

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71
- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 72
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 77
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 78

Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior

To configure VPLS root protection topology change actions to control global spanning-tree behavior:

1. Enable configuration of the spanning-tree protocol:

   ```
   [edit]
   user@host# edit protocols (STP Type) (mstp | rstp | vstp)
   ```

2. (Optional) Change the priority of the backup bridge in a VPLS multihomed Layer 2 ring with MPLS infrastructure:

   ```
   [edit protocols (rstp | mstp | vstp)]
   user@host# set backup-bridge-priority vpls-ring-backup-bridge-priority
   ```

3. (Optional) Change number of seconds to hold before switching to the primary priority when the first core domain comes up:

   ```
   [edit protocols (rstp | mstp | vstp)]
   user@host# set priority-hold-time seconds
   ```

4. Configure the system identifier for bridges in the ring:

   ```
   [edit protocols (rstp | mstp | vstp)]
   user@host# set system-id system-id-value bridge-host-ip-address(es)
   ```

   The ***system-id-value*** is configured in the format ***nnnnnn:nnnnnn***, where ***n*** = any digit from **0** to **9**.

   Each ***bridge-host-ip-address*** is a valid host IP address with a **/32** mask.

NOTE: There are no default values for the system identifier or host IP addresses.

5. Configure bridges to flush the MAC address cache (of the MAC addresses learned when other interfaces ports were blocked) when the spanning-tree topology changes:

   ```
   [edit protocols (rstp | mstp | vstp)]
   user@host# set vpls-flush-on-topology-change
   ```

6. Verify the configuration of VPLS root protection topology change actions to control global spanning-tree behavior:

   ```
   [edit]
   protocols {
     (mstp | rstp | vstp) {
       backup-bridge-priority priority; # Default is 32,768.
       priority-hold-time seconds; # Default is 2 seconds.
       system-id system-id-value {
         ip-address;
       }
       vpls-flush-on-topology-change;
     }
   }
   ```

Related Documentation

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71
- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 72
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 78
- Example: Configuring VPLS Root Topology Change Actions on page 76

Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior

To configure VPLS root protection topology change actions to control a particular VLAN:

1. Enable configuration of the spanning-tree protocol VLAN:

   ```
   [edit]
   user@host# edit protocols (STP Type) vstp vlan vlan-id
   ```

2. (Optional) Change the priority of the backup bridge in a VPLS multihomed Layer 2 ring with MPLS infrastructure:

   ```
   [edit protocols vstp vlan vlan-id]
   user@host# set backup-bridge-priority vpls-ring-backup-bridge-priority
   ```

3. (Optional) Change the hold time before switching to the primary priority when the first core domain comes up:

   ```
   [edit protocols vstp vlan vlan-id]
   user@host# set priority-hold-time seconds
   ```

4. Configure the system identifier for bridges in the ring:

   ```
   [edit protocols vstp vlan vlan-id]
   user@host# set system-id system-id-value bridge-host-ip-address(es)
   ```

   The ***system-id-value*** is configured in the format ***nnnnnn:nnnnnn***, where ***n*** = any digit from **0** to **9**.

Each ***bridge-host-ip-address*** is a valid host IP address with a **/32** mask.

NOTE: There are no default values for the system identifier or host IP addresses.

5. Configure bridges to flush the MAC address cache (of the MAC addresses learned when other interfaces ports were blocked) when the spanning-tree topology changes:

```
[edit protocols vstp vlan vlan-id]
user@host# setvpls-flush-on-topology-change
```

6. Verify the configuration of VPLS root protection topology change actions to control a particular VLAN:

```
[edit]
protocols {
  vstp {
    vlan vlan-id {
      backup-bridge-priority priority; # Default is 32,768.
      priority-hold-time seconds; # Default is 2 seconds.
      system-id system-id-value {
        ip-address;
      }
      vpls-flush-on-topology-change;
    }
  }
}
```

Related Documentation

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71
- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 72
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 77
- Example: Configuring VPLS Root Topology Change Actions on page 76

CHAPTER 5

Configuring Layer 2 Protocol Tunneling

Layer 2 Protocol Tunneling Through a Network Overview

Layer 2 protocol tunneling allows Layer 2 protocol data units (PDUs) to be tunneled through a network. This is useful to provide a single spanning-tree protocol domain for subscribers across a service provider network. It is also useful for tunneling Cisco Discovery Protocol (CDP) or VLAN Trunk Protocol (VTP) PDUs across a network.

Layer 2 protocol tunneling is supported on MX Series routers with Enhanced (Dense Port Concentrators) DPCs and Enhanced Queuing (DPCs), see Table 5 on page 82 for a list of the DPCs supported. Layer 2 protocol tunneling is supported on all Modular Port Concentrators (MPCs),

NOTE: **Layer 2 protocol tunneling is not supported on Rev-A DPCs on MX Series routers because of microcode space limitations.**

When a control packet for STP, CDP, or VTP is received on a service provider edge port configured for Layer 2 protocol tunneling, the multicast destination MAC address is rewritten with the predefined multicast tunnel MAC address of **01:00:0c:cd:cd:d0**. The packet is transported across the provider network transparently to the other end of the tunnel and the original multicast destination MAC address is restored when the packet is transmitted.

If a packet is received on a tunnel interface that already has a destination multicast MAC address of **01:00:0c:cd:cd:d0**, the port enters an error state and is shut down. To clear the error condition, the administrator must enter the **clear error mac-rewrite interface *interface-name*** command.

Layer 2 protocol tunneling and MAC rewrite are supported in VPLS, but only certain hardware configurations are supported.

Table 4 on page 82 shows the MPCs and Enhanced DPCs supported when configuring Layer 2 protocol tunneling and VPLS.

Table 4: MAC Rewrite and VPLS Configurations

CE-Facing Interface	PE-Core Facing Interface	Layer 2 Protocol Tunneling
MPC	MPC	Yes
MPC	Enhanced DPC	Yes
Enhanced DPC	MPC	Yes
Enhanced DPC	Enhanced DPC	No

Table 5 on page 82 lists the DPCs that support the Layer 2 tunneling protocol.

Table 5: DPCs Supported for Layer 2 Protocol Tunneling

DPC Name	DPC Model Number
Gigabit Ethernet	
Gigabit Ethernet Enhanced DPC with SFP	DPCE-R-40GE-SFP
Gigabit Ethernet Enhanced Ethernet Services DPC with SFP	DPCE-X-40GE-SFP
Gigabit Ethernet Enhanced Queuing Ethernet Services DPC with SFP	DPCE-X-Q-40GE-SFP
Gigabit Ethernet Enhanced Queuing IP Services DPCs with SFP	DPCE-R-Q-20GE-SFP
Gigabit Ethernet Enhanced Queuing IP Services DPCs with SFP	DPCE-R-Q-40GE-SFP
10-Gigabit Ethernet	
10-Gigabit Ethernet Enhanced DPCs with XFP	DPCE-R-2XGE-XFP
10-Gigabit Ethernet Enhanced DPCs with XFP	DPCE-R-4XGE-XFP
10-Gigabit Ethernet Enhanced Ethernet Services DPC with XFP	DPCE-X-4XGE-XFP
10-Gigabit Ethernet Enhanced Queuing Ethernet Services DPC with XFP	DPCE-X-Q-4XGE-XFP
10-Gigabit Ethernet Enhanced Queuing IP Services DPC with XFP	DPCE-R-Q-4XGE-XFP
Multi-Rate Ethernet	
Multi-Rate Ethernet Enhanced DPC with SFP and XFP	DPCE-R-20GE-2XGE

Table 5: DPCs Supported for Layer 2 Protocol Tunneling *(continued)*

DPC Name	DPC Model Number
Multi-Rate Ethernet Enhanced Ethernet Services DPC with SFP and XFP	DPCE-X-20GE-2XGE
Multi-Rate Ethernet Enhanced Queuing IP Services DPC with SFP and XFP	DPCE-R-Q-20GE-2XGE
Tri-Rate Ethernet	
Tri-Rate Enhanced DPC	DPCE-R-40GE-TX
Tri-Rate Enhanced Ethernet Services DPC	DPCE-X-40GE-TX

NOTE: When an MX Series router or EX Series switch sends a RADIUS access request, the **Chargeable-User-Identity** parameter is sent with an empty field. For more information about configuring RADIUS, see the *Junos Subscriber Access Configuration Guide*.

Related Documentation

- Configuring Layer 2 Protocol Tunneling on page 84
- Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 88
- Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 89

Layer 2 Protocol Tunneling Configuration Guidelines

To configure the interface where Layer 2 protocol tunneling is enabled, include the interface **ge-*fpc/pic/port*** statement at the **[edit protocols** layer2-control**]** hierarchy level.

Keep the following guidelines in mind when configuring Layer 2 protocol tunneling:

- Layer 2 protocol tunneling is supported on MX Series routers with enhanced queuing Dense Port Concentrators (DPCs).
- Layer 2 protocol tunneling must be configured on the interfaces at each end of the tunnel.
- You can enable Layer 2 protocol tunneling for untagged interfaces and single-identifier tagged interfaces only.
- For single-identifier tagged ports, configure a logical interface with the native VLAN identifier. This configuration associates the untagged control packets with a logical interface.
- You cannot enable Layer 2 protocol tunneling for double-identifier tagged interfaces.

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 81
- *MAC Address Rewriting Enabled for Layer 2 Protocol Tunneling*
- Configuring Layer 2 Protocol Tunneling on page 84

Configuring Layer 2 Protocol Tunneling

To configure Layer 2 protocol tunneling, you must specify the protocol that is to be tunneled using the Layer 2 tunnel:

- **cdp**—Cisco Discovery Protocol.
- **stp**—All versions of the spanning-tree protocol.
- **vtp**—Tunnel the VLAN trunk protocol.

For each protocol specified, a static destination MAC address corresponding to the protocol being tunneled is installed in the MAC table.

To specify the protocol that will be tunneled by the Layer 2 protocol tunneling, you can include the protocol **(cdp | stp | vtp)** statement at the **[edit protocols** layer2-control mac-rewrite interface **ge-*fpc/pic/port*]** hierarchy level.

NOTE: **When CDP, STP, or VTP is configured for tunneling on a customer-facing port in a provider bridge, the corresponding protocol should not be enabled for operation on that interface.**

To configure Layer 2 protocol tunneling, you must enable MAC address rewriting by installing the destination multicast tunnel MAC address of **01:00:0c:cd:cd:d0** in the MAC table.

To enable MAC address rewriting, include the mac-rewrite statement at the **[edit protocols** layer2-control**]** hierarchy level.

When enabling MAC address rewriting for Layer 2 protocol tunneling, the following guidelines apply:

- You can enable Layer 2 protocol tunneling for untagged interfaces.
- You can enable Layer 2 protocol tunneling for single-identifier tagged ports.
- You cannot enable Layer 2 protocol tunneling for double-identifier tagged interfaces

To configure Layer 2 protocol tunneling:

1. Enable MAC address rewriting for Layer 2 protocol tunneling using mac-rewrite.

   ```
   [edit]
   user@host# set protocols layer2-control mac-rewrite
   ```

2. Configure the Layer 2 protocol tunnel interface.

   ```
   [edit protocols layer2-control mac-rewrite]
   ```

```
user@host# set interface ge-fpc/pic/port
```

3. Configure the Layer 2 protocol to be tunneled.

```
[edit protocols layer2-control mac-rewrite interface ge-fpc/pic/port]
user@host# set protocol (cdp | stp | vtp | pvstp)
```

4. Verify the configuration.

```
user@host# show protocols
layer2-control {
  mac-rewrite {
    interface ge-fpc/pic/port {
      protocol (cdp | stp | vtp | pvstp);
    }
  }
}
```

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 81
- Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 88
- Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 89

CHAPTER 6

Monitoring Layer 2 Spanning-Tree Protocol

Checking the Status of Spanning-Tree Instance Interfaces

On an MX Series router with a spanning-tree protocol enabled, the detection of a possible bridging loop from spanning-tree protocol operation can raise a bridge protocol data unit (BPDU) error condition on the affected spanning-tree instance interface.

To check whether a spanning-tree instance interface is blocked due to a BPDU error condition:

1. To check the status of spanning-tree instance interface, use the **show interfaces** command:

   user@host> **show interfaces** *interface-name*

2. You can determine the status of the interface as follows:

   - If the **BPDU Error** field is **none**, the interface is enabled.
   - If the **BPDU Error** field is **Detected** and the link is **down**, the interface is blocked.

Related Documentation

- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69
- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57
- BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 59
- BPDU Protection on All Edge Ports of the Bridge on page 59

- Clearing the Blocked Status of a Spanning-Tree Instance Interface on page 88

Clearing the Blocked Status of a Spanning-Tree Instance Interface

To clear the blocked status of a spanning-tree instance interface:

- Use the **clear error bpdu** operational mode command:

  user@host> clear error bpdu interface **interface** ***interface-name***

NOTE: When you configure BPDU protection on individual interfaces (as opposed to on all the edge ports of the bridge), you can use the disable-timeout ***seconds*** option to specify that a blocked interface is automatically cleared after the specified time interval elapses (unless the interval is 0). For configuration details, see "Configuring BPDU Protection for Spanning-Tree Instance Interfaces" on page 60.

Related Documentation

- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69
- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57
- BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 59
- BPDU Protection on All Edge Ports of the Bridge on page 59
- Checking the Status of Spanning-Tree Instance Interfaces on page 87

Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface

To check whether a spanning-tree instance interface is blocked due to a MAC rewrite error condition:

1. Use the **show interfaces** operational mode command:

   user@host> **show interfaces** ***interface-name***

2. You can determine the status of the interface as follows:

   - If the value in the **Physical interface** includes **Enabled, Physical link is Up** and the value of the **BPDU Error** field is **None**, the interface is enabled
   - If the value in the **Physical interface** field is **Enabled, Physical link is Down** and the value in the **BPDU Error** field is **Detected**, the interface is blocked.

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 81
- Configuring Layer 2 Protocol Tunneling on page 84
- Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 89

Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface

To clear the blocked status of a spanning-tree instance interface:

- Use the **clear error bpdu** operational mode command:

  user@host> clear error bpdu interface **interface** *interface-name*

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 81
- Configuring Layer 2 Protocol Tunneling on page 84
- Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 88

Tracing Spanning-Tree Operations

You can enable global routing protocol tracing options at the **[edit routing-options]** Hierarchy Level. For general information about tracing and global tracing options, see the statement summary for the global *traceoptions* statement in the *Junos OS Routing Protocols Library*.

In addition, you can enable STP-specific trace options at the following hierarchy levels:

- **[edit** ***logical-systems logical-system-name*** protocols (mstp | rstp | vstp)**]**
- **[edit** ***logical-systems logical-system-name routing-instances routing-instance-name*** protocols (mstp | rstp | vstp)**]**
- **[edit** protocols (mstp | rstp | vstp)**]**
- **[edit** ***routing-instances routing-instance-name*** protocols (mstp | rstp | vstp)**]**

The routing instance type can be either **virtual-switch** or **layer2-control**.

To enable tracing of spanning-tree protocol operations:

1. Enable configuration of the spanning-tree protocol whose operations are to be traced:

   ```
   [edit]
   user@host# edit ... protocols (mstp | rstp | vstp)
   ```

2. Enable configuration of spanning-tree protocol-specific trace options:

   ```
   [edit ... protocols (mstp | rstp | vstp)]
   user@host# edit traceoptions
   ```

3. Configure the files that contain trace logging information:

   ```
   [edit ... protocols (mstp | rstp | vstp)]
   user@host# set file filename <files number> <size bytes>
   <world-readable | no-world-readable>
   ```

4. Configure spanning-tree protocol-specific options.

   a. To enable a spanning-tree protocol-specific option, include the **flag** statement:

      ```
      [edit ... protocols (mstp | rstp | vstp)]
      user@host# set flag flag <flag-modifier> <disable>
      ```

      You can specify the following spanning-tree protocol-specific ***flag*** options:

      - **all**—Trace all operations.
      - **all-failures**—Trace all failure conditions.
      - **bpdu**—Trace BPDU reception and transmission.
      - **bridge-detection-state-machine**—Trace the bridge detection state machine.
      - **events**—Trace events of the protocol state machine.
      - **port-information-state-machine**—Trace the port information state machine.
      - **port-migration-state-machine**—Trace the port migration state machine.
      - **port-receive-state-machine**—Trace the port receive state machine.
      - **port-role-transit-state-machine**—Trace the port role transit state machine.
      - **port-role-select-state-machine**—Trace the port role selection state machine.
      - **port-transmit-state-machine**—Trace the port transmit state machine.
      - **port-state-transit-state-machine**—Trace the port state transit state machine.
      - **ppmd**—Trace the state and events for the ppmd process.
      - **state-machine-variables**—Trace when the state machine variables change.
      - **timers**—Trace protocol timers.
      - **topology-change-state-machine**—Trace the topology change state machine.

      NOTE: Use the trace flag all with caution. This flag may cause the CPU to become very busy.

   b. To disable an individual spanning-tree protocol-specific option, include the **disable** option with the **flag** statement.

5. Verify the spanning-tree protocol-specific trace options:

   ```
   [edit]
   ...
     routing-options {
       traceoptions {
         ...global-trace-options-configuration...
       }
       }
     }
     protocols {
       (mstp | rstp | vstp) {
   ```

```
        traceoptions { # Spanning-tree protocol-specific.
          file filename <files number> <size bytes> <world-readable | no-world-readable>;
          flag flag <flag-modifier> <disable>;
        }
      }
    }
  ...
```

Related Documentation

- Example: Tracing Spanning-Tree Protocol Operations on page 91

Example: Tracing Spanning-Tree Protocol Operations

Trace only unusual or abnormal operations to **/var/log/stp-log**:

```
[edit]
routing-options {
  traceoptions {
    file routing-log size 10m world-readable;
    flag all;
  }
}
protocols {
  rstp {
    traceoptions {
      file rstp-log size 10m world-readable;
      flag all;
    }
  }
}
```

Related Documentation

- Tracing Spanning-Tree Operations on page 89

CHAPTER 7

Configuration Statements for Spanning-Tree Protocols

protocols (STP Type)

Syntax

```
protocols {
    mstp { ... }
    rstp { ... }
    vstp { ... }
}
```

Hierarchy Level

[edit],
[edit logical-systems *logical-system-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*],
[edit routing-instances *routing-instance-name*]

Release Information

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description

Configure the Spanning Tree Protocol type as MSTP, RSTP, or VSTP.

Options

mstp—Configure the protocol as Multiple Spanning Tree.

rstp—Configure the protocol as Rapid Spanning Tree.

vstp—Configure the protocol as VLAN Spanning Tree.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring RSTP (CLI Procedure)*
- *Configuring MSTP*
- Configuring MST Instances on a Physical Interface on page 34
- *Configuring VLAN Spanning Tree Protocol*
- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring VLAN Spanning Tree Protocol on page 36
- *Understanding MSTP for EX Series and QFX Series Switches*

access-trunk

Syntax access-trunk;

Hierarchy Level [edit logical-systems *logical-system-name* protocols vstp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp],
[edit protocols vstp vlan *vlan-identifier* interface *interface-name*],
[edit routing-instances *routing-instance-name* instance-type (layer2-control | virtual-switch)]

Description Enable untagged RTSP BDPUs to be sent and received on the interface.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Example: Configuring VSTP on a Trunk Port with Tagged Traffic*

backup-bridge-priority

Syntax backup-bridge-priority *priority*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*],
[edit protocols (mstp | rstp)],
[edit protocols vstp vlan *vlan-id*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*]

Release Information Statement introduced in Junos OS Release 10.0.

Description Determine the priority of the backup bridge in a VPLS multihomed Layer 2 ring with MPLS infrastructure.

Options *priority*—The backup bridge priority can be set only in increments of 4096.

Range: 0 through 61,440

Default: 32,768

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 78
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 77
- VPLS Multihoming: Priority of the Backup Bridge on page 74

bpdu-destination-mac-address (Spanning Tree)

Syntax bpdu-destination-mac-address provider-bridge-group;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit protocols (mstp | rstp)],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp)]

Release Information
Statement introduced in Junos OS Release 9.2.
Support for logical systems added in Junos OS Release 9.6.

Description Enable MX Series router to participate in the provider Rapid Spanning Tree Protocol (RSTP) instance or a provider Multiple Spanning Tree Protocol (MSTP) instance.

Default If the **bpdu-destination-mac-address** statement is not configured, the bridge participates in the customer RSTP instance, transmitting and receiving standard RSTP BPDU packets.

Options
provider-bridge-group—The destination MAC address of the BPDU packets transmitted is the provider bridge group address **01:80:c2:00:00:08**. Received BPDU packets with this destination MAC address are accepted and passed to the Routing Engine.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Understanding BPDUs Used for Exchanging Information Among Bridges on page 22
- Provider Bridge Participation in RSTP or MSTP Instances on page 51
- Configuring Rapid Spanning Tree Protocol on page 28
- Configuring Multiple Spanning Tree Protocol on page 31

bpdu-block-on-edge

Syntax bpdu-block-on-edge;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp | vstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp | vstp)],
[edit protocols (mstp | rstp| vstp)],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp | vstp)]

Release Information
Statement introduced in Junos OS Release 9.4.
Support for logical systems added in Junos OS Release 9.6.

Description Enable BPDU blocking on the edge ports of a virtual switch.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57
- BPDU Protection on All Edge Ports of the Bridge on page 59
- Configuring BPDU Protection on All Edge Ports on page 61
- *Configuring BPDU Protection on Spanning Tree Interfaces*
- *rstp*
- *mstp*
- *vstp*

bpdu-timeout-action

Syntax bpdu-timeout-action (log | block);

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp | vstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp | vstp)],
[edit protocols (mstp | rstp | vstp) interface],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp | vstp)]

Release Information
Statement introduced in Junos OS Release 9.4.
Support for logical systems added in Junos OS Release 9.6.

Description Provide STP loop protection for a given STP family protocol interface.

Default If the **bpdu-timeout-action** statement is not configured, an interface that stops receiving BPDUs will transition to the designated port (forwarding) state, creating a potential loop.

Options
log—The interface logs the fact that it has not received BPDUs during the timeout interval.

block—The interface is blocked and the fact that the interface has not received BPDUs during the timeout interval is logged.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding Loop Protection for Spanning-Tree Instance Interfaces on page 66
- Configuring Loop Protection for a Spanning-Tree Instance Interface on page 68
- Example: Enabling Loop Protection for Spanning-Tree Protocols on page 67
- *rstp*
- *mstp*
- *vstp*

bridge-priority

Syntax bridge-priority *priority*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* protocols mstp msti *msti-id*],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mstp msti *msti-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*],
[edit protocols (mstp | rstp)],
[edit protocols mstp msti *msti-id*],
[edit protocols vstp vlan *vlan-id*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit routing-instances *routing-instance-name* protocols mstp msti *msti-id*],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*]

Release Information
Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Determine which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.

Options ***priority***—The bridge priority can be set only in increments of 4096.

Range: 0 through 61,440

Default: 32,768

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Bridge Priority for Election of Root Bridge and Designated Bridge on page 51
- *Example: Configuring Network Regions for VLANs with MSTP*
- *Understanding MSTP for EX Series and QFX Series Switches*
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

configuration-name

Syntax configuration-name *configuration-name*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mstp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mstp],
[edit protocols mstp],
[edit routing-instances *routing-instance-name* protocols mstp]

Release Information Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Specify the configuration name , which is the MSTP region name carried in the MSTP BPDUs.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding BPDUs Used for Exchanging Information Among Bridges on page 22
- Configuring Multiple Spanning Tree Protocol on page 31
- *Configuring MSTP*
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Example: Configuring Network Regions for VLANs with MSTP*
- *Example: Configuring Faster Convergence and Improved Network Stability with RSTP*
- *Understanding MSTP for EX Series and QFX Series Switches*

cost

Syntax cost *cost*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit logical-systems *logical-system-name* protocols mstp msti *msti-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mstp msti *msti-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id* interface *interface-name*],
[edit protocols (mstp | rstp | vstp) interface *interface-name*],
[edit protocols mstp msti *msti-id* interface *interface-name*],
[edit protocols vstp vlan *vlan-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols mstp msti *msti-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id* interface *interface-name*]

Release Information Statement introduced in Junos OS Release 8.4.
Support for logical systems added in Junos OS Release 9.6.

Description Configure link cost to control which bridge is the designated bridge and which port is the designated port. By default, the link cost is determined by the link speed.

Options ***cost***—(Optional) Link cost associated with the port.

Range: 1 through 200,000,000

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Spanning-Tree Instance Interface on page 25
- Spanning-Tree Instance Interface Cost on page 27
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Understanding RSTP for EX Series and QFX Series Switches*
- *Understanding MSTP for EX Series and QFX Series Switches*
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

disable

Syntax disable;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols mstp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mstp],
[edit protocols mstp |rstp |vstp],
[edit routing-instances *routing-instance-name* protocols mstp]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Disable the entire MSTP, RSTP, or VSTP instance.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Multiple Spanning Tree Protocol on page 31
- Disabling MSTP on page 35
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Example: Configuring Network Regions for VLANs with MSTP*
- *Example: Configuring Faster Convergence and Improved Network Stability with RSTP*
- *Understanding RSTP for EX Series and QFX Series Switches*
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

edge

Syntax edge;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit logical-systems *logical-system-name* protocols mstp msti *msti-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mstp msti *msti-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id* interface *interface-name*],
[edit protocols (mstp | rstp | vstp) interface *interface-name*],
[edit protocols mstp msti *msti-id* interface *interface-name*],
[edit protocols vstp vlan *vlan-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols mstp msti *msti-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id* interface *interface-name*]

Release Information
Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Configure interfaces as edge ports. Edge ports do not expect to receive BPDUs. If a BPDU is received, the port becomes a nonedge port.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Spanning-Tree Instance Interface on page 25
- Configuring a Spanning-Tree Instance Interface as an Edge Port for Faster Convergence on page 54
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Example: Configuring Network Regions for VLANs with MSTP*
- *Example: Configuring Faster Convergence and Improved Network Stability with RSTP*
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

extended-system-id

Syntax extended-system-id *identifier*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols rstp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols rstp],
[edit protocols rstp],
[edit routing-instances *routing-instance-name* protocols rstp]

Release Information Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description The extended system ID is used to specify different bridge identifiers for different RSTP or STP routing instances.

Options ***identifier***—Specify the system identifier to use for the RSTP or STP instance.

Range: 0 through 4095

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28
- *Configuring RSTP (CLI Procedure)*
- *Example: Configuring Faster Convergence and Improved Network Stability with RSTP*
- *Understanding RSTP for EX Series and QFX Series Switches*

force-version (IEEE 802.1D STP)

Syntax force-version stp;

Hierarchy Level [edit logical-systems *logical-system-name* protocols (rstp | vstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (rstp | vstp)],
[edit protocols (rstp | vstp)],
[edit routing-instances *routing-instance-name* protocols (rstp | vstp)]

Release Information Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Force the spanning-tree version to be the original IEEE 803.1D STP.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 53
- Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 52
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

forward-delay

Syntax forward-delay *seconds*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*],
[edit protocols (mstp | rstp)],
[edit protocols vstp vlan *vlan-id*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*]

Release Information
Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Specify the length of time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.

Options
seconds—(Optional) Number of seconds the bridge port remains in the listening and learning states.

Range: 4 through 30

Default: 15 seconds

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Forward Delay Before Ports Transition to Forwarding State on page 23
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Example: Configuring Network Regions for VLANs with MSTP*
- *Example: Configuring Faster Convergence and Improved Network Stability with RSTP*
- *Understanding MSTP for EX Series and QFX Series Switches*
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

hello-time

Syntax hello-time *seconds*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*],
[edit protocols (mstp | rstp)],
[edit protocols vstp vlan *vlan-id*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*]

Release Information
Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Specify the number of seconds between transmissions of configuration BPDUs by the root bridge.

Options ***seconds***—(Optional) Number of seconds between transmissions of configuration BPDUs.

Range: 1 through 10

Default: 2 seconds

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Hello Time for Root Bridge to Transmit Hello BPDUs on page 58
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Example: Configuring Network Regions for VLANs with MSTP*
- *Example: Configuring Faster Convergence and Improved Network Stability with RSTP*
- *Understanding MSTP for EX Series and QFX Series Switches*
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

interface (Spanning Tree)

Syntax

```
interface interface-name {
  bpdu-timeout-action {
    alarm;
    block;
  }
  cost cost;
  edge;
  mode (p2p | shared);
  no-root-port;
  priority interface-priority;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (mstp | rstp | vstp)],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp | vstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*],
[edit protocols (mstp | rstp | vstp)],
[edit protocols vstp vlan *vlan-id*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp | vstp)],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*]

Release Information

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description

Configure the interface to participate in the RSTP, MSTP, or VSTP instance.

Options

interface-name—Name of a Gigabit Ethernet or 10-Gigabit Ethernet interface.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Spanning-Tree Instance Interface on page 25
- *show spanning-tree interface*
- *Understanding RSTP for EX Series and QFX Series Switches*
- *Understanding MSTP for EX Series and QFX Series Switches*
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

max-age

Syntax max-age *seconds*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*],
[edit protocols (mstp | rstp)],
[edit protocols vstp vlan *vlan-id*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*]

Release Information
Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Specify the maximum expected arrival time of hello BPDUs.

Options ***seconds***—(Optional) Number of seconds expected between hello BPDUs.

Range: 6 through 40

Default: 20 seconds

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Maximum Age for Awaiting Arrival of Hello BPDUs on page 58
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Example: Configuring Network Regions for VLANs with MSTP*
- *Example: Configuring Faster Convergence and Improved Network Stability with RSTP*
- *Understanding MSTP for EX Series and QFX Series Switches*
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

max-hops

Syntax max-hops *hops*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols mstp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mstp],
[edit protocols mstp],
[edit routing-instances *routing-instance-name* protocols mstp]

Release Information
Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Configure the maximum number of hops a BPDU can be forwarded in the MSTP region.

Options
hops—(Optional) Number of hops the BPDU can be forwarded.
Range: 1 through 255
Default: 19 hops

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Multiple Spanning Tree Protocol on page 31
- *Configuring MSTP*
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Example: Configuring Network Regions for VLANs with MSTP*
- *Understanding MSTP for EX Series and QFX Series Switches*

mode

Syntax mode (p2p | shared);

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id* interface *interface-name*],
[edit protocols (mstp | rstp | vstp) interface *interface-name*],
[edit protocols vstp vlan *vlan-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id* interface *interface-name*]

Release Information Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Configure link mode to identify point-to-point links.

Default When the link is configured as full-duplex, the default link mode is **p2p**. When the link is configured half-duplex, the default link mode is **shared**.

NOTE:

Options **p2p**—The link is point to point.

shared—The link is shared media.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Spanning-Tree Instance Interface on page 25
- Spanning-Tree Instance Interface Point-to-Point Link Mode on page 27
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Example: Configuring Network Regions for VLANs with MSTP*
- *Example: Configuring Faster Convergence and Improved Network Stability with RSTP*
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

msti

Syntax

```
msti msti-id {
  bridge-priority priority;
  vlan (vlan-id | vlan-range|open-set-of-values);
  interface (interface-name | all) {
    cost cost;
    edge;
    priority interface-priority;
  }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols mstp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mstp],
[edit protocols mstp],
[edit routing-instances *routing-instance-name* protocols mstp]

Release Information

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description

Configure the multiple spanning-tree instance (MSTI) identifier.

Options

msti-id—MSTI instance identifier.

Range: 1 through 64

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Multiple Spanning Tree Protocol on page 31
- Configuring MST Instances on a Physical Interface on page 34
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Example: Configuring Network Regions for VLANs with MSTP*
- *Understanding MSTP for EX Series and QFX Series Switches*

mstp

Syntax

```
mstp {
  bpdu-block-on-edge;
  bridge-priority priority;
  configuration-name configuration-name;
  disable;
  forward-delay seconds;
  hello-time seconds;
  max-age seconds;
  max-hops hops;
  priority-hold-time seconds;
  revision-level revision-level;
  interface interface-name {
    bpdu-timeout-action {
      alarm;
      block;
    }
    cost cost;
    edge;
    mode (p2p | shared);
    no-root-port;
    priority interface-priority;
  }
  msti msti-id {
    bridge-priority priority;
    interface interface-name {
      cost cost;
      edge;
      priority interface-priority;
    }
    vlan vlan-id;
  }
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols],
[edit protocols],
[edit routing-instances *routing-instance-name* protocols]

Release Information

Statement introduced in Junos OS Release 8.4.
bpdu-block-on-edge statement added in Junos OS Release 9.4.
bpdu-timeout-action statement added in Junos OS Release 9.4.
Support for logical systems added in Junos OS Release 9.6.

Description

Configure MSTP parameters.

Options

The statements are explained separately.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Multiple Spanning Tree Protocol on page 31

no-root-port

Syntax
no-root-port;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id* interface *interface-name*],
[edit protocols (mstp | rstp | vstp) interface *interface-name*],
[edit protocols vstp vlan *vlan-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id* interface *interface-name*]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description
Ensure the port is the spanning-tree designated port. If the port receives superior bridge protocol data unit (BPDU) packets, root protect moves this port to a root-prevented spanning-tree state.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 69
- Enabling Root Protection for a Spanning-Tree Instance Interface on page 70

priority (Protocols STP)

Syntax priority *interface-priority*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit logical-systems *logical-system-name* protocols mstp msti *msti-id* interface *interface-name*],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mstp msti *msti-id* interface *interface-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id* interface *interface-name*],
[edit protocols (mstp | rstp | vstp) interface *interface-name*],
[edit protocols mstp msti *msti-id* interface *interface-name*],
[edit protocols vstp *vlan-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp | vstp) interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols mstp msti *msti-id* interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id* interface *interface-name*]

Release Information Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Use the interface priority to control which interface is elected as the root port. The interface priority must be set in increments of 16.

Options ***priority***—(Optional) Interface priority.

Range: 0 through 240

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Spanning-Tree Instance Interface on page 25
- Configuring a Spanning-Tree Instance Interface as an Edge Port for Faster Convergence on page 54
- Spanning-Tree Instance Interface Priority on page 26

priority-hold-time

Syntax priority-hold-time *seconds*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit protocols (mstp | rstp)],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp)],

Release Information Statement introduced in Junos OS Release 10.0.

Description Specify the number of seconds to hold before switching to the primary priority when the first core domain comes up.

Options ***seconds***—Number of seconds to hold before switching to primary priority.

Range: 1 through 255

Default: 2 seconds

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- VPLS Multihoming: Hold Time Before Switching to Primary Priority on page 74

revision-level

Syntax revision-level *revision-level*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols mstp],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mstp],
[edit protocols mstp],
[edit routing-instances *routing-instance-name* protocols mstp]

Release Information Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Set the revision number of the MSTP configuration.

Options ***revision-level***—Configure the revision number of the MSTP region configuration.

Range: 0 through 65,535

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Multiple Spanning Tree Protocol on page 31
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Example: Configuring Network Regions for VLANs with MSTP*
- *Understanding MSTP for EX Series and QFX Series Switches*

rstp

Syntax

```
rstp {
  bpdu-block-on-edge;
  bpdu-destination-mac-address provider-bridge-group;
  bridge-priority priority;
  extended-system-id;
  force-version stp;
  forward-delay seconds;
  hello-time seconds;
  max-age seconds;
  interface interface-name {
    bpdu-timeout-action {
      alarm;
      block;
    }
    cost cost;
    edge;
    mode (p2p | shared);
    no-root-port;
    priority interface-priority;
  }
  priority-hold-time seconds;
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols],
[edit protocols],
[edit routing-instances *routing-instance-name* protocols]

Release Information

Statement introduced in Junos OS Release 8.4.
bpdu-block-on-edge statement added in Junos OS Release 9.4.
bpdu-timeout-action statement added in Junos OS Release 9.4.
Support for logic systems added in Junos OS Release 9.6.

Description

Configure RSTP parameters.

Options

The statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Rapid Spanning Tree Protocol on page 28

system-id

Syntax

```
system-id system-id-value {
  ip-address(es);
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*],
[edit protocols (mstp | rstp)],
[edit protocols vstp vlan *vlan-id*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*]

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Determine the system identifier value for bridges in a VPLS multihomed Layer 2 ring with MPLS infrastructure.

Options

system-id-value—System identifier in the format ***nnnnnn:nnnnnn***, where ***n*** = any digit from 0 through 9.

Range: Any valid value

Default: None

ip-address(es)—Valid IP host addresses in the format ***ip-address/32***.

Range: Any valid IP address

Default: None

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 71
- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 72
- VPLS Multihoming: System Identifier for Bridges in the Ring on page 75

traceoptions (Spanning Tree)

Syntax

```
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols (mstp | rstp | vstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp | vstp)],
[edit protocols (mstp | rstp | vstp | vstp vlan *vlan-id*)],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp | vstp)]

Release Information

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description

Set protocol-level tracing options for spanning-tree protocols.

Default

The default STP protocol-level trace options are inherited from the global **traceoptions** statement.

Options

disable—(Optional) Disable the tracing operation. One use of this option is to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks. We recommend that you place STP tracing output in the file **/var/log/stp-log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the **size** option.

Range: 2 through 1000 files

Default: 1 trace file only

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. The following are the STP-specific tracing options:

- **all**—Trace all operations.
- **all-failures**—Trace all failure conditions.
- **bpdu**—Trace BPDU reception and transmission.
- **bridge-detection-state-machine**—Trace the bridge detection state machine.

- **events**—Trace events of the protocol state machine.
- **port-information-state-machine**—Trace the port information state machine.
- **port-migration-state-machine**—Trace the port migration state machine.
- **port-receive-state-machine**—Trace the port receive state machine.
- **port-role-transit-state-machine**—Trace the port role transit state machine.
- **port-role-select-state-machine**—Trace the port role selection state machine.
- **port-state-transit-state-machine**—Trace the port state transit state machine.
- **port-transmit-state-machine**—Trace the port transmit state machine.
- **ppmd**—Trace the state and events for the ppmd process.
- **state-machine-variables**—Trace when the state machine variables change.
- **timers**—Trace protocol timers.
- **topology-change-state-machine**—Trace the topology change state machine.

The following are the global tracing options:

- **all**—All tracing operations.
- **config-internal**—Trace configuration internals.
- **general**—Trace general events.
- **normal**—All normal events.

Default: If you do not specify this option, only unusual or abnormal operations are traced.

- **parse**—Trace configuration parsing.
- **policy**—Trace policy operations and actions.
- **regex-parse**—Trace regular-expression parsing.
- **route**—Trace routing table changes.
- **state**—Trace state transitions.
- **task**—Trace protocol task processing.
- **timer**—Trace protocol task timer processing.

no-world-readable—(Optional) Prevent any user from reading the log file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the ***trace-file*** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you must also specify a maximum number of trace files with the files option.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through the maximum file size supported on your system

Default: 1 MB

world-readable—(Optional) Allow any user to read the log file.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Spanning-Tree Protocol Trace Options on page 28
- Tracing Spanning-Tree Operations on page 89
- Example: Tracing Spanning-Tree Protocol Operations on page 91

vlan (MSTP)

Syntax vlan *vlan-id*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols mstp msti *msti-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mstp msti *msti-id*],
[edit protocols mstp msti *msti-id*],
[edit routing-instances *routing-instance-name* protocols mstp msti *msti-id*]

Release Information
Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Configure the VLAN of an MSTI or VSTP instance or configure the VLAN range of an MSTI.

Options
vlan-id—The VLAN identifier associated with the MSTI.

vlan-id-range—Range of VLAN identifiers associated with the MSTI in the form ***minimum-vlan-id-maximum-vlan-id***. VLAN identifier ranges are not supported for VSTP.

Range: 1 through 4096

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Multiple Spanning Tree Protocol on page 31
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

vlan (VSTP)

Syntax

```
vlan vlan-id {
  bridge-priority priority;
  forward-delay seconds;
  hello-time seconds;
  max-age seconds;
  interface interface-name {
    cost cost;
    edge;
    mode (p2p | shared);
    no-root-port;
    priority interface-priority;
  }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* protocols vstp],
[edit protocols vstp]

Release Information Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.

Description Configure VSTP VLAN parameters.

Options The statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring VLAN Spanning Tree Protocol on page 36
- *Understanding VSTP for EX Series Switches and QFX Series Switches*

vpls-flush-on-topology-change

Syntax vpls-flush-on-topology-change;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* protocols vstp vlan *vlan-id*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*],
[edit protocols (mstp | rstp)],
[edit protocols vstp vlan *vlan-id*],
[edit routing-instances *routing-instance-name* protocols (mstp | rstp)],
[edit routing-instances *routing-instance-name* protocols vstp vlan *vlan-id*]

Release Information Statement introduced in Junos OS Release 10.0.

Description Determine the action the bridge should take when the topology of a multihomed Layer 2 ring with MPLS infrastructure changes: flush the media access control (MAC) cache or not. By default, the bridge does not flush the cache when the topology changes.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- VPLS Multihoming: Bridge Flush of MAC Cache on Topology Change on page 76

vstp

Syntax

```
vstp {
  bpdu-block-on-edge;
  force-version stp;
  interface interface-name {
    bpdu-timeout-action {
      alarm;
      block;
    }
    cost cost;
    edge;
    mode (p2p | shared);
    no-root-port;
    priority interface-priority;
  }
  priority-hold-time seconds;
  vlan vlan-id {
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    max-age seconds;
    interface interface-name {
      access-trunk
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost cost;
      edge;
      mode (p2p | shared);
      no-root-port;
      priority interface-priority;
    }
  }
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols],
[edit protocols],
[edit routing-instances *routing-instance-name* protocols]

Release Information

Statement introduced in Junos OS Release 9.0.
bpdu-block-on-edge statement added in Junos OS Release 9.4.
bpdu-timeout-action statement added in Junos OS Release 9.4.
Support for logical systems added in Junos OS Release 9.6.

Description

Configure VSTP parameters.

Options The statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring VLAN Spanning Tree Protocol on page 36

bpdu-block

Syntax

```
bpdu-block {
  interface (interface-name disable | all);
  disable-timeout seconds;
}
```

Hierarchy Level [edit protocols layer2-control]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Enable BPDU blocking on an interface.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57
- BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 59
- Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 60
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches*

disable-timeout

Syntax disable-timeout *seconds*;

Hierarchy Level [edit protocols layer2-control bpdu-block]

Release Information Statement introduced in Junos OS Release 9.4.

Description Configure the timeout value to periodically check to see if an interface is still disabled with BPDU blocking. If this option is not configured, the interface is not periodically checked and remains disabled.

Options *seconds*—Disable timeout value.

Range: 10 through 3600

Default: If this option is not configured, the interface is not periodically checked and remains disabled.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57
- BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 59

enable-all-ifl

Syntax enable-all-ifl;

Hierarchy Level [edit protocols layer2-control mac-rewrite interface *interface-name*]

Release Information Statement introduced in Junos OS Release 13.3.

Description Enable tunneling for STP, VTP, and CDP on all logical interfaces (VLANs) configured on the interface.

NOTE: Tunneling on all logical interfaces is enabled automatically for PVSTP.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 81
- protocol on page 134

interface (BPDU Blocking)

Syntax interface *interface-name*;

Hierarchy Level [edit protocols layer2-control bpdu-block]

Release Information Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure the interface to participate in BPDU blocking.

Options ***interface-name***—Name of a Gigabit Ethernet or 10-Gigabit Ethernet interface.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 57
- BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 59
- Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 60
- *show spanning-tree bridge*
- *show spanning-tree interface*
- *Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches*

interface (Layer 2 Protocol Tunneling)

Syntax

```
interface interface-name {
  enable-all-ifl
  protocol (cdp | stp | vtp | pvstp);
}
```

Hierarchy Level [edit protocols layer2-control mac-rewrite]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
enable-all-if statement added in Junos OS Release 13.3.
Support for PVSTP protocol introduced in Junos OS Release 13.3.

Description Configure an interface for Layer 2 protocol tunneling.

The remaining statement is explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 81

layer2-control

Syntax

```
layer2-control {
  bpdu-block {
    disable-timeout seconds;
    interface interface-name;
  }
  mac-rewrite {
    interface interface-name {
      enable-all-ifl
      protocol ( 802.1X |802.3AH | CDP | LACP | LLDP | MVRP | STP | VTP | GVRP | VSTP);
    }
  }
  nonstop-bridging;
  traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag <disable>;
  }
}
```

Hierarchy Level [edit protocols]

Release Information

Statement introduced in Junos OS Release 8.4.
bpdu-block statement added in Junos OS Release 9.4.
enable-all-if statement added in Junos OS Release 13.3.
Support for PVSTP protocol introduced in Junos OS Release 13.3.
Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Configure Layer 2 control protocols to enable features such as Layer 2 protocol tunneling or nonstop bridging.

NOTE: On EX4300 switches, the **mac-rewrite** statement does not support the 802.1X authentication protocol.

The remaining statements are explained separately.

NOTE: For a detailed description of configuring the **nonstop-bridging** statement, see the *Junos OS High Availability Library for Routing Devices*. When this statement is configured on routing platforms with two Routing Engines, a master Routing Engine switches over gracefully to a backup Routing Engine and preserves Layer 2 Control Protocol (L2CP) information.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 81
- Layer 2 Protocol Tunneling Configuration Guidelines on page 83
- Configuring Layer 2 Protocol Tunneling on page 84
- *instance-type*

mac-rewrite

Syntax

```
mac-rewrite {
  interface interface-name {
    enable-all-ifl
    protocol (802.1X | 802.3AH | CDP | LACP | LLDP | MVRP | STP | VTP | GVRP | VSTP);
    }
  }
}
```

Hierarchy Level [edit protocols layer2-control]

Release Information

Statement introduced in Junos OS Release 9.1.
Support for PVSTP introduced in Junos OS Release 13.3.
enable-all-if statement added in Junos OS Release 13.3.
Support for PVSTP protocol introduced in Junos OS Release 13.3.
Statement introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Enable rewriting of the MAC address for Layer 2 protocol tunneling. When a control packet for STP, CDP, VTP, or PVSTP is received on a service provider edge port configured for Layer 2 protocol tunneling, the multicast destination MAC address is rewritten with the predefined multicast tunnel MAC address of 01:00:0c:cd:cd:d0. The packet is transported across the provider network transparently to the other end of the tunnel and the original multicast destination MAC address is restored when the packet is transmitted.

NOTE: On EX4300 switches, the **mac-rewrite** statement does not support the 802.1X authentication protocol.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 81

protocol

Syntax protocol (cdp | stp | vtp | pvstp);

Hierarchy Level [edit protocols layer2-control mac-rewrite interface *interface-name*]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 13.2 for QFX series.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for PVSTP introduced in Junos OS Release 13.3.

Description Configure the protocol to be tunneled on an interface for Layer 2 protocol tunneling. To tunnel multiple protocols, include multiple **protocol** statements.

Options

cdp—Tunnel the Cisco discovery protocol.

stp—Tunnel all versions of the spanning-tree protocol.

vtp—Tunnel the VLAN trunk protocol.

pvstp—Tunnel the Per-VLAN Spanning Tree Plus (PVST+) protocol

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 81
- Layer 2 Protocol Tunneling Configuration Guidelines on page 83
- Configuring Layer 2 Protocol Tunneling on page 84

CHAPTER 8

Operational Mode Commands for Spanning-Tree Configuration

- clear spanning-tree protocol-migration
- clear spanning-tree statistics bridge
- clear spanning-tree stp-buffer
- show spanning-tree bridge
- show spanning-tree interface
- show spanning-tree mstp configuration
- show spanning-tree statistics
- show spanning-tree statistics bridge
- show spanning-tree statistics interface
- show spanning-tree statistics message-queues
- show spanning-tree stp-buffer see-all
- clear error bpdu interface
- clear error mac-rewrite
- show bridge mac-table
- show mac-rewrite interface

clear spanning-tree protocol-migration

Syntax clear spanning-tree protocol-migration
<interface *interface-name*>
<routing-instance *routing-instance-name*>

Release Information Command introduced in Junos OS Release 9.0.

Description Revert from the original IEEE 802.1D Spanning Tree Protocol (STP) back to the Rapid Spanning Tree Protocol after the **force-version** statement has been removed from the configuration.

Options **none**—Reset the STP protocol for all interfaces and all routing instances.

interface *interface-name*—(Optional) Reset the STP protocol for the specified interface only.

routing-instance *routing-instance-name*—(Optional) Reset the STP protocol for a particular routing instance.

Additional Information For information about the **force-version** statement, see the *Junos Routing Protocols Configuration Guide*.

Required Privilege Level clear

Sample Output

clear spanning-tree protocol-migration

```
user@host> clear spanning-tree protocol-migration
```

clear spanning-tree statistics bridge

Syntax clear spanning-tree statistics bridge

Release Information Command introduced in Junos OS Release 14.1.

Description Clear the statistics of the bridge.

Required Privilege Level clear

List of Sample Output clear spanning-tree statistics bridge (MX Series) on page 137

Sample Output

clear spanning-tree statistics bridge (MX Series)

```
user@host> clear spanning-tree statistics bridge
```

clear spanning-tree stp-buffer

Syntax clear spanning-tree stp-buffer

Release Information Command introduced in Junos OS Release 14.1.

Description Clear the stp-buffer.

Required Privilege Level clear

List of Sample Output clear spanning-tree stp-buffer (MX Series) on page 138

Sample Output

clear spanning-tree stp-buffer (MX Series)

```
user@host> clear spanning-tree stp-buffer
```


show spanning-tree bridge

List of Syntax
Syntax on page 139
Syntax (QFX Series) on page 139

Syntax
show spanning-tree bridge
<brief | detail>
<msti *msti-id*>
<routing-instance *routing-instance-name*>
<vlan-id *vlan-id*>

Syntax (QFX Series)
show spanning-tree bridge
<brief | detail>
<msti *msti-id*>
<vlan-id *vlan-id*>

Release Information
Command introduced in Junos OS Release 8.4.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display the configured or calculated Spanning Tree Protocol (STP) parameters.

Options
none—(Optional) Display brief STP bridge information for all multiple spanning-tree instances (MSTIs).

brief | detail—(Optional) Display the specified level of output.

msti *msti-id*—(Optional) Display STP bridge information for the specified MSTI.

routing-instance *routing-instance-name*—(Optional) Display STP bridge information for the specified routing instance.

vlan-id *vlan-id*—(Optional) Display STP bridge information for the specified VLAN.

Required Privilege Level
view

List of Sample Output
show spanning-tree bridge routing-instance on page 140
show spanning-tree bridge msti on page 141
show spanning-tree bridge vlan-id (MSTP) on page 142
show spanning-tree bridge (RSTP) on page 142
show spanning-tree bridge vlan-id (RSTP) on page 143

Output Fields
Table 6 on page 139 lists the output fields for the **show spanning-tree bridge** command. Output fields are listed in the approximate order in which they appear.

Table 6: show spanning-tree bridge Output Fields

Field Name	Field Description
Routing instance name	Name of the routing instance under which the bridge is configured.
Enabled protocol	Spanning Tree Protocol type enabled.

Table 6: show spanning-tree bridge Output Fields *(continued)*

Field Name	Field Description
Root ID	Bridge ID of the elected spanning-tree root bridge. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.
Root cost	Calculated cost to reach the root bridge from the bridge where the command is entered.
Root port	Interface that is the current elected root port for this bridge.
CIST regional root	Bridge ID of the elected MSTP regional root bridge.
CIST internal root cost	Calculated cost to reach the regional root bridge from the bridge where the command is entered.
Hello time	Configured number of seconds between transmissions of configuration BPDUs.
Maximum age	Configured maximum expected arrival time of hello bridge protocol data units (BPDUs).
Forward delay	How long an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hop count	Configured maximum number of hops a BPDU can be forwarded in the MSTP region.
Message age	Number of elapsed seconds since the most recent BPDU was received.
Number of topology changes	Total number of STP topology changes detected since the routing device last booted.
Time since last topology change	Number of elapsed seconds since the most recent topology change.
Bridge ID (Local)	Locally configured bridge ID. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.
Extended system ID	System identifier.
MSTI regional root	Bridge ID of the elected MSTP regional root bridge.

Sample Output

show spanning-tree bridge routing-instance

```
user@host> show spanning-tree bridge routing-instance vs1 detail
STP bridge parameters
Routing instance name              : vs1
Enabled protocol                   : MSTP
```

```
STP bridge parameters for CIST
  Root ID                              : 32768.00:13:c3:9e:c8:80
  Root cost                            : 0
  Root port                            : ge-10/2/0
  CIST regional root                   : 32768.00:13:c3:9e:c8:80
  CIST internal root cost              : 22000
  Hello time                           : 2 seconds
  Maximum age                          : 20 seconds
  Forward delay                        : 15 seconds
  Hop count                            : 18
  Message age                          : 0
  Number of topology changes           : 1
  Time since last topology change      : 1191 seconds
  Local parameters
    Bridge ID                          : 32768.00:90:69:0b:7f:d1
    Extended system ID                 : 1

STP bridge parameters for MSTI 1
  MSTI regional root                   : 32769.00:13:c3:9e:c8:80
  Root cost                            : 22000
  Root port                            : ge-10/2/0
  Hello time                           : 2 seconds
  Maximum age                          : 20 seconds
  Forward delay                        : 15 seconds
  Hop count                            : 18
  Number of topology changes           : 1
  Time since last topology change      : 1191 seconds
  Local parameters
    Bridge ID                          : 32769.00:90:69:0b:7f:d1
    Extended system ID                 : 1

STP bridge parameters for MSTI 2
  MSTI regional root                   : 32770.00:13:c3:9e:c8:80
  Root cost                            : 22000
  Root port                            : ge-10/2/0
  Hello time                           : 2 seconds
  Maximum age                          : 20 seconds
  Forward delay                        : 15 seconds
  Hop count                            : 18
  Number of topology changes           : 1
  Time since last topology change      : 1191 seconds
  Local parameters
    Bridge ID                          : 32770.00:90:69:0b:7f:d1
    Extended system ID                 : 1
```

show spanning-tree bridge msti

```
user@host> show spanning-tree bridge msti 1 routing-instance vs1 detail
STP bridge parameters
Routing instance name                  : vs1
Enabled protocol                       : MSTP

STP bridge parameters for MSTI 1
  MSTI regional root                   : 32769.00:13:c3:9e:c8:80
  Root cost                            : 22000
  Root port                            : xe-10/2/0
  Hello time                           : 2 seconds
  Maximum age                          : 20 seconds
  Forward delay                        : 15 seconds
  Hop count                            : 18
```

```
  Number of topology changes        : 1
  Time since last topology change   : 1191 seconds
  Local parameters
    Bridge ID                       : 32769.00:90:69:0b:7f:d1
    Extended system ID              : 1
```

show spanning-tree bridge vlan-id (MSTP)

```
user@host> show spanning-tree bridge vlan-id 1101 routing-instance vs1 detail
STP bridge parameters
Routing instance name               : vs1
Enabled protocol                    : MSTP

STP bridge parameters for CIST
  Root ID                           : 32768.00:13:c3:9e:c8:80
  Root cost                         : 0
  Root port                         : xe-10/2/0
  CIST regional root                : 32768.00:13:c3:9e:c8:80
  CIST internal root cost           : 22000
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Hop count                         : 18
  Message age                       : 0
  Number of topology changes        : 0
  Local parameters
    Bridge ID                       : 32768.00:90:69:0b:7f:d1
    Extended system ID              : 1
    Hello time                      : 2 seconds
    Maximum age                     : 20 seconds
    Forward delay                   : 15 seconds
    Path cost method                : 32 bit
    Maximum hop count               : 20
```

show spanning-tree bridge (RSTP)

```
user@host> show spanning-tree bridge
STP bridge parameters
Routing instance name               : GLOBAL
Enabled protocol                    : RSTP
  Root ID                           : 28672.00:90:69:0b:3f:d0
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Message age                       : 0
  Number of topology changes        : 58
  Time since last topology change   : 14127 seconds
  Local parameters
    Bridge ID                       : 28672.00:90:69:0b:3f:d0
    Extended system ID              : 0

 STP bridge parameters for bridge VLAN 10
   Root ID                          : 28672.00:90:69:0b:3f:d0
   Hello time                       : 2 seconds
   Maximum age                      : 20 seconds
   Forward delay                    : 15 seconds
   Message age                      : 0
   Number of topology changes       : 58
   Time since last topology change  : 14127 seconds
   Local parameters
     Bridge ID                      : 28672.00:90:69:0b:3f:d0
```

```
    Extended system ID            : 0

 STP bridge parameters for bridge VLAN 20
   Root ID                         : 28672.00:90:69:0b:3f:d0
   Hello time                      : 2 seconds
   Maximum age                     : 20 seconds
   Forward delay                   : 15 seconds
   Message age                     : 0
   Number of topology changes      : 58
   Time since last topology change : 14127 seconds
   Local parameters
     Bridge ID                     : 28672.00:90:69:0b:3f:d0
     Extended system ID            : 0
```

show spanning-tree bridge vlan-id (RSTP)

```
user@host> show spanning-tree bridge vlan-id 10
STP bridge parameters
Routing instance name               : GLOBAL
Enabled protocol                    : RSTP

 STP bridge parameters for VLAN 10
   Root ID                         : 28672.00:90:69:0b:3f:d0
   Hello time                      : 2 seconds
   Maximum age                     : 20 seconds
   Forward delay                   : 15 seconds
   Message age                     : 0
   Number of topology changes      : 58
   Time since last topology change : 14127 seconds
   Local parameters
     Bridge ID                     : 28672.00:90:69:0b:3f:d0
     Extended system ID            : 0
```

show spanning-tree interface

List of Syntax
Syntax on page 144
Syntax (EX Series Switches and the QFX Series) on page 144

Syntax
show spanning-tree interface
<brief | detail>
<msti *msti-id*>
<routing-instance *routing-instance-name*>
<vlan-id *vlan-id*>

Syntax (EX Series Switches and the QFX Series)
show spanning-tree interface
<brief | detail>
<msti *msti-id*>
<vlan-id *vlan-id*>

Release Information
Command introduced in Junos OS Release 8.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display the configured or calculated interface-level STP parameters.

Options
none—Display brief STP interface information.

brief | detail—(Optional) Display the specified level of output.

msti *msti-id*—(Optional) Display STP interface information for the specified MST instance.

routing-instance *routing-instance-name*—(Optional) Display STP interface information for the specified routing instance.

vlan-id *vlan-id*—(Optional) Display STP interface information for the specified VLAN.

Required Privilege Level
view

List of Sample Output
show spanning-tree interface on page 145
show spanning-tree interface (QFX Series) on page 146
show spanning-tree interface detail on page 146
show spanning-tree interface msti on page 148
show spanning-tree interface vlan-id on page 148
show spanning-tree interface (VSTP) on page 149
show spanning-tree interface vlan-id (VSTP) on page 149

Output Fields
Table 7 on page 144 lists the output fields for the **show spanning-tree interface** command. Output fields are listed in the approximate order in which they appear.

Table 7: show spanning-tree Interface Output Fields

Field Name	Field Description
Interface name	Interface configured to participate in the STP, RSTP, VSTP, or MSTP instance.

Table 7: show spanning-tree Interface Output Fields *(continued)*

Field Name	Field Description
Port ID	Logical interface identifier configured to participate in the MSTP or VSTP instance.
Designated port ID	Port ID of the designated port for the LAN segment to which this interface is attached.
Designated bridge ID	Bridge ID of the designated bridge for the LAN segment to which this interface is attached.
Port Cost	Configured cost for the interface.
Port State	STP port state: forwarding (**FWD**), blocking (**BLK**), listening, learning, or disabled.
Port Role	MSTP, VSTP, or RSTP port role: designated (**DESG**), backup (**BKUP**), alternate (**ALT**), (**ROOT**), or Root Prevented (**Root-Prev**).
Link type	MSTP, VSTP, or RSTP link type. Shared or point-to-point (pt-pt) and edge or nonedge.
Alternate	Identifies the interface as an MSTP, VSTP, or RSTP alternate root port (**Yes**) or nonalternate root port (**No**).
Boundary Port	Identifies the interface as an MSTP regional boundary port (**Yes**) or nonboundary port (**No**).

Sample Output

show spanning-tree interface

```
user@host> show spanning-tree interface routing-instance vs1 detail
Spanning tree interface parameters for instance 0

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID       bridge ID          Cost
ae1             128:1        128:1  32768.0090690b47d1      1000  FWD    DESG
ge-2/1/2        128:2        128:2  32768.0090690b47d1     20000  FWD    DESG
ge-2/1/5        128:3        128:3  32768.0090690b47d1     29999  FWD    DESG
ge-2/2/1        128:4       128:26  32768.0013c39ec880     20000  FWD    ROOT
xe-9/2/0        128:5        128:5  32768.0090690b47d1      2000  FWD    DESG
xe-9/3/0        128:6        128:6  32768.0090690b47d1      2000  FWD    DESG

Spanning tree interface parameters for instance 1

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID       bridge ID          Cost
ae1             128:1        128:1  32769.0090690b47d1      1000  FWD    DESG
ge-2/1/2        128:2        128:2  32769.0090690b47d1     20000  FWD    DESG
ge-2/1/5        128:3        128:3  32769.0090690b47d1     29999  FWD    DESG
ge-2/2/1        128:4       128:26  32769.0013c39ec880     20000  FWD    ROOT
xe-9/2/0        128:5        128:5  32769.0090690b47d1      2000  FWD    DESG
xe-9/3/0        128:6        128:6  32769.0090690b47d1      2000  FWD    DESG
```

```
Spanning tree interface parameters for instance 2

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID        bridge ID          Cost
ae1              128:1        128:1  32770.0090690b47d1      1000  FWD    DESG
ge-2/1/2         128:2        128:2  32770.0090690b47d1     20000  FWD    DESG
ge-2/1/5         128:3        128:3  32770.0090690b47d1     29999  FWD    DESG
ge-2/2/1         128:4       128:26  32770.0013c39ec880     20000  FWD    ROOT
xe-9/2/0         128:5        128:5  32770.0090690b47d1      2000  FWD    DESG
xe-9/3/0         128:6        128:6  32770.0090690b47d1      2000  FWD    DESG
```

show spanning-tree interface (QFX Series)

```
user@host> show spanning-tree interface routing-instance vs1 detail
Spanning tree interface parameters for instance 0

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID        bridge ID          Cost
ae1              128:1        128:1  32768.0090690b47d1      1000  FWD    DESG
ge-2/1/2         128:2        128:2  32768.0090690b47d1     20000  FWD    DESG
ge-2/1/5         128:3        128:3  32768.0090690b47d1     29999  FWD    DESG
ge-2/2/1         128:4       128:26  32768.0013c39ec880     20000  FWD    ROOT
xe-9/2/0         128:5        128:5  32768.0090690b47d1      2000  FWD    DESG
xe-9/3/0         128:6        128:6  32768.0090690b47d1      2000  FWD    DESG

Spanning tree interface parameters for instance 1

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID        bridge ID          Cost
ae1              128:1        128:1  32769.0090690b47d1      1000  FWD    DESG
ge-2/1/2         128:2        128:2  32769.0090690b47d1     20000  FWD    DESG
ge-2/1/5         128:3        128:3  32769.0090690b47d1     29999  FWD    DESG
ge-2/2/1         128:4       128:26  32769.0013c39ec880     20000  FWD    ROOT
xe-9/2/0    128:5        128:5  32769.0090690b47d1      2000  FWD    DESG
xe-9/3/0    128:6        128:6  32769.0090690b47d1      2000  FWD    DESG

Spanning tree interface parameters for instance 2

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID        bridge ID          Cost
ae1              128:1        128:1  32770.0090690b47d1      1000  FWD    DESG
ge-2/1/2         128:2        128:2  32770.0090690b47d1     20000  FWD    DESG
ge-2/1/5         128:3        128:3  32770.0090690b47d1     29999  FWD    DESG
ge-2/2/1         128:4       128:26  32770.0013c39ec880     20000  FWD    ROOT
xe-9/2/0    128:5        128:5  32770.0090690b47d1      2000  FWD    DESG
xe-9/3/0    128:6        128:6  32770.0090690b47d1      2000  FWD    DESG
```

show spanning-tree interface detail

```
user@host> show spanning-tree interface routing-instance vs1 detail
Spanning tree interface parameters for instance 0

Interface name                : ae1
Port identifier               : 128.1
Designated port ID            : 128.1
Port cost                     : 1000
Port state                    : Forwarding
Designated bridge ID          : 32768.00:90:69:0b:47:d1
Port role                     : Designated
Link type                     : Pt-Pt/NONEDGE
```

```
Boundary port                   : No

Interface name                 : ge-2/1/2
Port identifier                : 128.2
Designated port ID             : 128.2
Port cost                      : 20000
Port state                     : Forwarding
Designated bridge ID           : 32768.00:90:69:0b:47:d1
Port role                      : Designated
Link type                      : Pt-Pt/NONEDGE
Boundary port                   : No

Interface name                 : ge-2/1/5
Port identifier                : 128.3
Designated port ID             : 128.3
Port cost                      : 29999
Port state                     : Forwarding
Designated bridge ID           : 32768.00:90:69:0b:47:d1
Port role                      : Designated
Link type                      : Pt-Pt/NONEDGE
Boundary port                   : No

Interface name                 : ge-2/2/1
Port identifier                : 128.4
Designated port ID             : 128.26
Port cost                      : 20000
Port state                     : Forwarding
Designated bridge ID           : 32768.00:13:c3:9e:c8:80
Port role                      : Root
Link type                      : Pt-Pt/NONEDGE
Boundary port                   : No

Interface name                 : xe-9/2/0
Port identifier                : 128.5
Designated port ID             : 128.5
Port cost                      : 2000
Port state                     : Forwarding
Designated bridge ID           : 32768.00:90:69:0b:47:d1
Port role                      : Designated
Link type                      : Pt-Pt/NONEDGE
Boundary port                   : No

Interface name                 : xe-9/3/0
Port identifier                : 128.6
Designated port ID             : 128.6
Port cost                      : 2000
Port state                     : Forwarding
Designated bridge ID           : 32768.00:90:69:0b:47:d1
Port role                      : Designated
Link type                      : Pt-Pt/NONEDGE
Boundary port                   : No


Spanning tree interface parameters for instance 1

Interface name                 : ae1
Port identifier                : 128.1
Designated port ID             : 128.1
Port cost                      : 1000
Port state                     : Forwarding
Designated bridge ID           : 32768.00:90:69:0b:47:d1
```

```
Port role                       : Designated
Link type                       : Pt-Pt/NONEDGE
Boundary port                    : No

Interface name                  : ge-2/1/2
Port identifier                 : 128.2
Designated port ID              : 128.2
Port cost                       : 20000
Port state                      : Forwarding
Designated bridge ID            : 32768.00:90:69:0b:47:d1
Port role                       : Designated
Link type                       : Pt-Pt/NONEDGE
Boundary port                    : No

Interface name                  : ge-2/1/5
Port identifier                 : 128.3
Designated port ID              : 128.3
Port cost                       : 29999
Port state                      : Forwarding
Designated bridge ID            : 32768.00:90:69:0b:47:d1
Port role                       : Designated
Link type                       : Pt-Pt/NONEDGE
Boundary port                    : No

Interface name                  : ge-2/2/1
Port identifier                 : 128.4
Designated port ID              : 128.26
Port cost                       : 20000
Port state                      : Forwarding
Designated bridge ID            : 32768.00:13:c3:9e:c8:80
Port role                       : Root
Link type                       : Pt-Pt/NONEDGE
Boundary port                    : No

...
```

show spanning-tree interface msti

```
user@host> show spanning-tree interface msti 1 routing-instance vs1 detail
 Spanning tree interface parameters for instance 1

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID        bridge ID          Cost
xe-7/0/0         128:1         128:1  32769.0090690b4fd1      2000  FWD    DESG
ge-5/1/0         128:2         128:2  32769.0090690b4fd1     20000  FWD    DESG
ge-5/1/1         128:3         128:3  32769.0090690b4fd1     20000  FWD    DESG
ae1              128:4         128:1  32769.0090690b47d1     10000  BLK    ALT
ge-5/1/4         128:5         128:3  32769.0090690b47d1     20000  BLK    ALT
xe-7/2/0         128:6         128:6  32769.0090690b47d1      2000  FWD    ROOT
```

show spanning-tree interface vlan-id

```
user@host> show spanning-tree interface vlan-id 101 routing-instance vs1 detail
Spanning tree interface parameters for instance 0

Interface    Port ID    Designated      Designated         Port    State  Role
                         port ID        bridge ID          Cost
ge-11/0/5        128:1         128:1  32768.0090690b7fd1     20000  FWD    DESG
ge-11/0/6        128:2         128:1  32768.0090690b7fd1     20000  BLK    BKUP
ge-11/1/0        128:3         128:2  32768.0090690b4fd1     20000  BLK    ALT
ge-11/1/1        128:4         128:3  32768.0090690b4fd1     20000  BLK    ALT
```

```
ge-11/1/4        128:5        128:1  32768.0090690b47d1     20000  BLK    ALT
xe-10/0/0        128:6        128:5  32768.0090690b4fd1      2000  BLK    ALT
xe-10/2/0        128:7        128:4  32768.0090690b47d1      2000  FWD    ROOT
```

show spanning-tree interface (VSTP)

```
user@host> show spanning-tree interface
Spanning tree interface parameters for instance 0

Interface    Port ID    Designated      Designated         Cost    State  Role
                         port ID        bridge ID
ge-1/0/1         128:1        128:1  28672.0090690b3fe0     20000  FWD    DESG
ge-1/0/2         128:2        128:2  28672.0090690b3fe0     20000  FWD    DESG

Spanning tree interface parameters for VLAN 10

Interface    Port ID    Designated      Designated         Cost    State  Role
                         port ID        bridge ID
ge-1/0/1         128:1        128:1  28672.0090690b3fe0     20000  FWD    DESG
ge-1/0/2         128:2        128:2  28672.0090690b3fe0     20000  FWD    DESG

Spanning tree interface parameters for VLAN 20

Interface    Port ID    Designated      Designated         Cost    State  Role
                         port ID        bridge ID
ge-1/0/1         128:1        128:1  28672.0090690b3fe0     20000  FWD    DESG
ge-1/0/2         128:2        128:2  28672.0090690b3fe0     20000  FWD    DESG
```

show spanning-tree interface vlan-id (VSTP)

```
user@host> show spanning-tree interface vlan-id 10
Spanning tree interface parameters for VLAN 10

Interface    Port ID    Designated      Designated         Cost    State  Role
                         port ID        bridge ID
ge-1/0/1         128:1        128:1  28672.0090690b3fe0     20000  FWD    DESG
ge-1/0/2         128:2        128:2  28672.0090690b3fe0     20000  FWD    DESG
```

show spanning-tree mstp configuration

List of Syntax
Syntax on page 150
Syntax (EX Series Switch and the QFX Series) on page 150

Syntax
show spanning-tree mstp configuration
<brief | detail>
<routing-instance *routing-instance-name*>

Syntax (EX Series Switch and the QFX Series)
show spanning-tree mstp configuration
<brief | detail>

Release Information
Command introduced in Junos OS Release 8.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display the MSTP configuration.

Options
none—Display MSTP configuration information.

brief | detail—(Optional) Display the specified level of output.

routing-instance *routing-instance-name*—(Optional) Display MSTP configuration information for the specified routing instance.

Required Privilege Level
view

List of Sample Output
show spanning-tree mstp configuration detail on page 151
show spanning-tree mstp configuration detail (QFX Series) on page 151

Output Fields
Table 8 on page 150 lists the output fields for the **show spanning-tree mstp configuration** command. Output fields are listed in the approximate order in which they appear.

Table 8: show spanning-tree mstp configuration Output Fields

Field Name	Field Description
Context id	Internally generated identifier.
Region name	MSTP region name carried in the MSTP BPDUs.
Revision	Revision number of the MSTP configuration.
Configuration digest	Numerical value derived from the VLAN-to-instance mapping table.
MSTI	MST instance identifier.
Member VLANs	VLAN identifiers associated with the MSTI.

Sample Output

show spanning-tree mstp configuration detail

```
user@host> show spanning-tree mstp configuration routing-instance vs1 detail
MSTP configuration information
Context identifier     : 1
Region name            : henry
Revision               : 3
Configuration digest   : 0x6da4b5c4fd587757eef35675365e1


MSTI     Member VLANs
   0 0-99,101-199,201-4094
   1 100
   2 200
```

show spanning-tree mstp configuration detail (QFX Series)

```
user@lf0> show spanning-tree mstp configuration routing-instance vs1 detail
MSTP configuration information
Context identifier     : 1
Region name            : henry
Revision               : 3
Configuration digest   : 0x6da4b5c4fd587757eef35675365e1


MSTI     Member VLANs
   0 0-99,101-199,201-4094
   1 100
   2 200
```

show spanning-tree statistics

List of Syntax
Syntax on page 152
Syntax (EX Series Switch and the QFX Series) on page 152

Syntax
show spanning-tree statistics
<brief | detail>
<interface *interface-name*>
<routing-instance *routing-instance-name*>

Syntax (EX Series Switch and the QFX Series)
show spanning-tree statistics
<brief | detail>
<interface *interface-name* | vlan *vlan-id*>

Release Information
Command introduced in Junos OS Release 8.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for QFX Series switches.

Description
Display STP statistics.

Options
none—Display brief STP statistics.

brief | detail—(Optional) Display the specified level of output.

interface *interface-name*—(Optional) Display STP statistics for the specified interface.

routing-instance *routing-instance-name*—(Optional) Display STP statistics for the specified routing instance.

Required Privilege Level
view

List of Sample Output
show spanning-tree statistics routing-instance on page 153
show spanning-tree statistics interface routing-instance detail on page 153

Output Fields
Table 9 on page 152 lists the output fields for the **show spanning-tree statistics** command. Output fields are listed in the approximate order in which they appear.

Table 9: show spanning-tree statistics Output Fields

Field Name	Field Description
Message type	Type of message being counted.
BPDUs sent	Total number of BPDUs sent.
BPDUs received	Total number of BPDUs received.
BPDUs sent in last interval	Number of BPDUs sent within a specified interval.
BPDUs received in last interval	Number of BPDUs received within a specified interval.

Table 9: show spanning-tree statistics Output Fields *(continued)*

Field Name	Field Description
Interface	Interface for which the statistics are being displayed.
Next BPDU transmission	Number of seconds until the next BPDU is scheduled to be sent.

Sample Output

show spanning-tree statistics routing-instance

```
user@host> show spanning-tree statistics routing-instance vs1 detail
Routing instance level STP statistics
Message type                    : bpdus
BPDUs sent                      : 1396
BPDUs received                  : 1027
BPDUs sent in last interval     : 5         (duration: 4 sec)
BPDUs received in last interval: 4          (duration: 4 sec)
```

show spanning-tree statistics interface routing-instance detail

```
user@host> show spanning-tree statistics interface ge-11/1/4 routing-instance vs1 detail
Interface   BPDUs sent   BPDUs received      Next BPDU
                                            transmission
ge-11/1/4            7           190                0
```

show spanning-tree statistics bridge

Syntax show spanning-tree statistics bridge

Release Information Command introduced in Junos OS Release 14.1.

Description Display the STP statistics of the bridge.

Required Privilege Level view

List of Sample Output show spanning-tree statistics bridge (MX Series) on page 154

Output Fields Table 10 on page 154 describes the output fields for the **show spanning-tree statistics bridge** command. Output fields are listed in the approximate order in which they appear.

Table 10: show spanning-tree statistics bridge Output Fields

Field Name	Field Description
STP Context	Context of STP instances saved for each routing instance. All STP instances in the same routing instances have same context.
STP Instance	Instance number that uniquely identifies each STP session per routing instance.
Number of Root Bridge Changes	Counts the number of Root Bridge change events.
Number of Root Port Changes	Counts the number of Root Port change events.
Recent TC Received	Details about the last topology change received.

Sample Output

show spanning-tree statistics bridge (MX Series)

```
user@host> show spanning-tree statistics bridge
STP Context  : default
STP Instance : 0
Number of Root Bridge Changes: 1           Last Changed: Wed Oct 23 07:10:05
2013
Number of Root Port Changes:   2           Last Changed: Wed Oct 23 07:10:05
2013
Recent TC  Received:  ge-3/1/4.32767       Received    : Wed Oct 23 07:10:07
2013
```

show spanning-tree statistics interface

Syntax show spanning-tree statistics interface

Release Information Command introduced in Junos OS Release 14.1.

Description Display the STP statistics related to the interface.

Required Privilege Level view

List of Sample Output show spanning-tree statistics interface (MX Series) on page 155

Output Fields Table 11 on page 155 describes the output fields for the **show spanning-tree statistics interface** command. Output fields are listed in the approximate order in which they appear.

Table 11: show spanning-tree statistics interface Output Fields

Field Name	Field Description
Interface	Interface name.
BPDUs sent	Total number of BPDUs sent from the bridge on the interface.
BPDUs received	Total number of BPDUs received by the bridge on the interface.
Next BPDU Transmission	Time after which the next BPDU is sent by the bridge on the interface.
TC Tx/Rx	Total number of Topology Change BPDUs sent or received on the interface.
Proposal Tx/Rx	Total number of Proposal BPDUs sent or received on the interface.
Agreement Tx/Rx	Total number of Agreement BPDUs sent or received on the interface.

Sample Output

show spanning-tree statistics interface (MX Series)

```
user@host> show spanning-tree statistics interface

Interface BPDUs   BPDUs     Next BPDU     TCs     Proposal  Agreement
          Sent    Received  Transmission  Tx/Rx   Tx/Rx     Tx/Rx
xe-0/0/0   49       3            1        5/2      0/2       1/0

ge-1/0/0   48       1            1        5/1      0/1       1/1
```

show spanning-tree statistics message-queues

Syntax show spanning-tree statistics message-queues

Release Information Command introduced in Junos OS Release 14.1.

Description Display the STP message queues-related statistics.

Required Privilege Level view

List of Sample Output show spanning-tree statistics message-queues (MX Series) on page 156

Output Fields Table 12 on page 156 describes the output fields for the **show spanning-tree statistics message-queues** command. Output fields are listed in the approximate order in which they appear.

Table 12: show spanning-tree statistics message-queues Output Fields

Field Name	Field Description
Queue	PPMD name.
Current size	Number of packets currently present in the queue.
High-watermark	Maximum number of packets present in the queue at any time.
max/avg wait time	Maximum or average time packet waiting to be consumed.

Sample Output

show spanning-tree statistics message-queues (MX Series)

```
user@host> show spanning-tree statistics message-queues

Queue          Current size          High-watermark       max/avg wait time
PPMD-TX          15                        142             17636884/17636884
PPMD-RX          18                        83              18866272/18866272
```

show spanning-tree stp-buffer see-all

Syntax show spanning-tree stp-buffer see-all
<**stp-instance** *stp-instance-id* **routing-instance** *instance-name*>
<**vlan** *vlan-id* **routing-instance** *instance-name*>

Release Information Command introduced in Junos OS Release 14.1.

Description Display the configured STP (RSTP, MSTP, VSTP) interface parameters.

Options **none**— Display STP (RSTP, MSTP, VSTP) interface role/state changes that are logged into internal memory called the buffer. Entries in the buffer depend on the user configuration.

stp-instance ***stp-instance-id*** **routing-instance** ***instance-name***— (Optional) Display the STP buffer for the specified stp-instance and routing instance.

vlan ***vlan-id*** **routing-instance** ***instance-name***— (Optional) Display the STP buffer for the specified vlan id and routing instance.

Required Privilege Level view

List of Sample Output
show spanning-tree stp-buffer see-all (MX Series) on page 158
show spanning-tree stp-buffer see-all stp-instance stp-instance-id routing-instance instance-name (MX Series) on page 159
show spanning-tree stp buffer see-all vlan vlan-id routing-instance instance-name (MX Series) on page 160

Output Fields Table 13 on page 157 describes the output fields for the **show spanning-tree stp-buffer see-all** command. Output fields are listed in the approximate order in which they appear.

Table 13: show spanning-tree stp-buffer see-all Output Fields

Field Name	Field Description	Level of Output
Global Events	Displays events when PPMD RX/TX queues reach 70 % of their maximum queue size. The following indicates received queue status: • GT — Greater than 70 % of their maximum queue size. • LT — Less than 70 % of their maximum queue size.	none, **stp-instance**, **vlan**
Per STP instance Information	Information about every STP instance.	none, **stp-instance**, **vlan**
Routing Inst	Routing instance to which the STP instance belongs.	none, **stp-instance**, **vlan**
STP Instance	Instance number that uniquely identifies each STP session per routing-instance.	none, **stp-instance**

Table 13: show spanning-tree stp-buffer see-all Output Fields *(continued)*

Field Name	Field Description	Level of Output
Root Bridge	Bridge priority and bridge ID of ROOT bridge in the topology.	none, **vlan**
Root Port	Information about ROOT port, if any, on the local bridge at the displayed timestamp.	none, **vlan**
TC Received	Time at which topology change was received and on which port.	none, **stp-instance**, **vlan**
TC Generated	Time at which topology change occurred and on which port.	none, **stp-instance**, **vlan**
Port	The interface where the event is occurring.	none, **stp-instance**, **vlan**
State	STP state of the port. The following are the types of state: • Forwarding — Port forwards the traffic and is included in active topology and learns MAC addresses. • Blocking — Port does not forward traffic and is not included in active topology. Does not learn MAC addresses.	none, **vlan**
Role	Role of the port. The following are the types of ports: • Root — Port closest to the Root bridge. • Designated — Port sends the best BPDU on the connected segment. • Alternate — Port blocked for receiving more useful BPDUs from another bridge. • Disabled — Port is disabled. Cannot send or receive BPDUs.	none, **stp-instance**, **vlan**

Sample Output

show spanning-tree stp-buffer see-all (MX Series)

```
user@host> show spanning-tree stp-buffer see-all
1. Global Events:
Time at which different Queue's reached 70% of the Maximum Q-size
Mar 18 13:18:04 RCV_Q GT
Mar 18 13:18:57 RCV_Q LT
Mar 18 13:19:33 XMIT_Q GT

2. Per STP Instance Information :
Routing Inst    :  default
```

```
STP Instance  : 02
Root Bridge     : 12288.00:23:9c:f0:17:d0 Mar 18 13:18:04
STP Instance  : 03
Root Port        : ge-0/1/2 Mar 18 13:18:38
STP Instance  : 03
TC  Received  : ge-0/0/2 Mar 18 15:12:12
STP Instance  : 03
TC  Generated: ge-0/2/2 Mar 18 15:13:27

3. This section will print the time stamp for per Instance - port event changes.
STP Instance :  02
Port         :  ge-1/0/0 Mar 22 13:35:02
State        :  FWD  S
Role         :  DESG

STP Instance :  00
Port         :  ge-0/0/3 Mar 22 14:03:46
State        :  BLK
Role         :  ALT  R
STP Instance :  00
Port         :  ge-1/0/0 Mar 28 02:03:49
State        :  BLK  S
Role         :  ALT
```

show spanning-tree stp-buffer see-all stp-instance stp-instance-id routing-instance instance-name (MX Series)

```
user@host> show spanning-tree stp-buffer see-all stp-instance 0 routing-instance mstp_inst

1. Global Events:
Time at which different Queue's reached 70% of the Maximum Q-size
No Entry So far

2. Per STP Instance Information :

Routing Inst : mstp_inst



STP Instance : 0
TC Generated : ge-3/0/5.32767 Tue Dec 17 06:00:50 2013
STP Instance : 0
TC Generated : ge-3/1/1.32767 Tue Dec 17 06:00:50 2013
STP Instance : 0
TC  Received : ge-3/0/5.32767 Tue Dec 17 06:00:50 2013
STP Instance : 0
TC  Received : ge-3/0/5.32767 Tue Dec 17 06:00:50 2013
STP Instance : 0
TC  Received : ge-3/0/5.32767 Tue Dec 17 06:00:51 2013
STP Instance : 0
TC  Received : ge-3/0/5.32767 Tue Dec 17 06:00:53 2013

3.  This section will print the time stamp for per Instance, Port Event changes.


STP Instance : 0
Port         : ge-3/0/5.32767 Tue Dec 17 06:00:49 2013
State        : BLK S
Role         : DIS

STP Instance : 0
```

```
Port         : ge-3/0/5.32767 Tue Dec 17 06:00:49 2013
State        : BLK
Role         : DESG R

STP Instance : 0
Port         : ge-3/1/1.32767 Tue Dec 17 06:00:49 2013
State        : BLK S
Role         : DIS

STP Instance : 0
Port         : ge-3/1/1.32767 Tue Dec 17 06:00:49 2013
State        : BLK
Role         : DESG R

STP Instance : 0
Port         : ge-3/0/5.32767 Tue Dec 17 06:00:50 2013
State        : FWD S
Role         : DESG

STP Instance : 0
Port         : ge-3/1/1.32767 Tue Dec 17 06:00:50 2013
State        : FWD S
Role         : DESG
```

show spanning-tree stp buffer see-all vlan vlan-id routing-instance instance-name (MX Series)

```
user@host> show spanning-tree stp-buffer see-all vlan 10 routing-instance vstp_inst
1. Global Events:
Time at which different Queue's reached 70% of the Maximum Q-size
Mar 18 13:18:04 RCV_Q GT
Mar 18 13:18:57 RCV_Q LT
Mar 18 13:19:33 XMIT_Q GT

2. Per STP Instance Information :
Routing Inst    :  default
VLAN ID  : 02
Root Bridge     : 12288.00:23:9c:f0:17:d0 Mar 18 13:18:04
VLAN ID  : 03
Root Port        : ge-0/1/2 Mar 18 13:18:38
VLAN ID  : 03
TC  Received  : ge-0/0/2 Mar 18 15:12:12
VLAN ID  : 03
TC  Generated: ge-0/2/2 Mar 18 15:13:27

3. This section will print the time stamp for per Instance - port event changes.
VLAN ID :  02
Port         :  ge-1/0/0 Mar 22 13:35:02
State       :  FWD  S
Role        :  DESG

VLAN ID :  00
Port         :  ge-0/0/3 Mar 22 14:03:46
State       :  BLK
Role        :  ALT  R
VLAN ID :  00
Port         :  ge-1/0/0 Mar 28 02:03:49
State       :  BLK  S
Role        :  ALT
```

clear error bpdu interface

Syntax clear error bpdu interface *interface-name*

Release Information Command introduced in Junos OS Release 9.4.

Description Clear a bridge protocol data unit (BPDU) error condition caused by the detection of a possible bridging loop from Spanning Tree Protocol (STP) operation.

Required Privilege Level clear

Related Documentation

- Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 60
- Configuring BPDU Protection on All Edge Ports on page 61
- *Unblocking an Interface That Receives BPDUs in Error (CLI Procedure)*

List of Sample Output clear error bpdu interface on page 161

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear error bpdu interface

```
user@host> clear error bpdu interface ge-1/1/1
```

clear error mac-rewrite

Syntax clear error mac-rewrite
<interface *interface-name*>

Release Information Command introduced in Junos OS Release 9.1.

Description (MX Series routers only) Clear a MAC rewrite error condition caused by the reception of tunneled Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunk Protocol (VTP) packets on an interface with Layer 2 protocol tunneling enabled.

Options interface *interface-name*—(Optional) Clear the MAC rewrite error condition for the specified interface.

Required Privilege Level clear

List of Sample Output clear error mac-rewrite interface on page 162

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear error mac-rewrite interface

```
user@host> clear error mac-rewrite interface ge-1/0/1
```

show bridge mac-table

Syntax

show bridge mac-table
<age>
<brief | count | detail | extensive>
<bridge-domain (all | *bridge-domain-name*)>
<global-count>
<instance *instance-name*>
<interface *interface-name*>
<*mac-address*>
<instance *instance-name*>
<vlan-id (all-vlan | *vlan-id*)>

Release Information

Command introduced in Junos OS Release 8.4.
Command introduced in Junos OS Release 15.1
Support for PBB-EVPN instance added in Junos OS Release 16.1
MAC Flag P to indicate a MAC Pinned interface introduced in Junos OS 16.2

Description

(MX Series routers only) Display Layer 2 MAC address information.

Options

none—Display all learned Layer 2 MAC address information.

age— (Optional) Display age of a single mac-address.

brief | count | detail | extensive—(Optional) Display the specified level of output.

bridge-domain (all | *bridge-domain-name*)—(Optional) Display learned Layer 2 MAC addresses for all bridging domains or for the specified bridging domain.

global-count—(Optional) Display the total number of learned Layer 2 MAC addresses on the system.

instance *instance-name*—(Optional) Display learned Layer 2 MAC addresses for the specified routing instance.

interface *interface-name*—(Optional) Display learned Layer 2 MAC addresses for the specified interface.

mac-address—(Optional) Display the specified learned Layer 2 MAC address information.

vlan-id (all-vlan | *vlan-id*)—(Optional) Display learned Layer 2 MAC addresses for all VLANs or for the specified VLAN.

Additional Information

When Layer 2 protocol tunneling is enabled, the tunneling MAC address 01:00:0c:cd:cd:d0 is installed in the MAC table. When the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunk Protocol (VTP) is configured for Layer 2 protocol tunneling on an interface, the corresponding protocol MAC address is installed in the MAC table.

Required Privilege Level

view

List of Sample Output

show bridge mac-table on page 165

Output Fields Table 14 on page 164 describes the output fields for the **show bridge mac-table** command. Output fields are listed in the approximate order in which they appear.

Table 14: show bridge mac-table Output Fields

Field Name	Field Description
Age	Age of a single mac-address.
Routing instance	Name of the routing instance.
Bridging domain	Name of the bridging domain.
MAC address	MAC address or addresses learned on a logical interface.
MAC flags	Status of MAC address learning properties for each interface: • **S**—Static MAC address is configured. • **D**—Dynamic MAC address is configured. • **L**—Locally learned MAC address is configured. • **C**—Control MAC address is configured. • **SE**—MAC accounting is enabled. • **NM**—Non-configured MAC. • **R**—Remote PE MAC address is configured. • **P**—MAC Pinned interface is configured
Logical interface	Name of the logical interface.
MAC count	Number of MAC addresses learned on the specific routing instance or interface.
Learning interface	Name of the logical interface on which the MAC address was learned.
Learning VLAN	VLAN ID of the routing instance or bridge domain in which the MAC address was learned.
VXLAN ID/VXLAN	VXLAN Network Identifier (VNI).
Layer 2 flags	Debugging flags signifying that the MAC address is present in various lists.
Epoch	Spanning Tree Protocol epoch number identifying when the MAC address was learned. Used for debugging.

Table 14: show bridge mac-table Output Fields *(continued)*

Field Name	Field Description
Sequence number	Sequence number assigned to this MAC address. Used for debugging.
Learning mask	Mask of the Packet Forwarding Engines where this MAC address was learned. Used for debugging.
IPC generation	Creation time of the logical interface when this MAC address was learned. Used for debugging.

Sample Output

show bridge mac-table

```
user@host> show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
           SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : default-switch
 Bridging domain : test1, VLAN : 1
   MAC                 MAC      Logical          NH     RTR
   address             flags    interface        Index  ID
   01:00:0c:cc:cc:cc   S,NM     NULL
   01:00:0c:cc:cc:cd   S,NM     NULL
   01:00:0c:cd:cd:d0   S,NM     NULL
   64:87:88:6a:17:d0   D        ae0.1
   64:87:88:6a:17:f0   D        ae0.1
```

show bridge mac-table (with Layer 2 Services over GRE Interfaces)

```
user@host> show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned
           SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : default-switch
 Bridging domain : vlan-1, VLAN : 1
   MAC                 MAC      Logical
   address             flags    interface
   00:01:01:00:01:f7   D,SE     gr-1/2/10.0
   00:03:00:32:01:f7   D,SE     gr-1/2/10.0
   00:00:21:11:11:10   DL       ge-1/0/0.0
   00:00:21:11:11:11   DL       ge-1/1/0.0


Routing instance : default-switch
 Bridging domain : vlan-2, VLAN : 2
   MAC                 MAC      Logical
   address             flags    interface
   00:02:01:33:01:f7   D,SE     gr-1/2/10.1
   00:00:21:11:21:10   DL       ge-1/0/0.1
   00:00:21:11:21:11   DL       ge-1/1/0.1
```

show bridge mac-table (with VXLAN enabled)

```
user@host> show bridge mac-table
```

```
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned
           SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : default-switch
 Bridging domain : vlan-1, VLAN : 1
  VXLAN: Id : 100, Multicast group: 233.252.0.1
   MAC                 MAC      Logical
   address             flags    interface
   00:01:01:00:01:f7   D,SE     vtep.1052010
   00:03:00:32:01:f7   D,SE     vtep.1052011
   00:00:21:11:11:10   DL       ge-1/0/0.0
   00:00:21:11:11:11   DL       ge-1/1/0.0


Routing instance : default-switch
 Bridging domain : vlan-2, VLAN : 2, VXLAN : 200
  VXLAN: Id : 200, Multicast group: 233.252.0.2
   MAC                 MAC      Logical
   address             flags    interface
   00:02:01:33:01:f7   D,SE     vtep.1052010
   00:04:00:14:01:f7   D,SE     vtep.1052011
   00:00:21:11:21:10   DL       ge-1/0/0.1
   00:00:21:11:21:11   DL       ge-1/1/0.1
```

show bridge mac-table age (for GE interface)

```
user@host> show vpls mac-table age 00:02:03:aa:bb:1a instance vpls_instance_1
MAC Entry Age information
Current Age: 4 seconds
```

show bridge mac-table age (for AE interface)

```
user@host> show vpls mac-table age 00:02:03:aa:bb:1a instance vpls_instance_1
MAC Entry Age information
Current Age on FPC1: 102 seconds
Current Age on FPC2: 94 seconds
```

show bridge mac-table count

```
user@host> show bridge mac-table count
2 MAC address learned in routing instance vs1 bridge domain vlan100

  MAC address count per interface within routing instance:
    Logical interface        MAC count
    ge-11/0/3.0                     1
    ge-11/1/4.100                   0
    ge-11/1/1.100                   0
    ge-11/1/0.100                   0
    xe-10/2/0.100                   1
    xe-10/0/0.100                   0

  MAC address count per learn VLAN within routing instance:
    Learn VLAN ID            MAC count
                0                   2

0 MAC address learned in routing instance vs1 bridge domain vlan200

  MAC address count per interface within routing instance:
    Logical interface        MAC count
    ge-11/1/0.200                   0
    ge-11/1/1.200                   0
    ge-11/1/4.200                   0
```

```
    xe-10/0/0.200                   0
    xe-10/2/0.200                   0

  MAC address count per learn VLAN within routing instance:
    Learn VLAN ID            MAC count
                0                   0
```

show bridge mac-table detail

```
user@host> show bridge mac-table detail
MAC address: 00:00:00:19:1c:db
  Routing instance: vs1
   Bridging domain: vlan100
   Learning interface: ge-11/0/3.0     Learning VLAN: 0
   Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
   Epoch: 4                            Sequence number: 0
   Learning mask: 0x800                IPC generation: 0

MAC address: 00:00:00:59:3a:2f
  Routing instance: vs1
   Bridging domain: vlan100
   Learning interface: xe-10/2/0.100   Learning VLAN: 0
   Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
   Epoch: 7                            Sequence number: 0
   Learning mask: 0x400                IPC generation: 0
```

show bridge mac-table instance pbb-evpn

```
user@host> show bridge mac-table instance pbb-evpn
Routing instance : pbb-evpn
 Bridging domain : isid-bd10000, ISID : 10000
   MAC                    MAC      Logical          NH     RTR
   address               flags      interface        Index  ID
   00:19:e2:b0:76:eb   D         cbp.1000
   aa:bb:cc:dd:ee:f2   DC                        1048576 1048576
   aa:bb:cc:dd:ee:f3   DC                        1048575 1048575
```

show bridge mac-table

```
user@host>run show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
O -OVSDB MAC, SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC,
P -Pinned MAC)

Routing instance : VS-541
Bridging domain : 541, VLAN : 541
MAC MAC Logical NH RTR
address flags interface Index ID
00:00:01:00:00:01 DPRC xe-0/0/3.0
00:00:02:00:00:01 DP xe-0/0/3.0
```

show mac-rewrite interface

Syntax **show mac-rewrite interface**
<brief | detail>
<interface-name>

Release Information Command introduced in Junos OS Release 9.1.
Command introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

Description Display Layer 2 protocol tunneling information.

Options **brief | detail**—(Optional) Display the specified level of output.

interface *interface-name*—(Optional) Display Layer 2 protocol tunneling information for the specified interface.

Required Privilege Level view

Related Documentation
- layer2-control on page 132
- mac-rewrite on page 133

List of Sample Output
show mac-rewrite interface on page 168
show mac-rewrite interface (EX Series Switch) on page 169

Output Fields Table 15 on page 168 lists the output fields for the **show mac-rewrite interface** command. Output fields are listed in the approximate order in which they appear.

Table 15: show mac-rewrite interface Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface that has Layer 2 protocol tunneling configured on it.	**brief detail**
Protocols	Layer 2 protocols being tunneled on this interface: Cisco Discovery Protocol (**CDP**), Spanning Tree Protocol (**STP**), Per-VLAN Spanning Tree Plus (**PVSTP+**), or VLAN Trunk Protocol (**VTP**). On EX Series switches, the following Layer 2 protocols are supported: 802.3A, CDP, LACP, LLDP, MVRP, STP, VTP, GVRP, VSTP.	**brief detail**

Sample Output

show mac-rewrite interface

```
user@host> show mac-rewrite interface
Interface       Protocols

 ge-1/0/5       STP VTP CDP PVSTP+
```

show mac-rewrite interface (EX Series Switch)

```
user@switch> show mac-rewrite interface
Interface       Protocols

  ge-0/0/1       STP
```

CHAPTER 9

Index

Index

F

H

I

L

M

T

V