JUNIPER NETWORKS | Engineering Simplicity

Spanning-Tree Protocols User Guide

Published
2020-09-18

JUNOS

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

Spanning-Tree Protocols User Guide

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

9

Operational Commands

About the Documentation

IN THIS SECTION

Spanning-tree protocols on routers and switches address provide link redundancy while simultaneously preventing undesirable loops.

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 https://www.juniper.net/documentation/.

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 https://www.juniper.net/books.

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 xiv 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 xiv 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**
`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*

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

Convention	Description	Examples
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		

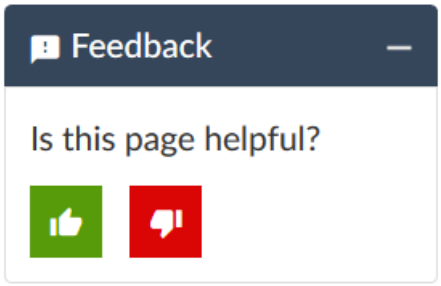
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
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**.
> (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 so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide 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 Juniper Care or Partner Support Services 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 https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- 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 https://support.juniper.net/support/requesting-support/.

1
CHAPTER

Overview

Spanning-Tree Protocol Overview

IN THIS SECTION

How Spanning Tree Protocols Work

IN THIS SECTION

Ethernet networks are susceptible to broadcast storms if loops are introduced. However, an Ethernet network needs to include loops because they provide redundant paths in case of a link failure. Spanning-tree protocols address both of these issues because they provide link redundancy while simultaneously preventing undesirable loops.

Juniper Networks devices provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP). RSTP is the default spanning-tree protocol for preventing loops on Ethernet networks.

This topic describes:

Benefits of Using Spanning Tree Protocols

Spanning Tree protocols have the following benefits:

- Provide link redundancy while simultaneously preventing undesirable loops
- Prevent Broadcast Storms
- Connects to devices that are not STP-capable, such as PCs, servers, routers, or hubs that are not connected to other switches, by using edge ports

Spanning Tree Protocols Help Prevent Broadcast Storms

Spanning-tree protocols intelligently avoid loops in a network by creating a tree topology (spanning tree) of the entire bridged network with only one available path between the tree root and a leaf. All other paths are forced into a standby state. The tree *root* is a switch within the network elected by the STA (spanning-tree algorithm) to use when computing the best path between bridges throughout the network and the root bridge. Frames travel through the network to their destination–a *leaf* such as an end-user PC–along branches. A tree *branch* is a network segment, or link, between bridges. Switches that forward frames through an STP spanning tree are called *designated bridges*.

> **NOTE:** If you are using Junos OS for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can force the original IEEE 802.1D Spanning Tree Protocol (STP) version to run in place of RSTP or VSTP by setting **force-version**.

Port Roles Determine Participation in the Spanning Tree

Each port has both a role and a state. A port's *role* determines how it participates in the spanning tree. The five port roles used in RSTP are:

- Root port—The port closest to the root bridge (has the lowest path cost from a bridge). This is the only port that receives frames from and forwards frames to the root bridge.
- Designated port—The port that forwards traffic away from the root bridge toward a leaf. A designated bridge has one designated port for every link connection it serves. A root bridge forwards frames from all of its ports, which serve as designated ports.
- Alternate port—A port that provides an alternate path toward the root bridge if the root port fails and is placed in the discarding state. This port is not part of the active spanning tree, but if the root port fails, the alternate port immediately takes over.
- Backup port—A port that provides a backup path toward the leaves of the spanning tree if a designated port fails and is placed in the discarding state. A backup port can exist only where two or more bridge

ports connect to the same LAN for which the bridge serves as the designated bridge. A backup port for a designated port immediately takes over if the port fails.

- Disabled port—The port is not part of the active spanning tree.

Port States Determine How a Port Processes a Frame

Each port has both a state and a role. A port's *state* determines how it processes a frame. RSTP places each port of a designated bridge in one of three states:

- Discarding—The port discards all BPDUs. A port in this state discards all frames it receives and does not learn MAC addresses.
- Learning—The port prepares to forward traffic by examining received frames for location information in order to build its MAC address table.
- Forwarding—The port filters and forwards frames. A port in the forwarding state is part of the active spanning tree.

Edge Ports Connect to Devices That Cannot Be Part of a Spanning Tree

Spanning Tree also defines the concept of an *edge port*, which is a designated port that connects to devices that are not STP-capable, such as PCs, servers, routers, or hubs that are not connected to other switches. Because edge ports connect directly to end stations, they cannot create network loops and can transition to the forwarding state immediately. You can manually configure edge ports, and a switch can also detect edge ports by noting the absence of communication from the end stations.

The edge ports themselves do send BPDUs to the spanning tree. If you have a good understanding of the implications on your network and want to modify RSTP on the edge port interface.

BPDUs Maintain the Spanning-Tree

Spanning-tree protocols use frames called bridge protocol data units (BPDUs) to create and maintain the spanning tree. A BPDU frame is a message sent from one switch to another to communicate information about itself, such as its bridge ID, root path costs, and port MAC addresses. The initial exchange of BPDUs between switches determines the root bridge. Simultaneously, BPDUs are used to communicate the cost of each link between branch devices, which is based upon port speed or user configuration. RSTP uses this path cost to determine the ideal route for data frames to travel from one leaf to another leaf and then blocks all other routes. If an edge port receives a BPDU, it automatically transitions to a regular RSTP port.

When the network is in a steady state, the spanning tree converges when the spanning-tree algorithm (STA) identifies both the root and designated bridges and all ports are in either a forwarding or blocking state. To maintain the tree, the root bridge continues to send BPDUs at a *hello time* interval (default 2 seconds). These BPDUs continue to communicate the current tree topology. When a port receives a hello

BPDU, it compares the information to that already stored for the receiving port. One of three actions takes place when a switch receives a BPDU:

- If the BPDU data matches the existing entry in the MAC address table, the port resets a timer called *max age* to zero and then forwards a new BPDU with the current active topology information to the next port in the spanning tree.
- If the topology in the BPDU has been changed, the information is updated in the MAC address table, *max age* is again set to zero, and a new BPDU is forwarded with the current active topology information to the next port in the spanning tree.
- When a port does not receive a BPDU for three hello times, it reacts one of two ways. If the port is the root port, a complete rework of the spanning tree occurs—see When an RSTP Root Bridge Fails. If the bridge is any non-root bridge, RSTP detects that the connected device cannot send BPDUs and converts that port to an edge port.

When a Root Bridge Fails

When a link to the root port goes down, a flag called a topology change notification (TCN) is added to the BPDU. When this BPDU reaches the next port in the VLAN, the MAC address table is flushed and the BPDU is sent to the next bridge. Eventually, all ports in the VLAN have flushed their MAC address tables. Then, RSTP configures a new root port.
After a root port or a designated port fails, the alternate or backup port takes over after an exchange of BPDUs called the proposal-agreement handshake. RSTP propagates this handshake over *point-to-point links*, which are dedicated links between two network nodes, or switches, that connect one port to another. If a local port becomes a new root or designated port, it negotiates a rapid transition with the receiving port on the nearest neighboring switch by using the proposal-agreement handshake to ensure a loop-free topology.

Devices Must Relearn MAC Addresses After a Link Failure

Because a link failure causes all associated ports to flush their MAC address table, the network might be slower as it floods to relearn the MAC addresses. There is a way to speed up this relearning process. During TCN propagation, the Layer 2 forwarding table of switches is flushed, resulting in a flood of data packets. The Address Resolution Protocol (ARP) feature causes the switch to proactively send ARP requests for IP addresses in the ARP cache (present because of Layer 3 VLAN interface). With ARP on STP enabled, as the reply comes through, the switches builds up the Layer 2 forwarding table, thus limiting the flooding later. Enabling ARP on STP is most useful to prevent excessive flooding in large Layer 2 networks using RVIs.

> **NOTE:** The ARP feature is not available on Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style.

SEE ALSO

Understanding STP | 40
Understanding MSTP | 97
Understanding RSTP | 44
Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | 72
Example: Configuring Faster Convergence and Network Stability on ELS Switches with RSTP | 49
Configuring RSTP on EX Series Switches (CLI Procedure) | 48

Choosing a Spanning Tree Protocol

IN THIS SECTION

When selecting a spanning-tree protocol, consider two basic questions:

- What STP features do I need?
- What switch or router will be used?

Comparison of Spanning Tree Features

Table 3 on page 24 describes differences between spanning-tree protocols STP, RSTP, MSTP and VSTP.

Table 3: Selecting a Spanning-Tree Protocol

Protocol	Advantages	Disadvantages
RSTP	• Rapid Spanning Tree Protocol is the default switch configuration and is recommended for most network configurations because it converges more quickly than STP after a failure. • Voice and video work better with RSTP than they do with STP. • RSTP is backward compatible with STP; therefore, switches do not all have to run RSTP. • RSTP supports more ports than MSTP or VSTP. • On MX and ACX routers, you can configure RSTP, MSTP, and VSTP instance interfaces as edge ports.	• STP and RSTP are limited to a single instance on any physical interface. Use the **set rstp interface** statement to configure interfaces participating in the RSTP instance. • RSTP does not work with 802.1D 1998 bridges. Use STP instead—see "Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure)" on page 96 • RSTP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic. Use MSTP instead.

TIP: Use the **set rstp interface** configuration statement to indicate which logical interfaces participate in RSTP. See

.

TIP: If RSTP has been forced to run as the original STP version, you can revert back to RSTP by "Reverting to RSTP or VSTP from Forced IEEE 802.1D STP" on page 164.

Table 3: Selecting a Spanning-Tree Protocol *(continued)*

Protocol	Advantages	Disadvantages
STP	• Spanning Tree Protocol works with 802.1D 1998 bridges. • RSTP is backward compatible with STP; therefore, you can run RSTP on some switches and STP on others with 802.1D 1998 bridges.	• STP and RSTP are limited to a single instance on any physical interface. Use the **set stp interface** statement to configure interfaces participating in the RSTP instance. • STP is slower than RSTP. • STP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic. Use MSTP instead. • Although STP provides basic loop prevention functionality, it does not provide fast network convergence when there are topology changes. The STP process to determine network state transitions is slower than the RSTP process because it is timer-based. RSTP converges faster because it uses a handshake mechanism based on point-to-point links instead of the timer-based process used by STP. • Edge ports are not supported when the original IEEE 802.1D STP is configured. If you specify **edge** at the **[edit protocols stp]** hierarchy level, the software ignores the option.

Table 3: Selecting a Spanning-Tree Protocol *(continued)*

Protocol	Advantages	Disadvantages
TIP: Use the **set stp interface** statement to configure interfaces to participate in the STP instance. See "Configuring STP on EX Series Switches (CLI Procedure)" on page 42.		
MSTP	• Multiple Spanning Tree Protocol works with most VLANs. • MSTP supports multiple instances on a single physical interface. • On MX and ACX routers, you can configure RSTP, MSTP, and VSTP instance interfaces as edge ports.	• Some protocols require compatibility not provided by MSTP. In this case, use VSTP. • MSTP supports a limited number of ports. An MSTP region supports up to 64 MSTIs with each instance supporting from 1 through 4094 VLANs • MSTP uses more CPU than RSTP and does not converge as fast as RSTP.
TIP: Use the **set mstp interface** configuration statement to indicate which logical interfaces participate in MSTP. See "Configuring MSTP on Switches" on page 101.		

Table 3: Selecting a Spanning-Tree Protocol *(continued)*

Protocol	Advantages	Disadvantages
VSTP	• VSTP works with VLANs that require device compatibility. Enable VSTP on all VLANs that could receive VSTP bridge protocol data units (BPDUs). • VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a switch. • 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. • On MX and ACX routers, you can configure RSTP, MSTP, and VSTP instance interfaces as edge ports.	

Table 3: Selecting a Spanning-Tree Protocol *(continued)*

Protocol	Advantages	Disadvantages
		• With VSTP, there can be only one STP instance per VLAN, where MSTP lets you combine multiple VLANs in one instance. • VSTP supports a limited number of ports compared to RSTP. • You can configure VSTP for a maximum of 509 VLANs. However, having a large number of VSTP and RSTP instances can cause continuous changes in the topology. As a performance workaround, reduce the number of VSTP instances to fewer than 190. • Using the same VLAN for RSTP and VSTP is not supported. For example, if you are configuring a VLAN under VSTP, configuring RSTP with an interface that contains the same VLAN is not supported. • If you configure VSTP and RSTP at the same time and the switch has more than 253 VLANs, VSTP is configured only for the first 253 VLANs. For the remaining VLANs, only RSTP is configured. • When you configure VSTP with the **set protocol vstp vlan vlan-id interface interface-name** command, the VLAN named **default** is excluded. You must manually configure a VLAN

Table 3: Selecting a Spanning-Tree Protocol *(continued)*

Protocol	Advantages	Disadvantages
		with the name **default** to run VSTP.

TIP: When using VSTP, we recommend that you enable VSTP on all VLANs that can receive VSTP bridge protocol data units (BPDUs).

TIP: When you configure VSTP with the **set protocol vstp vlan all** command, VLAN ID 1 is not set; it is excluded so that the configuration is compatible with Cisco PVST+. If you want VLAN ID 1 to be included in the VSTP configuration on your switch, you must set it separately with the **set protocol vstp vlan 1** command. For more information, see Knowledge Base articles KB15138 and KB18291 at https://kb.juniper.net/InfoCenter/index

TIP: The maximum number of VLANs supported by VSTP on a switch depends upon whether you are using Junos OS for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style or Junos OS that does not support ELS.

You can use Juniper Networks switches with VSTP and Cisco switches with PVST+ and Rapid-PVST+ in the same network. Cisco supports a proprietary Per-VLAN Spanning Tree (PVST) protocol, which maintains a separate spanning tree instance per each VLAN. One Spanning Tree per VLAN allows fine grain load balancing but requires more BPDU CPU processing as the number of VLANs increases. PVST runs on Cisco proprietary ISL trunks which is not supported by Juniper. Juniper switches only inter-operate with PVST+ and Rapid-PVST+.

TIP: Spanning-tree protocols all generate their own BPDUs. User bridge applications running on a PC can also generate BPDUs. If these BPDUs are picked up by STP applications running on the switch, they can trigger STP miscalculations, and those miscalculations can lead to network outages. See *Configuring BPDU Protection on Spanning Tree Interfaces*.

NOTE: If you are configuring an interface for any spanning tree protocol (STP, MSTP, RSTP, and VSTP), the **interface all**, **vlan all**, and **vlan-group** options are not available when you configure an interface with the **flexible-vlan-tagging** family option.

Switch and Router Spanning Tree Support and Limitations

Not all switches and routers support the exact same features and configurations. Known differences are listed in Table 4 on page 30.

Table 4: Spanning Tree Hardware Considerations

Router or Switch	Considerations
MX Series Routers	Only MX Series routers can use the virtual-switch routing instance type to isolate a LAN segment with its spanning-tree instance and to separate its VLAN ID space. See "Configuring a Virtual Switch Routing Instance on MX Series Routers" on page 37 Tracing and global tracing are available on ACX and MX routers with the global **traceoptions** statement—see "Understanding Spanning-Tree Protocol Trace Options" on page 281. Beginning with Release 14.1R1, these STP log enhancements are supported on MX Series routers: • Logging of information in the internal ring buffer about events like Spanning Tree (such as STP, MSTP, RSTP, or VSTP) interface role or state change without having to configure STP traceoptions. • Capturing information as to what triggered the spanning-tree role or state change. On MX and ACX routers, you can configure RSTP, MSTP, and VSTP instance interfaces as edge ports for faster convergence than the original 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. On an MX Series router running RSTP or MSTP in a provider network, you can enable provider bridge participation in the RSTP or MSTP instance—see *Understanding Provider Bridge Participation in RSTP or MSTP Instances*.

TIP: For 802.1ad provider bridge networks (stacked VLANs) on MX Series and M Series routers, 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.

Table 4: Spanning Tree Hardware Considerations *(continued)*

Router or Switch	Considerations
ACX Series Routers	On MX and ACX routers, you can configure RSTP, MSTP, and VSTP instance interfaces as edge ports for faster convergence than the original 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. Tracing and global tracing are available on ACX and MX routers with the global **traceoptions** statement—see "Understanding Spanning-Tree Protocol Trace Options" on page 281.
QFX Series Switches	See *Configuring STP*. If your network includes IEEE 802.1D 1998 bridges, remove RSTP and explicitly configure STP—see "Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure)" on page 96. When you explicitly configure STP, the QFX Series products use the IEEE 802.1D 2004 specification, force version 0. This configuration runs a version of RSTP that is compatible with the classic, basic STP. If you use virtual LANs (VLANs), you can enable VSTP on your network. The STP support provided for the QFX Series includes: • IEEE 802.1d • 802.1w RSTP • 802.1s MSTP Use Rapid Spanning Tree Protocol (RSTP) on the network side of the QFX Series to provide quicker convergence time than the base Spanning Tree Protocol (STP) does. RSTP identifies certain links as point to point. When a point-to-point link fails, the alternate link can transition to the forwarding state, which speeds up convergence. An interface can be configured for either root protection or loop protection, but not for both. On EX Series (except EX9200) and QFX Series switches running Junos OS that supports ELS—VSTP can support up to 510 VLANs. If your EX Series or QFX Series switch interoperates with a Cisco device running Rapid per VLAN Spanning Tree (Rapid PVST+), we recommend that you enable both VSTP and RSTP on the EX Series or QFX Series interface.

Table 4: Spanning Tree Hardware Considerations *(continued)*

Router or Switch	Considerations
EX Series Switches	• There are two versions of EX Series switches. Be sure to use the correct commands for each version. Some EX switches run the Juniper Networks Junos operating system (Junos OS) that supports the Enhanced Layer 2 Software (ELS) configuration (for example, EX4300, EX2300, EX3400 and EX4600 support ELS) and some do not support the ELS configuration. • EX Series switches configured to use STP actually run RSTP force version 0, which is compatible with STP. If you are using Junos OS for EX Series switches with support for ELS, you can force the original IEEE 802.1D Spanning Tree Protocol (STP) version to run in place of RSTP or VSTP. See "Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure)" on page 96. • On EX Series (except EX9200) and QFX Series switches running Junos OS that supports ELS—VSTP can support up to 510 VLANs. However, on EX9200 switches, VSTP can support only up to 253 VLANs. • The EX Series switches EX4300, EX4600 and the QFX platforms QFX5100, QFX3500, QFX3600 support 510 Vlans on VSTP. • On EX9200 switches—VSTP can support up to 4000 VLANs. • On an EX Series switch running Junos OS that does not support ELS—VSTP can support up to 253 VLANs. • EX4300 switches can be configured for STP only by enabling RSTP and forcing it to act as STP. Select the Force STP check box from the RSTP configuration page. • An interface can be configured for either root protection or loop protection, but not for both. • If your EX Series or QFX Series switch interoperates with a Cisco device running Rapid per VLAN Spanning Tree (Rapid PVST+), we recommend that you enable both VSTP and RSTP on the EX Series or QFX Series interface. • The ARP feature is not available for EX Series switches supporting the Enhanced Layer 2 Software (ELS) configuration style.

TIP: EX Series switches can have a maximum of 253 VLANs on VSTP. Therefore, to have as many spanning-tree protocol VLANs as possible, use both VSTP and RSTP. RSTP will then be applied to VLANs that exceed the limit for VSTP. Because RSTP is enabled by default, you just need to additionally enable VSTP.

Table 4: Spanning Tree Hardware Considerations *(continued)*

Router or Switch	Considerations
QFabric	Although there is no need to run STP in a QFabric system, you can connect a QFabric system to another Layer 2 device and use STP. STP traffic can only be processed on network Node groups. Other Node groups, such redundant server Node groups and server Node groups, discard the STP bridge protocol data units (BPDUs) traffic and disable the interface automatically. Server Node groups only process host-facing protocols, whereas Network Node groups process all supported protocols.
SRX Series devices	• Provide Layer 2 loop prevention through STP, RSTP, or MSTP only. VSTP is not supported on the SRX platform. • There are two versions of SRX Series devices. Be sure to use the correct commands for each version. Some SRX Series devices run the Juniper Networks Junos operating system (Junos OS) that supports the Enhanced Layer 2 Software (ELS) configuration and some do not support the ELS configuration. • Starting in Junos OS Release 15.1X49-D70, the Spanning Tree Protocol (STP) is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices. Spanning Tree Protocol (STP) is not supported from Junos Os Release 15.1X49-D40 to Junos OS Release 15.1X49-D60. • An interface can be configured for either root protection or loop protection, but not for both.

2

CHAPTER

Spanning-Tree Instances and Interfaces

Spanning Tree Instances and Interfaces

IN THIS SECTION

Understanding Spanning-Tree Instance Interfaces

IN THIS SECTION

An instance is analogous to one computer process. The 802.1Q standard defines one unique Spanning-Tree instance to be used by all VLANs in the network. STP runs on the Native VLAN so that it can communicate with both 802.1Q and non-802.1Q compatible switches. This single instance of STP is also referred to as 802.1Q Mono Spanning Tree or Common Spanning Tree (CST).

Benefits of Spanning-Tree Instance Interface Configuration

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 (Spanning Tree)** mode is configured at both the VSTP global and VLAN levels, the configuration at the VLAN level overrides the global configuration.

How Many Instances Do Spanning Tree Protocols Have?

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

MSTP supports multiple instances on a single physical interface. Again, use the **interface (Spanning Tree)** 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.

Spanning-Tree Instance Interfaces Have Priorities

The reason that instances must have priorities is because a root port for a spanning tree 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.

What is 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.

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

Configuring a Virtual Switch Routing Instance on MX Series Routers

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* .

SEE ALSO

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.

SEE ALSO

Example: Configuring BPDU Protection on MX Edge Interfaces to Prevent STP Miscalculations | **194**

Configuring Rapid Spanning Tree Protocol | **45**

Configuring Multiple Spanning Tree Protocol | **105**

Configuring VLAN Spanning Tree Protocol

edge | **313**

interface (Spanning Tree) | **324**

Configuring RSTP on EX Series Switches (CLI Procedure) | **48**

Configuring MSTP on Switches | **101**

3

CHAPTER

Configuring Spanning-Tree Protocols

Configuring STP Protocol

IN THIS SECTION

Understanding STP

IN THIS SECTION

Spanning Tree Protocol (STP), defined in IEEE 802.1D, creates a tree of links in the Ethernet switched network. Links that cause loops in the network are disabled, thereby providing a single active link between any two devices.

Benefits of Using the Original STP

Some benefits of using the original STP are:

- Some legacy networks require the slower convergence times of basic STP.
- STP supports older 802.1D 1998 bridges.
- You can run RSTP on some switches and STP on others with 802.1D 1998 bridges. They are compatible.

STP on MX Routers

Beginning with Release 14.1R1, these enhancements are supported on STP logs in the MX Series support:

- Logging of information in the internal ring buffer about events like Spanning Tree (such as STP, MSTP, RSTP, or VSTP) interface role or state change without having to configure STP traceoptions.
- Capturing information as to what triggered the spanning-tree role or state change.

STP on SRX Firewalls

Spanning Tree Protocol (STP) is not supported on SRX devices from Junos Os Release 15.1X49-D40 to Junos OS Release 15.1X49-D60.

Starting in Junos OS Release 15.1X49-D70, the Spanning Tree Protocol (STP) is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

STP on EX Series Switches

EX Series switches configured to use STP actually run RSTP force version 0, which is compatible with STP. If you are using Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can force the original IEEE 802.1D Spanning Tree Protocol (STP) version to run in place of RSTP or VSTP by setting **force-version**.

STP Operation Mode Commands

You can use the operational mode commands **show spanning-tree statistics message-queues**, **show spanning-tree stp-buffer see-all**, **show spanning-tree statistics bridge**, and **show spanning-tree statistics interface** to get the information from ring-buffer, bridge, and port statistics. **clear spanning-tree stp-buffer** clears the stp-buffer, and **clear spanning-tree statistics bridge** clears the statistics of the bridge.

SEE ALSO

> *Understanding Layer 2 Protocol Tunneling*

Understanding System Identifiers for Bridges in STP or RSTP Instances

Spanning tree protocols work by creating bridges. A root bridge (switch) is a bridge at the top of a Spanning Tree. Ethernet connections branch out from the root switch, connecting to other switches in the Local

Area Network (LAN). An extended system identifier is assigned to bridges in STP or RSTP routing instances—see **extended-system-id**.

When you configure STP or RSTP, you specify the extended system identifier.

SEE ALSO

Configuring STP on EX Series Switches (CLI Procedure)

The default spanning-tree protocol for EX Series switches is Rapid Spanning Tree Protocol (RSTP). RSTP provides faster convergence times than the original Spanning Tree Protocol (STP). However, some legacy networks require the slower convergence times of basic STP that work with 802.1D 1998 bridges.

If your network includes 802.1D 1998 bridges, you can remove RSTP and explicitly configure STP. When you explicitly configure STP, the switches use the IEEE 802.1D 2004 specification, force version 0. This configuration runs a version of RSTP that is compatible with the classic, basic STP.

To configure STP:

1. Either delete RSTP on the entire switch or disable RSTP on specific interfaces:
   - To delete RSTP on the entire switch:

     ```
     [edit protocols]
     user@switch# delete rstp
     ```

   - To disable RSTP on a specific interface:

     ```
     [edit protocols]
     user@switch# set rstp interface interface-name disable
     ```

2. Enable STP either on all interfaces or on a specific interface:
   - To enable STP on all interfaces:

     ```
     [edit protocols]
     user@switch# set stp interface all
     ```

   - To enable STP on a specific interface:

     ```
     [edit protocols]
     user@switch# set stp interface interface-name
     ```

3. (Optional) Only if a routed VLAN interface (RVI) is configured, enable the Address Resolution Protocol (ARP) for faster MAC address recovery:

   - To enable ARP on STP on all interfaces:

     ```
     [edit protocols]
     user@switch#  set stp interface all arp-on-stp
     ```

   - To enable ARP on STP on a specific interface:

     ```
     [edit protocols]
     user@switch#  set stp interface interface-name  arp-on-stp
     ```

RELATED DOCUMENTATION

Understanding Layer 2 Protocol Tunneling

Configuring RSTP Protocol

IN THIS SECTION

Understanding RSTP

IN THIS SECTION

Juniper Networks products use Rapid Spanning Tree Protocol (RSTP) on the network side of devices by default to provide quicker convergence time than the base Spanning Tree Protocol (STP) does. RSTP identifies certain links as point to point. When a point-to-point link fails, the alternate link can transition to the forwarding state, which speeds up convergence.

Benefits of Using RSTP

Some benefits of using the original STP are:

- RSTP is faster than STP.
- Voice and video work better with RSTP than they do with STP.
- RSTP supports more ports than MSTP or VSTP.
- RSTP is backward compatible with STP; therefore, switches do not all have to run RSTP.
- On MX and ACX routers, you can configure RSTP, MSTP, and VSTP instance interfaces as edge ports.

Why is RSTP the Default Spanning-Tree Protocol?

RSTP evolved from the original STP IEEE 802.1D protocol to provide faster spanning-tree reconvergence after a switch port, switch, or LAN failure. Where STP took up to 50 seconds to respond to topology changes, RSTP responds to changes within the timeframe of three hello BPDUs (bridge protocol data units), or 6 seconds. This is the primary reason that RSTP is the default spanning-tree configuration.

TIP: EX Series switches configured to use STP actually run RSTP force version 0, which is compatible with STP.

SEE ALSO

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 281.

6. Configure the bridge priority:

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

For more information, see "Understanding Bridge Priority for Election of Root Bridge and Designated Bridge" on page 258.

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.
        }
    }
}
```

Configuring RSTP on EX Series Switches (CLI Procedure)

The default spanning-tree protocol for EX Series switches is Rapid Spanning Tree Protocol (RSTP). RSTP provides faster convergence times than the original Spanning Tree Protocol (STP). Because RSTP is configured by default, you only need to use this procedure If another spanning-tree protocol has been configured. In that case, you can reconfigure RSTP.

To enable RSTP:

1. Disable the other configured spanning-tree protocol (MSTP):
   - To disable MSTP:

     ```
     [edit protocols]
     user@switch# set mstp disable
     ```

2. Configure RSTP
   - To enable RSTP on a specific interface:

     ```
     [edit protocols]
     user@switch# set rstp interface interface-name
     ```

   - To disable RSTP on a specific interface:

     ```
     [edit protocols]
     user@switch# set rstp interface interface-name disable
     ```

   - To enable RSTP on a range of interfaces:

     ```
     [edit protocols]
     user@switch# set rstp interface interface-range-name
     ```

   - To enable RSTP on all interfaces:

     ```
     [edit protocols]
     user@switch# set rstp interface all
     ```

Example: Configuring Faster Convergence and Network Stability on ELS Switches with RSTP

IN THIS SECTION

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches" on page 72. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

EX Series switches use Rapid Spanning Tree Protocol (RSTP) by default to provide a loop-free topology.

When switches that support redundant Routing Engines use RSTP, it is important to keep RSTP synchronized on both Routing Engines so that no loss of service occurs after a Routing Engine switchover. Nonstop bridging protocol keeps Routing Engines synchronized.

This example describes how to configure RSTP and NSB on four EX Series switches:

Requirements

This example uses the following software and hardware components:

- Junos OS Release 15.1 or later or later for EX Series switches
- Four EX Series switches

Before you configure the switches for RSTP, be sure you have:

- Installed and connected the four switches. See the hardware documentation for your switch.

- Performed the initial software configuration on all switches. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.

Overview and Topology

RSTP works by identifying certain links as point to point links and blocking other possible paths. When one of the point-to-point links fails, a designated alternate link transitions to the forwarding state and take over. Configuring nonstop bridging (NSB) on a switch with redundant Routing Engines keeps RSTP synchronized on both Routing Engines. This way, RSTP remains active immediately after a switchover because it is already synchronized to the backup Routing Engine. RSTP does not have to reconverge after a Routing Engine switchover when NSB is enabled because the neighbor devices do not detect an RSTP change on the switch. In this example, four EX Series switches are connected in the topology displayed in Figure 1 on page 50 to create a loop-free topology with NSB applied to switches with dual Routing Engines.

Figure 1: Network Topology for RSTP

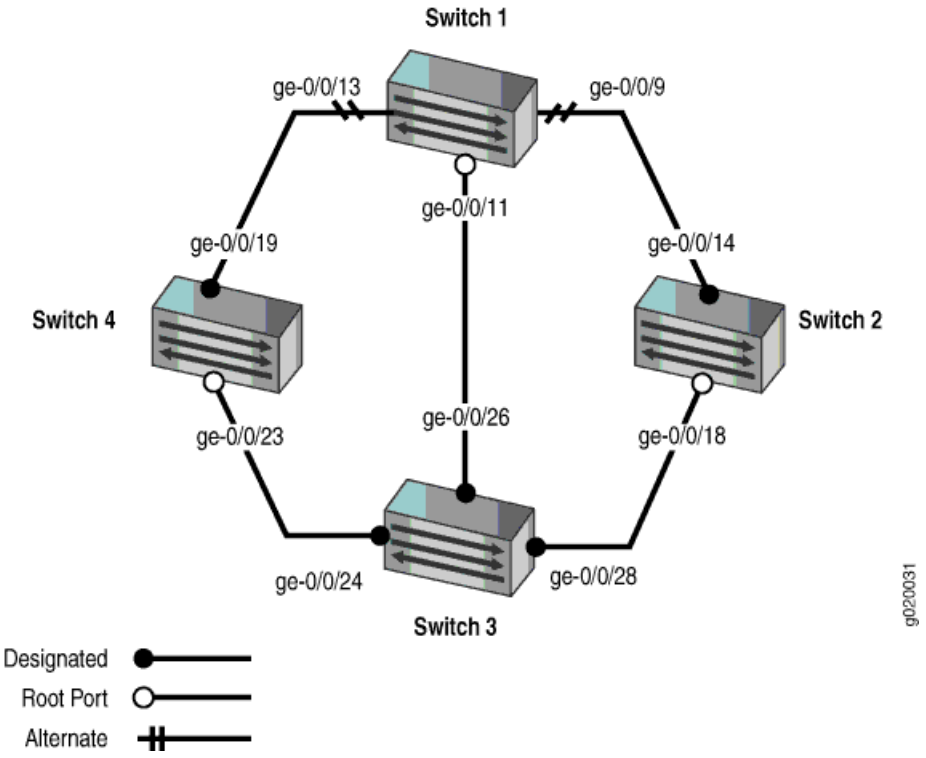


Table 5 on page 51 shows the components of the topology for this example.

NOTE: You can configure RSTP only on physical interfaces, not on logical interfaces.

Table 5: Components of the Topology for Configuring RSTP

Property	Settings
Switch 1	The following interfaces on Switch 1 are connected in this way: • **ge-0/0/9** is connected to Switch 2 • **ge-0/0/13** is connected to Switch 4 • **ge-0/0/11** is connected to Switch 3
Switch 2	The following interfaces on Switch 2 are connected in this way: • **ge-0/0/14** is connected to Switch 1 • **ge-0/0/18** is connected to Switch 3
Switch 3	The following interfaces on Switch 3 are connected in this way: • **ge-0/0/26** is connected to Switch 1 • **ge-0/0/28** is connected to Switch 2 • **ge-0/0/24** is connected to Switch 4
Switch 4	The following interfaces on Switch 4 are connected in this way: • **ge-0/0/19** is connected to Switch 1 • **ge-0/0/23** is connected to Switch 3
VLAN names and tag IDs	**voice-vlan**, tag **10** **employee-vlan**, tag **20** **guest-vlan**, tag **30** **camera-vlan**, tag **40**

This configuration example creates a loop-free topology between four EX Series switches using RSTP.

An RSTP topology contains ports that have specific roles:

- The *root port* is responsible for forwarding data to the root bridge.
- The *alternate port* is a standby port for the root port. When a root port goes down, the alternate port becomes the active root port.
- The *designated port* forwards data to the downstream network segment or device.
- The *backup port* is a backup port for the designated port. When a designated port goes down, the backup port becomes the active designated port and starts forwarding data.

NOTE: You also can create a loop-free topology between the aggregation layer and the distribution layer using redundant trunk links. For more information about configuring redundant trunk links, see *Example: Configuring Redundant Trunk Links for Faster Recovery on Devices with ELS Support*.

Configuring RSTP and Nonstop Bridging on Switch 1

CLI Quick Configuration

To quickly configure RSTP and nonstop bridging on Switch 1, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans voice-vlan description “Voice VLAN”
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description “Employee VLAN”
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description “Guest VLAN”
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description “Camera VLAN”
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/9 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/13 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/9 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode trunk
set protocols rstp bridge-priority 16k
set protocols rstp interface all cost 1000
```

set protocols rstp interface all mode point-to-point

If Switch 1 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 1, copy the following commands and paste them into the switch terminal window:

set chassis redundancy graceful-switchover

set system commit synchronize

set protocols layer2-control nonstop-bridging

> **NOTE:** NFX150 devices support only a single Routing Engine.

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 1:

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch1# set voice-vlan description “Voice VLAN”
user@switch1# set voice-vlan vlan-id 10
user@switch1# set employee-vlan description “Employee VLAN”
user@switch1# set employee-vlan vlan-id 20
user@switch1# set guest-vlan description “Guest VLAN”
user@switch1# set guest-vlan vlan-id 30
user@switch1# set camera-vlan description “Camera VLAN”
user@switch1# set camera-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:

```
[edit interfaces]
user@switch1# set ge-0/0/13 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch1# set ge-0/0/9 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch1# set ge-0/0/11 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch1# set ge-0/0/13 unit 0 family ethernet-switching interface-mode trunk
user@switch1# set ge-0/0/9 unit 0 family ethernet-switching interface-mode trunk
```

```
user@switch1# set ge-0/0/11 unit 0 family ethernet-switching interface-mode trunk
```

4. Configure RSTP on the switch:

```
[edit protocols]
user@switch1# rstp bridge-priority 16k
user@switch1# rstp interface all cost 1000
user@switch1# rstp interface all mode point-to-point
```

Step-by-Step Procedure

If Switch 1 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 1:

1. Enable graceful Routing Engine switchover (GRES):

```
[edit chassis redundancy]
user@switch1# set graceful-switchover
```

2. Configure the switch to always synchronize configuration changes between the Routing Engines:

```
[edit system]
user@switch1# set commit synchronize
```

   If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

```
[edit protocols layer2-control]
user@switch1# set nonstop-bridging
```

> **NOTE:** This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

Results

Check the results of the configuration:

```
user@switch1> show configuration
interfaces {
    ge-0/0/13 {
        unit 0 {
```

```
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
    ge-0/0/9 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
    ge-0/0/11 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
}
protocols {
    layer2-control {
        nonstop-bridging;
    }
    rstp {
        bridge-priority 16k;
            interface ge-0/0/13 {
                cost 1000;
                mode point-to-point;
            }
            interface ge-0/0/9 {
                cost 1000;
                mode point-to-point;
            }
            interface ge-0/0/11 {
```

```
            cost 1000;
            mode point-to-point;
          }
        }
      }
    }
    vlans {
      voice-vlan {
        vlan-id 10;
      }
      employee-vlan {
        vlan-id 20;
      }
      guest-vlan {
        vlan-id 30;
      }
      camera-vlan {
        vlan-id 40;
      }
    }
    system {
      commit synchronize;
    }
    chassis {
      redundancy {
        graceful-switchover;
      }
```

Configuring RSTP and Nonstop Bridging on Switch 2

CLI Quick Configuration

To quickly configure RSTP and nonstop bridging on Switch 2, copy the following commands and paste them into the switch terminal window:

```
[edit]
```

set vlans voice-vlan description “Voice VLAN”

set vlans voice-vlan vlan-id 10

set vlans employee-vlan description “Employee VLAN”

set vlans employee-vlan vlan-id 20

set vlans guest-vlan description “Guest VLAN”

set vlans guest-vlan vlan-id 30

set vlans camera-vlan description “Camera VLAN”

set vlans camera-vlan vlan-id 40

set interfaces ge-0/0/14 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/18 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/14 unit 0 family ethernet-switching interface-mode trunk

set interfaces ge-0/0/18 unit 0 family ethernet-switching interface-mode trunk

set protocols rstp bridge-priority 32k

set protocols rstp interface ge-0/0/14 cost 1000

set protocols rstp interface ge-0/0/14 mode point-to-point

set protocols rstp interface ge-0/0/18 cost 1000

set protocols rstp interface ge-0/0/18 mode point-to-point

> **NOTE:** Starting with Junos OS Release 15.1 for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can configure spanning tree parameters globally on all spanning tree interfaces. See “Configuring RSTP on EX Series Switches (CLI Procedure)” on page 48 for additional information.

If Switch 2 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 2, copy the following commands and paste them into the switch terminal window:

set chassis redundancy graceful-switchover

set system commit synchronize

set protocols layer2-control nonstop-bridging

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 2:

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch2# set voice-vlan description “Voice VLAN”
user@switch2# set voice-vlan vlan-id 10
user@switch2# set employee-vlan description “Employee VLAN”
user@switch2# set employee-vlan vlan-id 20
user@switch2# set guest-vlan description “Guest VLAN”
user@switch2# set guest-vlan vlan-id 30
user@switch2# set camera-vlan vlan-description “Camera VLAN”
user@switch2# set camera-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:

```
[edit interfaces]
user@switch2# set ge-0/0/14 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch2# set ge-0/0/18 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch2# set ge-0/0/14 unit 0 family ethernet-switching interface-mode trunk
user@switch2# set ge-0/0/18 unit 0 family ethernet-switching interface-mode trunk
```

4. Configure RSTP on the switch:

```
[edit protocols]
user@switch2# rstp bridge-priority 32k
user@switch2# rstp interface ge-0/0/14 cost 1000
user@switch2# rstp interface ge-0/0/14 mode point-to-point
user@switch2# rstp interface ge-0/0/18 cost 1000
user@switch2# rstp interface ge-0/0/18 mode point-to-point
```

Step-by-Step Procedure

If Switch 2 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 2:

1. Enable graceful Routing Engine switchover (GRES):

```
[edit chassis redundancy]
user@switch2# set graceful-switchover
```

2. Configure the switch to always synchronize configuration changes between the Routing Engines:

```
[edit system]
user@switch2# set commit synchronize
```

If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

```
[edit protocols layer2-control]
user@switch2# set nonstop-bridging
```

> **NOTE:** This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

Results

Check the results of the configuration:

```
user@switch2> show configuration
interfaces {
    ge-0/0/14 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
    ge-0/0/18 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
```

```
}
protocols {
    layer2-control {
        nonstop-bridging;
    }
    rstp {
        bridge-priority 32k;
            interface ge-0/0/14 {
                cost 1000;
                mode point-to-point;
            }
            interface ge-0/0/18 {
                cost 1000;
                mode point-to-point;
            }
        }
    }
}
vlans {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
system {
    commit synchronize;
}
chassis {
    redundancy {
        graceful-switchover;
    }
```

Configuring RSTP and Nonstop Bridging on Switch 3

CLI Quick Configuration

To quickly configure RSTP and nonstop bridging on Switch 3, copy the following commands and paste them into the switch terminal window:

```
[edit]
```

set vlans voice-vlan description “Voice VLAN”

set vlans voice-vlan vlan-id 10

set vlans employee-vlan description “Employee VLAN”

set vlans employee-vlan vlan-id 20

set vlans guest-vlan description “Guest VLAN”

set vlans guest-vlan vlan-id 30

set vlans camera-vlan description “Camera VLAN”

set vlans camera-vlan vlan-id 40

set interfaces ge-0/0/26 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/28 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/26 unit 0 family ethernet-switching interface-mode trunk

set interfaces ge-0/0/28 unit 0 family ethernet-switching interface-mode trunk

set interfaces ge-0/0/24 unit 0 family ethernet-switching interface-mode trunk

set protocols rstp bridge-priority 8k

set protocols rstp interface ge-0/0/26 cost 1000

set protocols rstp interface ge-0/0/26 mode point-to-point

set protocols rstp interface ge-0/0/28 cost 1000

set protocols rstp interface ge-0/0/28 mode point-to-point

set protocols rstp interface ge-0/0/24 cost 1000

set protocols rstp interface ge-0/0/24 mode point-to-point

If Switch 3 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 3, copy the following commands and paste them into the switch terminal window:

set chassis redundancy graceful-switchover

set system commit synchronize

set protocols layer2-control nonstop-bridging

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 3:

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch3# set voice-vlan description “Voice VLAN”
user@switch3# set voice-vlan vlan-id 10
user@switch3# set employee-vlan description “Employee VLAN”
user@switch3# set employee-vlan vlan-id 20
user@switch3# set guest-vlan description “Guest VLAN”
user@switch3# set guest-vlan vlan-id 30
user@switch3# set camera-vlan description “Camera VLAN”
user@switch3# set camera-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:

```
[edit interfaces]
user@switch3# set ge-0/0/26 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch3# set ge-0/0/28 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch3# set ge-0/0/24 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch3# set ge-0/0/26 unit 0 family ethernet-switching interface-mode trunk
user@switch3# set ge-0/0/28 unit 0 family ethernet-switching interface-mode trunk
user@switch3# set ge-0/0/24 unit 0 family ethernet-switching interface-mode trunk
```

4. Configure RSTP on the switch:

```
[edit protocols]
user@switch3# rstp bridge-priority 8k
user@switch3# rstp interface ge-0/0/26 cost 1000
```

```
user@switch3# rstp interface ge-0/0/26 mode point-to-point
user@switch3# rstp interface ge-0/0/28 cost 1000
user@switch3# rstp interface ge-0/0/28 mode point-to-point
user@switch3# rstp interface ge-0/0/24 cost 1000
user@switch3# rstp interface ge-0/0/24 mode point-to-point
```

Step-by-Step Procedure

If Switch 3 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 3:

1. Enable graceful Routing Engine switchover (GRES):

   ```
   [edit chassis redundancy]
   user@switch3# set graceful-switchover
   ```

2. Configure the switch to always synchronize configuration changes between the Routing Engines:

   ```
   [edit system]
   user@switch3# set commit synchronize
   ```

   If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

   ```
   [edit protocols layer2-control]
   user@switch3# set nonstop-bridging
   ```

> **NOTE:** This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

Results

Check the results of the configuration:

```
user@switch3> show configuration
  interfaces {
    ge-0/0/26 {
      unit 0 {
        family ethernet-switching {
          interface-mode trunk;
          vlan {
```

```
                members [10 20 30 40];
            }
        }
    }
    ge-0/0/28 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
    ge-0/0/24 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
}
protocols {
    layer2-control {
        nonstop-bridging;
    }
    rstp {
        bridge-priority 8k;
        interface ge-0/0/26 {
            cost 1000;
            mode point-to-point;
        }
        interface ge-0/0/28 {
            cost 1000;
            mode point-to-point;
        }
        interface ge-0/0/24 {
            cost 1000;
            mode point-to-point;
```

```
            }
        }
        bridge-priority 8k;
            }
        }
    }
}
vlans {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
system {
    commit synchronize;
}
chassis {
    redundancy {
        graceful-switchover;
    }
```

Configuring RSTP and Nonstop Bridging on Switch 4

CLI Quick Configuration

To quickly configure RSTP and nonstop bridging on Switch 4, copy the following commands and paste them into the switch terminal window:

```
[edit]
```

set vlans voice-vlan description “Voice VLAN”

set vlans voice-vlan vlan-id 10

set vlans employee-vlan description “Employee VLAN”

set vlans employee-vlan vlan-id 20

set vlans guest-vlan description “Guest VLAN”

set vlans guest-vlan vlan-id 30

set vlans camera-vlan description “Camera VLAN”

set vlans camera-vlan vlan-id 40

set interfaces ge-0/0/23 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/19 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/23 unit 0 family ethernet-switching interface-mode trunk

set interfaces ge-0/0/19 unit 0 family ethernet-switching interface-mode trunk

set protocols rstp bridge-priority 16k

set protocols rstp interface ge-0/0/23 cost 1000

set protocols rstp interface ge-0/0/23 mode point-to-point

set protocols rstp interface ge-0/0/19 cost 1000

set protocols rstp interface ge-0/0/19 mode point-to-point

If Switch 4 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 4, copy the following commands and paste them into the switch terminal window:

set chassis redundancy graceful-switchover

set system commit synchronize

set protocols layer2-control nonstop-bridging

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 4:

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch4# set voice-vlan description “Voice VLAN”
user@switch4# set voice-vlan vlan-id 10
user@switch4# set employee-vlan description “Employee VLAN”
user@switch4# set employee-vlan vlan-id 20
user@switch4# set guest-vlan description “Guest VLAN”
user@switch4# set guest-vlan vlan-id 30
user@switch4# set camera-vlan description “Camera VLAN”
user@switch4# set camera-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:

```
[edit interfaces]
user@switch4# set ge-0/0/23 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch4# set ge-0/0/19 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch4# set ge-0/0/23 unit 0 family ethernet-switching interface-mode trunk
user@switch4# set ge-0/0/19 unit 0 family ethernet-switching interface-mode trunk
```

4. Configure RSTP on the switch:

```
[edit protocols]
user@switch4# rstp bridge-priority 16k
user@switch4# rstp interface ge-0/0/23 cost 1000
user@switch4# rstp interface ge-0/0/23 mode point-to-point
user@switch4# rstp interface ge-0/0/19 cost 1000
user@switch4# rstp interface ge-0/0/19 mode point-to-point
```

Step-by-Step Procedure

If Switch 4 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 4:

1. Enable graceful Routing Engine switchover (GRES):

```
[edit chassis redundancy]
user@switch4# set graceful-switchover
```

2. Configure the switch to always synchronize configuration changes between the Routing Engines:

```
[edit system]
user@switch4# set commit synchronize
```

If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

```
[edit protocols layer2-control]
user@switch4# set nonstop-bridging
```

> **NOTE:** This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

Results

Check the results of the configuration:

```
user@switch4> show configuration
interfaces {
    ge-0/0/23 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
    ge-0/0/19 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
```

```
}
protocols {
    layer2-control {
        nonstop-bridging;
    }
    rstp {
        bridge-priority 16k;
            interface ge-0/0/23 {
                cost 1000;
                mode point-to-point;
            }
            interface ge-0/0/19 {
                cost 1000;
                mode point-to-point;
            }
        }
    }
}
vlans {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
system {
    commit synchronize;
}
chassis {
    redundancy {
        graceful-switchover;
    }
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks on both Routing Engines:

Verifying RSTP Configuration on Switch 1

Purpose

Verify the RSTP configuration on Switch 1.

Action

Use the operational mode command:

```
user@switch1>  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-0/0/13    128:526      128:526  16384.0019e25040e0      1000  BLK    ALT
ge-0/0/9     128:522      128:522  32768.0019e2503d20      1000  BLK    ALT
ge-0/0/11    128:524      128:524   8192.0019e25051e0      1000  FWD    ROOT
```

Meaning

The operational mode command **show spanning-tree interface** shows that **ge-0/0/13** is in a forwarding state. The other interfaces on Switch 1 are blocking.

Verifying RSTP Configuration on Switch 2

Purpose

Use this procedure to verify the RSTP configuration on both Switch 2 Routing Engines.

Action

Use the operational mode command:

```
user@switch2>  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-0/0/14     128:527      128:527  32768.0019e2503d20      1000  FWD    DESG
ge-0/0/18     128:529      128:529   8192.0019e25051e0      1000  FWD    ROOT
```

Meaning

The operational mode command **show spanning-tree interface** shows that **ge-0/0/18** is in a forwarding state and is the root port.

Verifying RSTP Configuration on Switch 3

Purpose

Use this procedure to verify the RSTP configuration on both Switch 3 Routing Engines.

Action

Use the operational mode commands:

```
user@switch3>  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-0/0/26     128:539      128:539   8192.0019e25051e0      1000  FWD    DESG
ge-0/0/28     128:541      128:541   8192.0019e25051e0      1000  FWD    DESG
ge-0/0/24     128:537      128:537   8192.0019e25051e0      1000  FWD    DESG
```

Meaning

The operational mode command **show spanning-tree interface** shows that no interface is the root interface.

Verifying RSTP Configuration on Switch 4

Purpose

Use this procedure to verify the RSTP configuration on both Switch 4 Routing Engines.

Action

Use the operational mode commands:

```
user@switch4>  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-0/0/23    128:536      128:536   8192.0019e25051e0      1000  FWD    ROOT
ge-0/0/19    128:532      128:532   16384.0019e25040e0     1000  FWD    DESG
```

Meaning

The operational mode command **show spanning-tree interface** shows that interface **ge-0/0/23** is the root interface and forwarding.

Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches

IN THIS SECTION

EX Series switches use Rapid Spanning Tree Protocol (RSTP) by default to provide a loop-free topology.

When switches that support redundant Routing Engines use RSTP, it is important to keep RSTP synchronized on both Routing Engines so that no loss of service occurs after a Routing Engine switchover. Nonstop bridging protocol keeps Routing Engines synchronized.

This example describes how to configure RSTP and NSB on four EX Series switches:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.3 or later for EX Series switches
- Four EX Series switches

Before you configure the switches for RSTP, be sure you have:

- Installed the four switches. See *Connecting and Configuring an EX Series Switch (J-Web Procedure)*.
- Performed the initial software configuration on all switches. See *Installing and Connecting an EX3200 Switch*.

Overview and Topology

RSTP works by identifying certain links as point to point links and blocking other possible paths. When one of the point-to-point links fails, a designated alternate link transitions to the forwarding state and take over. Configuring nonstop bridging (NSB) on a switch with redundant Routing Engines keeps RSTP synchronized on both Routing Engines. This way, RSTP remains active immediately after a switchover because it is already synchronized to the backup Routing Engine. RSTP does not have to reconverge after a Routing Engine switchover when NSB is enabled because the neighbor devices do not detect an RSTP change on the switch. In this example, four EX Series switches are connected in the topology displayed in Figure 2 on page 74 to create a loop-free topology with NSB applied to switches with dual Routing Engines.

Figure 2: Network Topology for RSTP

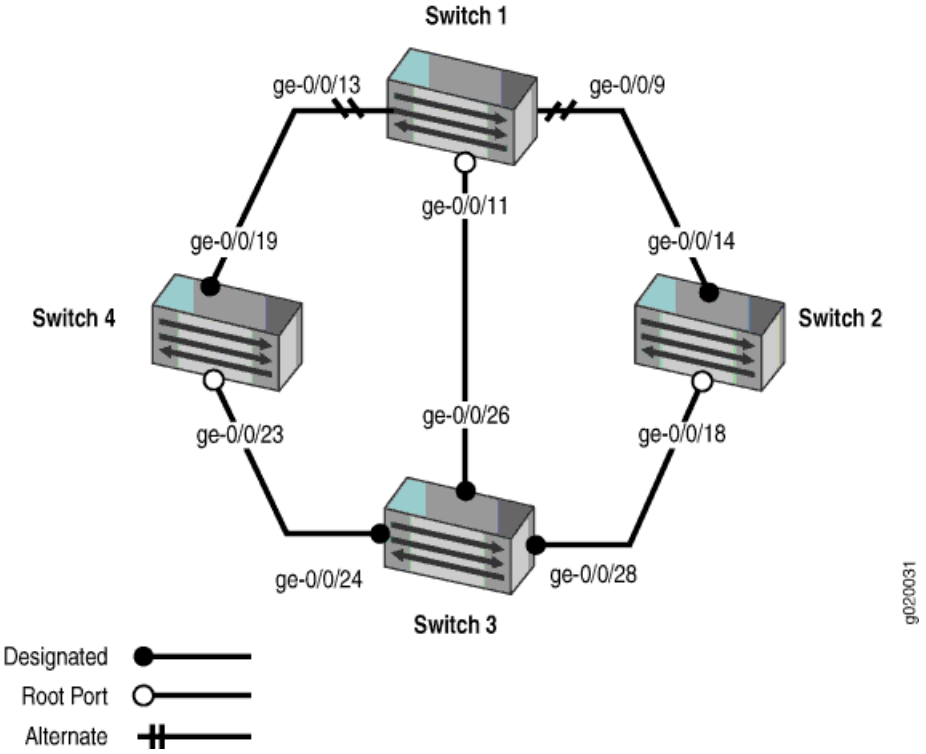


Table 6 on page 74 shows the components of the topology for this example.

> **NOTE:** You can configure RSTP on logical or physical interfaces. This example shows RSTP configured on logical interfaces.

Table 6: Components of the Topology for Configuring RSTP

Property	Settings
Switch 1	The following interfaces on Switch 1 are connected in this way: • **ge-0/0/9** is connected to Switch 2 • **ge-0/0/13** is connected to Switch 4 • **ge-0/0/11** is connected to Switch 3
Switch 2	The following interfaces on Switch 2 are connected in this way: • **ge-0/0/14** is connected to Switch 1 • **ge-0/0/18** is connected to Switch 3

Table 6: Components of the Topology for Configuring RSTP *(continued)*

Property	Settings
Switch 3	The following interfaces on Switch 3 are connected in this way: • **ge-0/0/26** is connected to Switch 1 • **ge-0/0/28** is connected to Switch 2 • **ge-0/0/24** is connected to Switch 4
Switch 4	The following interfaces on Switch 4 are connected in this way: • **ge-0/0/19** is connected to Switch 1 • **ge-0/0/23** is connected to Switch 3
VLAN names and tag IDs	**voice-vlan**, tag **10** **employee-vlan**, tag **20** **guest-vlan**, tag **30** **camera-vlan**, tag **40**

This configuration example creates a loop-free topology between four EX Series switches using RSTP.

An RSTP topology contains ports that have specific roles:

- The *root port* is responsible for forwarding data to the root bridge.
- The *alternate port* is a standby port for the root port. When a root port goes down, the alternate port becomes the active root port.
- The *designated port* forwards data to the downstream network segment or device.
- The *backup port* is a backup port for the designated port. When a designated port goes down, the backup port becomes the active designated port and starts forwarding data.

> **NOTE:** You also can create a loop-free topology between the aggregation layer and the distribution layer using redundant trunk links. For more information about configuring redundant trunk links, see *Example: Configuring Redundant Trunk Links for Faster Recovery on EX Series Switches*.

Configuring RSTP and Nonstop Bridging on Switch 1

CLI Quick Configuration

To quickly configure RSTP and nonstop bridging on Switch 1, copy the following commands and paste them into the switch terminal window:

```
[edit]
```

set vlans voice-vlan description “Voice VLAN”

set vlans voice-vlan vlan-id 10

set vlans employee-vlan description “Employee VLAN”

set vlans employee-vlan vlan-id 20

set vlans guest-vlan description “Guest VLAN”

set vlans guest-vlan vlan-id 30

set vlans camera-vlan description “Camera VLAN”

set vlans camera-vlan vlan-id 40

set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge–0/0/9 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge–0/0/11 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge–0/0/13 unit 0 family ethernet-switching port-mode trunk

set interfaces ge-0/0/9 unit 0 family ethernet-switching port-mode trunk

set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode trunk

set protocols rstp bridge-priority 16k

set protocols rstp interface ge-0/0/13.0 cost 1000

set protocols rstp interface ge-0/0/13.0 mode point-to-point

set protocols rstp interface ge-0/0/9.0 cost 1000

set protocols rstp interface ge-0/0/9.0 mode point-to-point

set protocols rstp interface ge-0/0/11.0 cost 1000

set protocols rstp interface ge-0/0/11.0 mode point-to-point

If Switch 1 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 1, copy the following commands and paste them into the switch terminal window:

set chassis redundancy graceful-switchover

set system commit synchronize

set ethernet-switching-options nonstop-bridging

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 1:

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch1# set voice-vlan description “Voice VLAN”
user@switch1# set voice-vlan vlan-id 10
user@switch1# set employee-vlan description “Employee VLAN”
user@switch1# set employee-vlan vlan-id 20
user@switch1# set guest-vlan description “Guest VLAN”
user@switch1# set guest-vlan vlan-id 30
user@switch1# set camera-vlan description “Camera VLAN”
user@switch1# set camera-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:

```
[edit interfaces]
user@switch1# set ge-0/0/13 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch1# set ge-0/0/9 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch1# set ge-0/0/11 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch1# set ge-0/0/13 unit 0 family ethernet-switching port-mode trunk
user@switch1# set ge-0/0/9 unit 0 family ethernet-switching port-mode trunk
user@switch1# set ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
```

4. Configure RSTP on the switch:

```
[edit protocols]
user@switch1# rstp bridge-priority 16k
user@switch1# rstp interface ge-0/0/13.0 cost 1000
user@switch1# rstp interface ge-0/0/13.0 mode point-to-point
user@switch1# rstp interface ge-0/0/9.0 cost 1000
user@switch1# rstp interface ge-0/0/9.0 mode point-to-point
user@switch1# rstp interface ge-0/0/11.0 cost 1000
user@switch1# rstp interface ge-0/0/11.0 mode point-to-point
```

Step-by-Step Procedure

If Switch 1 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 1:

1. Enable graceful Routing Engine switchover (GRES):

   ```
   [edit chassis redundancy]
   user@switch1# set graceful-switchover
   ```

2. Configure the switch to always synchronize configuration changes between the Routing Engines:

   ```
   [edit system]
   user@switch1# set commit synchronize
   ```

   If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

   ```
   [edit ethernet-switching-options]
   user@switch1# set nonstop-bridging
   ```

   NOTE: This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

Results

Check the results of the configuration:

```
user@switch1> show configuration
interfaces {
    ge-0/0/13 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
    ge-0/0/9 {
        unit 0 {
            family ethernet-switching {
```

```
            port-mode trunk;
            vlan {
                members [10 20 30 40];
            }
        }
    }
  }
  ge-0/0/11 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members [10 20 30 40];
        }
      }
    }
  }
}
protocols {
  rstp {
    bridge-priority 16k;
      interface ge-0/0/13.0 {
        cost 1000;
        mode point-to-point;
      }
      interface ge-0/0/9.0 {
        cost 1000;
        mode point-to-point;
      }
      interface ge-0/0/11.0 {
        cost 1000;
        mode point-to-point;
      }
    }
  }
}
vlans {
  voice-vlan {
    vlan-id 10;
  }
  employee-vlan {
    vlan-id 20;
  }
  guest-vlan {
```

```
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
system {
    commit synchronize;
}
chassis {
    redundancy {
        graceful-switchover;
    }
ethernet-switching-options {
    nonstop-bridging;
}
```

Configuring RSTP and Nonstop Bridging on Switch 2

CLI Quick Configuration

To quickly configure RSTP and nonstop bridging on Switch 2, copy the following commands and paste them into the switch terminal window:

```
[edit]
```

set vlans voice-vlan description “Voice VLAN”

set vlans voice-vlan vlan-id 10

set vlans employee-vlan description “Employee VLAN”

set vlans employee-vlan vlan-id 20

set vlans guest-vlan description “Guest VLAN”

set vlans guest-vlan vlan-id 30

set vlans camera-vlan description “Camera VLAN”

set vlans camera-vlan vlan-id 40

set interfaces ge-0/0/14 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/18 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/14 unit 0 family ethernet-switching port-mode trunk

set interfaces ge-0/0/18 unit 0 family ethernet-switching port-mode trunk

set protocols rstp bridge-priority 32k

set protocols rstp interface ge-0/0/14.0 cost 1000

set protocols rstp interface ge-0/0/14.0 mode point-to-point

set protocols rstp interface ge-0/0/18.0 cost 1000

set protocols rstp interface ge-0/0/18.0 mode point-to-point

If Switch 2 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 2, copy the following commands and paste them into the switch terminal window:

set chassis redundancy graceful-switchover

set system commit synchronize

set ethernet-switching-options nonstop-bridging

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 2:

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch2# set voice-vlan description “Voice VLAN”
user@switch2# set voice-vlan vlan-id 10
user@switch2# set employee-vlan description “Employee VLAN”
user@switch2# set employee-vlan vlan-id 20
user@switch2# set guest-vlan description “Guest VLAN”
user@switch2# set guest-vlan vlan-id 30
user@switch2# set camera-vlan vlan-description “Camera VLAN”
user@switch2# set camera-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:

```
[edit interfaces]
user@switch2# set ge-0/0/14 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch2# set ge-0/0/18 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
```

```
user@switch2# set ge-0/0/14 unit 0 family ethernet-switching port-mode trunk
user@switch2# set ge-0/0/18 unit 0 family ethernet-switching port-mode trunk
```

4. Configure RSTP on the switch:

```
[edit protocols]
user@switch2# rstp bridge-priority 32k
user@switch2# rstp interface ge-0/0/14.0 cost 1000
user@switch2# rstp interface ge-0/0/14.0 mode point-to-point
user@switch2# rstp interface ge-0/0/18.0 cost 1000
user@switch2# rstp interface ge-0/0/18.0 mode point-to-point
```

Step-by-Step Procedure

If Switch 2 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 2:

1. Enable graceful Routing Engine switchover (GRES):

```
[edit chassis redundancy]
user@switch2# set graceful-switchover
```

2. Configure the switch to always synchronize configuration changes between the Routing Engines:

```
[edit system]
user@switch2# set commit synchronize
```

   If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

```
[edit ethernet-switching-options]
user@switch2# set nonstop-bridging
```

> **NOTE:** This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

Results

Check the results of the configuration:

```
user@switch2> show configuration
interfaces {
    ge-0/0/14 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
    ge-0/0/18 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
}
protocols {
    rstp {
        bridge-priority 32k;
            interface ge-0/0/14.0 {
                cost 1000;
                mode point-to-point;
            }
            interface ge-0/0/18.0 {
                cost 1000;
                mode point-to-point;
            }
        }
    }
}
vlans {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
```

```
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
system {
    commit synchronize;
}
chassis {
    redundancy {
        graceful-switchover;
    }
ethernet-switching-options {
    nonstop-bridging;
}
```

Configuring RSTP and Nonstop Bridging on Switch 3

CLI Quick Configuration

To quickly configure RSTP and nonstop bridging on Switch 3, copy the following commands and paste them into the switch terminal window:

```
[edit]
```

set vlans voice-vlan description “Voice VLAN”

set vlans voice-vlan vlan-id 10

set vlans employee-vlan description “Employee VLAN”

set vlans employee-vlan vlan-id 20

set vlans guest-vlan description “Guest VLAN”

set vlans guest-vlan vlan-id 30

set vlans camera-vlan description “Camera VLAN”

set vlans camera-vlan vlan-id 40

set interfaces ge-0/0/26 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/28 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members [10 20 30 40]

set interfaces ge-0/0/26 unit 0 family ethernet-switching port-mode trunk

set interfaces ge-0/0/28 unit 0 family ethernet-switching port-mode trunk

set interfaces ge-0/0/24 unit 0 family ethernet-switching port-mode trunk

set protocols rstp bridge-priority 8k

set protocols rstp interface ge-0/0/26.0 cost 1000

set protocols rstp interface ge-0/0/26.0 mode point-to-point

set protocols rstp interface ge-0/0/28.0 cost 1000

set protocols rstp interface ge-0/0/28.0 mode point-to-point

set protocols rstp interface ge-0/0/24.0 cost 1000

set protocols rstp interface ge-0/0/24.0 mode point-to-point

If Switch 3 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 3, copy the following commands and paste them into the switch terminal window:

set chassis redundancy graceful-switchover

set system commit synchronize

set ethernet-switching-options nonstop-bridging

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 3:

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch3# set voice-vlan description “Voice VLAN”
user@switch3# set voice-vlan vlan-id 10
user@switch3# set employee-vlan description “Employee VLAN”
user@switch3# set employee-vlan vlan-id 20
user@switch3# set guest-vlan description “Guest VLAN”
user@switch3# set guest-vlan vlan-id 30
user@switch3# set camera-vlan description “Camera VLAN”
user@switch3# set camera-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:

```
[edit interfaces]
user@switch3# set ge-0/0/26 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch3# set ge-0/0/28 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch3# set ge-0/0/24 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch3# set ge-0/0/26 unit 0 family ethernet-switching port-mode trunk
user@switch3# set ge-0/0/28 unit 0 family ethernet-switching port-mode trunk
user@switch3# set ge-0/0/24 unit 0 family ethernet-switching port-mode trunk
```

4. Configure RSTP on the switch:

```
[edit protocols]
user@switch3# rstp bridge-priority 8k
user@switch3# rstp interface ge-0/0/26.0 cost 1000
user@switch3# rstp interface ge-0/0/26.0 mode point-to-point
user@switch3# rstp interface ge-0/0/28.0 cost 1000
user@switch3# rstp interface ge-0/0/28.0 mode point-to-point
user@switch3# rstp interface ge-0/0/24.0 cost 1000
user@switch3# rstp interface ge-0/0/24.0 mode point-to-point
```

Step-by-Step Procedure

If Switch 3 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 3:

1. Enable graceful Routing Engine switchover (GRES):

```
[edit chassis redundancy]
user@switch3# set graceful-switchover
```

2. Configure the switch to always synchronize configuration changes between the Routing Engines:

```
[edit system]
user@switch3# set commit synchronize
```

   If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

```
[edit ethernet-switching-options]
user@switch3# set nonstop-bridging
```

> **NOTE:** This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

Results

Check the results of the configuration:

```
user@switch3> show configuration
  interfaces {
    ge-0/0/26 {
      unit 0 {
        family ethernet-switching {
          port-mode trunk;
          vlan {
            members [10 20 30 40];
          }
        }
      }
    }
    ge-0/0/28 {
      unit 0 {
        family ethernet-switching {
          port-mode trunk;
          vlan {
            members [10 20 30 40];
          }
        }
      }
    }
    ge-0/0/24 {
      unit 0 {
        family ethernet-switching {
          port-mode trunk;
          vlan {
            members [10 20 30 40];
          }
        }
      }
    }
```

```
    }
}
protocols {
    rstp {
        bridge-priority 8k;
            interface ge-0/0/26.0 {
                cost 1000;
                mode point-to-point;
            }
            interface ge-0/0/28.0 {
                cost 1000;
                mode point-to-point;
            }
            interface ge-0/0/24.0 {
                cost 1000;
                mode point-to-point;
            }
        }
        bridge-priority 8k;
            }
        }
    }
}
vlans {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
system {
    commit synchronize;
}
chassis {
    redundancy {
        graceful-switchover;
    }
```

```
ethernet-switching-options {
    nonstop-bridging;
}
```

Configuring RSTP and Nonstop Bridging on Switch 4

CLI Quick Configuration

To quickly configure RSTP and nonstop bridging on Switch 4, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans voice-vlan description “Voice VLAN”
set vlans voice-vlan vlan–id 10
set vlans employee-vlan description “Employee VLAN”
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description “Guest VLAN”
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description “Camera VLAN”
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/23 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/19 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/23 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/19 unit 0 family ethernet-switching port-mode trunk
set protocols rstp bridge-priority 16k
set protocols rstp interface ge-0/0/23.0 cost 1000
set protocols rstp interface ge-0/0/23.0 mode point-to-point
set protocols rstp interface ge-0/0/19.0 cost 1000
set protocols rstp interface ge-0/0/19.0 mode point-to-point
```

If Switch 4 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 4, copy the following commands and paste them into the switch terminal window:

set chassis redundancy graceful-switchover

set system commit synchronize

set ethernet-switching-options nonstop-bridging

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 4:

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch4# set voice-vlan description “Voice VLAN”
user@switch4# set voice-vlan vlan-id 10
user@switch4# set employee-vlan description “Employee VLAN”
user@switch4# set employee-vlan vlan-id 20
user@switch4# set guest-vlan description “Guest VLAN”
user@switch4# set guest-vlan vlan-id 30
user@switch4# set camera-vlan description “Camera VLAN”
user@switch4# set camera-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:

```
[edit interfaces]
user@switch4# set ge-0/0/23 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch4# set ge-0/0/19 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch4# set ge-0/0/23 unit 0 family ethernet-switching port-mode trunk
user@switch4# set ge-0/0/19 unit 0 family ethernet-switching port-mode trunk
```

4. Configure RSTP on the switch:

```
[edit protocols]
user@switch4# rstp bridge-priority 16k
user@switch4# rstp interface all cost 1000
user@switch4# rstp interface ge-0/0/23.0 cost 1000
user@switch4# rstp interface ge-0/0/23.0 mode point-to-point
```

```
user@switch4# rstp interface ge-0/0/19.0 cost 1000
user@switch4# rstp interface ge-0/0/19.0 mode point-to-point
```

Step-by-Step Procedure

If Switch 4 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 4:

1. Enable graceful Routing Engine switchover (GRES):

   ```
   [edit chassis redundancy]
   user@switch4# set graceful-switchover
   ```

2. Configure the switch to always synchronize configuration changes between the Routing Engines:

   ```
   [edit system]
   user@switch4# set commit synchronize
   ```

   If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

   ```
   [edit ethernet-switching-options]
   user@switch4# set nonstop-bridging
   ```

   NOTE: This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

Results

Check the results of the configuration:

```
user@switch4> show configuration
interfaces {
    ge-0/0/23 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
```

```
        }
    }
    ge-0/0/19 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
}
protocols {
    rstp {
        bridge-priority 16k;
            interface ge-0/0/23.0 {
                cost 1000;
                mode point-to-point;
            }
            interface ge-0/0/19.0 {
                cost 1000;
                mode point-to-point;
            }
        }
    }
}
vlans {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
system {
    commit synchronize;
}
```

```
chassis {
    redundancy {
        graceful-switchover;
    }
ethernet-switching-options {
    nonstop-bridging;
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks on both Routing Engines:

Verifying RSTP Configuration on Switch 1

Purpose

Verify the RSTP configuration on Switch 1.

Action

Use the operational mode command:

```
user@switch1>  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-0/0/13.0    128:526      128:526  16384.0019e25040e0      1000  BLK    ALT
ge-0/0/9.0     128:522      128:522  32768.0019e2503d20      1000  BLK    ALT
ge-0/0/11.0    128:524      128:524   8192.0019e25051e0      1000  FWD    ROOT
```

Meaning

The operational mode command **show spanning-tree interface** shows that **ge-0/0/13.0** is in a forwarding state. The other interfaces on Switch 1 are blocking.

Verifying RSTP Configuration on Switch 2

Purpose

Use this procedure to verify the RSTP configuration on both Switch 2 Routing Engines.

Action

Use the operational mode command:

```
user@switch2>  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-0/0/14.0     128:527      128:527  32768.0019e2503d20      1000  FWD    DESG
ge-0/0/18.0     128:529      128:529   8192.0019e25051e0      1000  FWD    ROOT
```

Meaning

The operational mode command **show spanning-tree interface** shows that **ge-0/0/18.0** is in a forwarding state and is the root port.

Verifying RSTP Configuration on Switch 3

Purpose

Use this procedure to verify the RSTP configuration on both Switch 3 Routing Engines.

Action

Use the operational mode commands:

```
user@switch3>  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-0/0/26.0     128:539      128:539   8192.0019e25051e0      1000  FWD    DESG
ge-0/0/28.0     128:541      128:541   8192.0019e25051e0      1000  FWD    DESG
ge-0/0/24.0     128:537      128:537   8192.0019e25051e0      1000  FWD    DESG
```

Meaning

The operational mode command **show spanning-tree interface** shows that no interface is the root interface.

Verifying RSTP Configuration on Switch 4

Purpose

Use this procedure to verify the RSTP configuration on both Switch 4 Routing Engines.

Action

Use the operational mode commands:

```
user@switch4>  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-0/0/23.0    128:536      128:536   8192.0019e25051e0      1000  FWD    ROOT
ge-0/0/19.0    128:532      128:532   16384.0019e25040e0     1000  FWD    DESG
```

Meaning

The operational mode command **show spanning-tree interface** shows that interface **ge-0/0/23.0** is the root interface and forwarding.

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 *Using the Enhanced Layer 2 Software CLI*.

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.

SEE ALSO

Release History Table

Release	Description
15.1	Starting with Junos OS Release 15.1 for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can configure spanning tree parameters globally on all spanning tree interfaces.

RELATED DOCUMENTATION

Using the Enhanced Layer 2 Software CLI

Example: Configuring Redundant Trunk Links for Faster Recovery on Devices with ELS Support

Configuring MSTP Protocol

IN THIS SECTION

Multiple Spanning Tree Protocol (MSTP) maps multiple VLANs into a spanning tree instance, with each instance having a spanning tree topology independent of other spanning tree instances.

Understanding MSTP

IN THIS SECTION

Ethernet networks are susceptible to broadcast storms if loops are introduced. However, an Ethernet network needs to include loops because they provide redundant paths in case of a link failure. Spanning-tree protocols address both of these issues because they provide link redundancy while simultaneously preventing undesirable loops.

Spanning-tree protocols intelligently avoid loops in a network by creating a tree topology (spanning tree) of the entire bridged network with only one available path between the tree root and a leaf. All other paths are forced into a standby state. The tree *root* is a switch within the network elected by the STA (spanning-tree algorithm) to use when computing the best path between bridges throughout the network and the root bridge. Frames travel through the network to their destination– a *leaf*. A tree *branch* is a network segment, or link, between bridges. Switches that forward frames through an STP spanning-tree are called *designated bridges*.

Juniper Networks devices provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP). This topic explains MSTP.

> **NOTE:** If you are using Junos OS for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can force the original IEEE 802.1D Spanning Tree Protocol (STP) version to run in place of RSTP or VSTP by setting **force-version**.

This topic describes:

Benefits of MSTP

MSTP has the following benefits:

- Multiple Spanning Tree Protocol works with most VLANs.
- MSTP supports multiple instances on a single physical interface.
- On MX and ACX routers, you can configure RSTP, MSTP, and VSTP instance interfaces as edge ports.

MSTP Maps Multiple VLANs

MSTP is an extension of RSTP that maps multiple independent spanning-tree instances onto one physical topology. Each spanning-tree instance (STI) includes one or more VLANs. Unlike in STP and RSTP configurations, a port might belong to multiple VLANs and be dynamically blocked in one spanning-tree instance, but forwarding in another. This behavior significantly improves network resource utilization by load-balancing across the network and maintaining switch CPU loads at moderate levels. MSTP also leverages the fast reconvergence time of RSTP when a network, switch, or port failure occurs within a spanning-tree instance.

MSTP creates a common and internal spanning tree (CIST) to interconnect and manage all MSTP regions and even individual devices that run RSTP or STP, which are recognized as distinct spanning-tree regions by MSTP. The CIST views each MSTP region as a virtual bridge, regardless of the actual number of devices participating in the MSTP region, and enables multiple spanning-tree instances (MSTIs) to link to other regions. The CIST is a single topology that connects all switches (STP, RSTP, and MSTP devices) through an active topology, ensuring connectivity between LANs and devices within a bridged network. This functionality provided by MSTP enables you to better utilize network resources while remaining backward-compatible with older network devices.

Configuring MSTP Regions

When enabling MSTP, you define one or more MSTP regions. An MSTP region defines a logical domain where multiple spanning-tree instances (MSTIs) can be administered independently of MSTIs in other regions, setting the boundary for bridge protocol data units (BPDUs) sent by one MSTI. An MSTP region is a group of switches that is defined by three parameters:

- Region name—User-defined alphanumeric name for the region.
- Revision level—User-defined value that identifies the region.
- Mapping table—Numerical digest of VLAN-to-instance mappings.

An MSTP region can support up to 64 MSTIs,, and each MSTI can support from 1 to 4094 VLANs. When you define a region, MSTP automatically creates an internal spanning-tree instance (IST instance 0) that provides the root switch for the region and includes all currently configured VLANs that are not specifically assigned to a user-defined MSTI. An MSTI includes all static VLANs that you specifically add to it. The switch places any dynamically created VLANs in the IST instance by default, unless you explicitly map them to another MSTI. Once you assign a VLAN to a user-defined MSTI, the switch removes the VLAN from the IST instance.

Selecting a Spanning Tree Protocol

The default factory configuration is RSTP, a faster version of STP. To determine which spanning-tree protocol is best for your situation, see Table 7 on page 100 below.

Table 7: Selecting a Spanning Tree Protocol

Protocol	Advantages	Disadvantages
RSTP	• Rapid Spanning Tree Protocol is the default switch configuration and is recommended for most network configurations because it converges more quickly than STP after a failure. • Voice and video work better with RSTP than they do with STP. • RSTP is backward compatible with STP; therefore, switches do not all have to run RSTP.	• RSTP does not work with 802.1D 1998 bridges. • RSTP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic.
STP	• Spanning Tree Protocol works with 802.1D 1998 bridges. • RSTP is backward compatible with STP; therefore, switches do not all have to run STP.	• STP is slower than RSTP. • STP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic. • If you are using Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can force the original IEEE 802.1D Spanning Tree Protocol (STP) version to run in place of RSTP or VSTP by setting force-version. However, the CLI does not include **[edit protocols stp].**
MSTP	• Multiple Spanning Tree Protocol works with most VLANs. • RSTP and STP are recognized as distinct spanning-tree regions by MSTP.	• Some protocols require compatibility that is not provided by MSTP. In this case, use VSTP. • MSTP uses more CPU than RSTP and does not converge as fast as RSTP.
VSTP	• VLAN Spanning Tree Protocol works with VLANs that require device compatibility. • VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a switch.	• With VSTP there can be only STP instance per VLAN, whereas MSTP lets you combine multiple VLANs in one instance. • VSTP supports a limited number of ports compared to RSTP. • VSTP uses more CPU than RSTP and does not converge as fast as RSTP. • Having a large number of VSTP and RSTP instances can cause continuous changes in the topology. Ensure to check the scale limits before configuring large number of VSTP instances.

SEE ALSO

Understanding RSTP | 44

Understanding VSTP

Configuring MSTP on Switches

You can configure the Multiple Spanning Tree Protocol (MSTP) under **[edit protocols].**

To configure the Multiple Spanning Tree Protocol:

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

   ```
   [edit]
   user@switch@ edit ... protocols mstp
   ```

2. Configure the interfaces that participate in the MSTP instance for all interfaces at one time, or for configured interface ranges, or for specific interfaces individually:

   - Enable MSTP on all the interfaces at one time, for switches that support this option (most switches):

     ```
     [edit ... protocols mstp]
     user@switch# set interface all
     ```

     > **NOTE:** You cannot disable MSTP on all the interfaces with one command. See the configuration steps for configuring MSTP on specific interfaces later in this topic for how to disable MSTP on interfaces individually.

     For QFX5100 switches, which do not support the **interface all** option, you must configure interface ranges for the applicable interfaces on which you want to enable MSTP, and then issue the **set protocols mstp interface *name*** command for each *name* that you have configured as an interface range (described next).

   - Enable MSTP on a range of interfaces, for switches such as QFX5100 switches that do not support the **interface all** option:

     a. Configure interface ranges using the **interface-range** statement at the **[edit interfaces]** hierarchy level for the applicable interfaces on which you want to enable MSTP:

        ```
        [edit interfaces]
        user@switch# set interface-range interface-range-name member-range interface-name1 to
        interface-name2
        ```

b. Enable MSTP for each configured interface range *interface-range-name* at the **[edit ... protocols mstp]** hierarchy level:

```
[edit ... protocols mstp]
user@switch# set interface interface-range-name
```

- Configure a specific interface individually to enable MSTP and various MSTP options on that interface, or to disable MSTP on that interface:

a. Enable MSTP on the specified interface:

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

b. Configure the interface priority:

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

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

```
[edit ... protocols mstp interface interface-name]
user@switch# 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@switch# 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 nonedge port

f. (Optional) Disable MSTP on a specific interface:

```
[edit protocols mstp interface interface-name]
user@switch# set disable
```

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 281.

3. Configure the bridge priority

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

For more information, see "Understanding Bridge Priority for Election of Root Bridge and Designated Bridge" on page 258.

4. Configure hello BPDU timers.

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

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

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

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

5. (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@switch# set forward-delay seconds
```

6. Configure MSTP-specific options.

   a. Configure the MSTP region configuration name:

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

   b. Configure the MSTP revision level:

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

SEE ALSO

Configuring MSTP Instances on a Physical Interface | 109

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 281.

4. Configure the bridge priority:

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

For more information, see "Understanding Bridge Priority for Election of Root Bridge and Designated Bridge" on page 258.

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.
      }
    }
}
```

Configuring MSTP 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 Multiple Spanning Tree Protocol" on page 105.

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 "Understanding Bridge Priority for Election of Root Bridge and Designated Bridge" on page 258.

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;
            }
        }
    }
}
```

SEE ALSO

Example: Configuring Network Regions for VLANs with MSTP on Switches

IN THIS SECTION

NOTE: This example uses Junos OS for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. The example also describes the configuration statement differences that can be substituted in the same configuration on EX Series switches that do not support ELS.

Multiple Spanning Tree Protocol (MSTP) is used to create a loop-free topology in networks using multiple spanning-tree regions in which each region contains multiple spanning-tree instances (MSTIs). MSTIs provide different paths for different VLANs. This functionality facilitates better load sharing across redundant links.

Up to 64 MSTIs can be created for an EX Series switch, and each MSTI can support up to 4094 VLANs.

This example describes how to configure MSTP on four EX Series switches:

Requirements

This example uses the following software and hardware components:

- Junos OS Release 13.2X50-D10 or later for EX Series or QFX Series switches
- Four QFX Series switches

Before you configure the switches for MSTP, be sure you have:

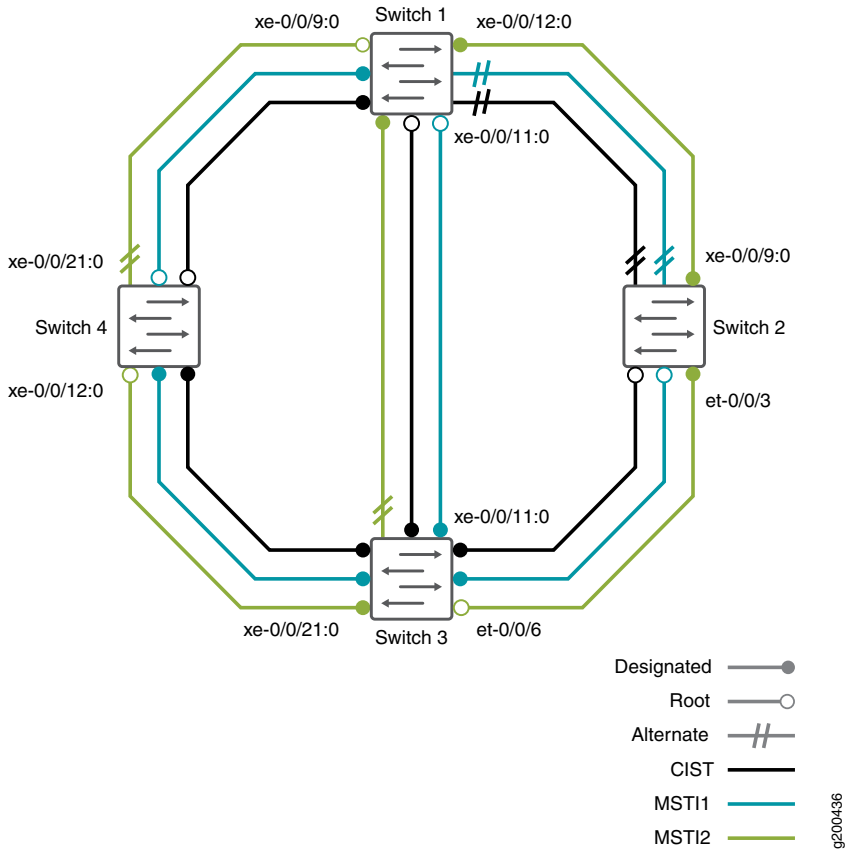
- Installed and connected the four switches. See the hardware documentation for your switch.

- Performed the initial software configuration on all switches. See *Connecting and Configuring an EX Series Switch (CLI Procedure)* or *Connecting and Configuring an EX Series Switch (J-Web Procedure)*.

Overview and Topology

When the number of VLANs grows in a network, MSTP provides an efficient way of creating a loop-free topology by using MSTIs. Each MSTI in the spanning-tree domain maintains its own tree. Each tree can be mapped to different links, utilizing bandwidth that would be unavailable to a single tree. MSTIs reduce the demand on system resources.

Figure 3: Network Topology for MSTP



The interfaces shown in Figure 3 on page 112 will be configured for MSTP.

Table 8: Components of the Topology for Configuring MSTP on EX Series Switches

Property	Settings
Switch 1	The following interfaces on Switch 1 are connected in this way: • **xe-0/0/12:0** is connected to Switch 2 • **xe-0/0/9:0** is connected to Switch 4 • **xe-0/0/11:0** is connected to Switch 3
Switch 2	The following interfaces on Switch 2 are connected in this way: • **xe-0/0/9:0** is connected to Switch 1 • **et-0/0/3** is connected to Switch 3
Switch 3	The following interfaces on Switch 3 are connected in this way: • **xe-0/0/11:0** is connected to Switch 1 • **et-0/0/6** is connected to Switch 2 • **xe-0/0/21:0** is connected to Switch 4
Switch 4	The following interfaces on Switch 4 are connected in this way: • **xe-0/0/21:0** is connected to Switch 1 • **xe-0/0/12:0** is connected to Switch 3
VLAN names and tag IDs	**voice-vlan**, tag **10** **employee-vlan**, tag **20** **guest-vlan**, tag **30** **camera-vlan**, tag **40**
MSTIs	**1** **2**
MSTI region	**region1**

The topology in Figure 3 on page 112 shows a common and internal spanning tree (CIST). The CIST is a single spanning tree connecting all devices in the network. The switch with the lowest bridge priority is elected as the root bridge of the CIST. You can control the election of the root bridge by configuring the bridge priority. Switch 3 is the root bridge of the CIST.

The ports in an MSTP topology have specific roles:

- The *root port* is responsible for forwarding data to the root bridge.
- The *alternate port* is a standby port for the root port. When a root port goes down, the alternate port becomes the active root port.

- The *designated port* forwards data to the downstream network segment or device.
- The *backup port* becomes the active designated port and starts forwarding data when the designated port goes down.

In this example, one MSTP region contains Switch 1, Switch 2, Switch 3, and Switch 4. Within the region, four VLANs are created:

- **voice-vlan** supports voice traffic and has the VLAN tag identifier of **10**.
- **employee-vlan** supports data traffic and has the VLAN tag identifier of **20**.
- **guest-vlan** supports guest VLAN traffic (for supplicants that fail authentication) and has the VLAN tag identifier of **30**.
- **camera-vlan** supports video traffic and has the VLAN tag identifier of **40**.

The VLANs are associated with specific interfaces on each of the four switches. Two MSTIs, **1** and **2**, are then associated with the VLAN tag identifiers, and some MSTP parameters, such as cost, are configured on each switch.

Configuring MSTP on Switch 1

CLI Quick Configuration

To quickly configure interfaces and MSTP on Switch 1, for ELS switches, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans voice-vlan description “Voice VLAN”
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description “Employee VLAN”
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description “Guest VLAN”
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description “Camera VLAN”
set vlans camera-vlan vlan-id 40
set interfaces xe-0/0/9:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces xe-0/0/12:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces xe-0/0/11:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces xe-0/0/9:0 unit 0 family ethernet-switching interface-mode trunk
set interfaces xe-0/0/12:0 unit 0 family ethernet-switching interface-mode trunk
set interfaces xe-0/0/11:0 unit 0 family ethernet-switching interface-mode trunk
set protocols mstp configuration-name region1
set protocols mstp bridge-priority 16k
set protocols mstp interface xe-0/0/9:0 cost 1000
set protocols mstp interface xe-0/0/9:0 mode point-to-point
set protocols mstp interface xe-0/0/12:0 cost 1000
```

```
set protocols mstp interface xe-0/0/12:0 mode point-to-point
set protocols mstp interface xe-0/0/11:0 cost 1000
set protocols mstp interface xe-0/0/11:0 mode point-to-point
set protocols mstp msti 1 bridge-priority 16k
set protocols mstp msti 1 vlan [10 20]
set protocols mstp msti 1 interface xe-0/0/11:0 cost 1000
set protocols mstp msti 2 bridge-priority 8k
set protocols mstp msti 2 vlan [30 40]
```

NOTE: For non-ELS switches, instead of the following command used above for ELS switches that sets an interface into trunk mode using the **interface-mode** statement:

set interfaces *interface-name* unit 0 family ethernet-switching interface-mode trunk

substitute the following command for those lines in the configuration, which uses the non-ELS **port-mode** statement to set an interface into trunk mode:

set interfaces *interface-name* unit 0 family ethernet-switching port-mode trunk

Step-by-Step Procedure

To configure interfaces and MSTP on Switch 1:

> **NOTE:** Starting with Junos OS Release 15.1 for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can configure spanning tree parameters globally on all spanning tree interfaces. See "Configuring MSTP on Switches" on page 101 for additional information.

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch1# set voice-vlan description "Voice VLAN"
user@switch1# set voice-vlan vlan-id 10
user@switch1# set employee-vlan description "Employee VLAN"
user@switch1# set employee-vlan vlan-id 20
user@switch1# set guest-vlan description "Guest VLAN"
user@switch1# set guest-vlan vlan-id 30
user@switch1# set camera-vlan description "Camera VLAN"
user@switch1# set guest-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet Switching protocol:

```
[edit interfaces]
user@switch1# set xe-0/0/9:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch1# set xe-0/0/12:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch1# set xe-0/0/11:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch1# set xe-0/0/9:0 unit 0 family ethernet-switching interface-mode trunk
user@switch1# set xe-0/0/12:0 unit 0 family ethernet-switching interface-mode trunk
user@switch1# set xe-0/0/11:0 unit 0 family ethernet-switching interface-mode trunk
```

NOTE: For non-ELS switches, instead of the following command used above for ELS switches that sets an interface into trunk mode using the **interface-mode** statement:

set interfaces *interface-name* unit 0 family ethernet-switching interface-mode trunk

substitute the following command for those lines in the configuration, which uses the non-ELS **port-mode** statement to set an interface into trunk mode:

set interfaces *interface-name* unit 0 family ethernet-switching port-mode trunk

4. Configure MSTP on the switch, including the two MSTIs:

```
[edit protocols]
user@switch1# mstp configuration-name region1
user@switch1# mstp bridge-priority 16k
user@switch1# mstp interface xe-0/0/9:0 cost 1000
user@switch1# mstp interface xe-0/0/9:0 mode point-to-point
user@switch1# mstp interface xe-0/0/12:0 cost 1000
user@switch1# mstp interface xe-0/0/12:0 mode point-to-point
user@switch1# mstp interface xe-0/0/11:0 cost 1000
user@switch1# mstp interface xe-0/0/11:0 mode point-to-point
user@switch1# mstp msti 1 bridge-priority 16k
user@switch1# mstp msti 1 vlan [10 20]
user@switch1# mstp msti 1 interface xe-0/0/11:0 cost 1000
user@switch1# mstp msti 2 bridge-priority 8k
user@switch1# mstp msti 2 vlan [30 40]
```

Results

Check the results of the configuration:

```
user@switch1> show configuration
interfaces {
    xe-0/0/9:0 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members 10;
```

```
                members 20;
                members 30;
                members 40;
            }
        }
    }
    xe-0/0/12:0 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members 10;
                    members 20;
                    members 30;
                    members 40;
                }
            }
        }
    }
    xe-0/0/11:0 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members 10;
                    members 20;
                    members 30;
                    members 40;
                }
            }
        }
    }
}
protocols {
    mstp {
        configuration-name region1;
    bridge-priority 16k;
        interface xe-0/0/9:0 {
            cost 1000;
            mode point-to-point;
        }
        interface xe-0/0/12:0 {
            cost 1000;
```

```
            mode point-to-point;
        }
        interface xe-0/0/11:0 {
            cost 1000;
            mode point-to-point;
        }
    msti 1 {
        bridge-priority 16k;
        vlan [ 10 20];
        interface xe-0/0/11:0 {
            cost 1000;
        }
    }
    msti 2 {
        bridge-priority 8k;
        vlan [ 30 40 ];
    }
}
vlans {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
```

Configuring MSTP on Switch 2

CLI Quick Configuration

To quickly configure interfaces and MSTP on Switch 2, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans voice-vlan description “Voice VLAN”
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description “Employee VLAN”
```

```
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description “Guest VLAN”
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description “Camera VLAN”
set vlans camera-vlan vlan-id 40
set interfaces xe-0/0/9:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces et-0/0/3 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces xe-0/0/9:0 unit 0 family ethernet-switching interface-mode trunk
set interfaces et-0/0/3 unit 0 family ethernet-switching interface-mode trunk
set protocols mstp configuration-name region1
set protocols mstp bridge-priority 32k
set protocols mstp interface xe-0/0/9:0 cost 1000
set protocols mstp interface xe-0/0/9:0 mode point-to-point
set protocols mstp interface et-0/0/3 cost 1000
set protocols mstp interface et-0/0/3 mode point-to-point
set protocols mstp msti 1 bridge-priority 32k
set protocols mstp msti 1 vlan [10 20]
set protocols mstp msti 2 bridge-priority 4k
set protocols mstp msti 2 vlan [30 40]
```

NOTE: For non-ELS switches, instead of the following command used above for ELS switches that sets an interface into trunk mode using the **interface-mode** statement:

set interfaces *interface-name* unit 0 family ethernet-switching interface-mode trunk

substitute the following command for those lines in the configuration, which uses the non-ELS **port-mode** statement to set an interface into trunk mode:

set interfaces *interface-name* unit 0 family ethernet-switching port-mode trunk

Step-by-Step Procedure

To configure interfaces and MSTP on Switch 2:

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch2# set voice-vlan description “Voice VLAN”
user@switch2# set voice-vlan vlan-id 10
user@switch2# set employee-vlan description “Employee VLAN”
user@switch2# set employee-vlan vlan-id 20
user@switch2# set guest-vlan description “Guest VLAN”
user@switch2# set guest-vlan vlan-id 30
user@switch2# set camera-vlan vlan-description “Camera VLAN”
user@switch2# set guest-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet Switching protocol:

```
[edit interfaces]
user@switch2# set xe-0/0/9:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch2# set et-0/0/3 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch2# set xe-0/0/9:0 unit 0 family ethernet-switching interface-mode trunk
user@switch2# set et-0/0/3 unit 0 family ethernet-switching interface-mode trunk
```

> **NOTE:** For non-ELS switches, instead of the following command used above for ELS switches that sets an interface into trunk mode using the **interface-mode** statement:
>
> **set interfaces *interface-name* unit 0 family ethernet-switching interface-mode trunk**
>
> substitute the following command for those lines in the configuration, which uses the non-ELS **port-mode** statement to set an interface into trunk mode:
>
> **set interfaces *interface-name* unit 0 family ethernet-switching port-mode trunk**

4. Configure MSTP on the switch, including the two MSTIs:

```
[edit protocols]
user@switch2# mstp configuration-name region1
user@switch2# mstp bridge-priority 32k
```

```
user@switch2# mstp interface xe-0/0/9:0 cost 1000
user@switch2# mstp interface xe-0/0/9:0 mode point-to-point
user@switch2# mstp interface et-0/0/3 cost 1000
user@switch2# mstp interface et-0/0/3 mode point-to-point
user@switch2# mstp msti 1 bridge-priority 32k
user@switch2# mstp msti 1 vlan [10 20]
user@switch2# mstp msti 2 bridge-priority 4k
user@switch2# mstp msti 2 vlan [30 40]
```

Results

Check the results of the configuration:

```
user@switch2> show configuration
interfaces {
    xe-0/0/9:0 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members 10;
                    members 20;
                    members 30;
                    members 40;
                }
            }
        }
    }
    et-0/0/3 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members 10;
                    members 20;
                    members 30;
                    members 40;
                }
            }
        }
    }
}
protocols {
```

```
    mstp {
        configuration-name region1;
        bridge-priority 32k;
        interface xe-0/0/9:0 {
            cost 1000;
            mode point-to-point;
        }
        interface et-0/0/3 {
            cost 1000;
            mode point-to-point;
        }
        msti 1 {
            bridge-priority 32k;
            vlan [10 20];
        }
        msti 2 {
            bridge-priority 4k;
            vlan [30 40];
        }
    }
}
vlans {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
```

Configuring MSTP on Switch 3

CLI Quick Configuration

To quickly configure interfaces and MSTP on Switch 3, copy the following commands and paste them into the switch terminal window:

```
[edit]
```

```
set vlans voice-vlan description “Voice VLAN”
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description “Employee VLAN”
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description “Guest VLAN”
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description “Camera VLAN”
set vlans camera-vlan vlan—id 40
set interfaces xe-0/0/11:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces et-0/0/6 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces xe-0/0/21:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces xe-0/0/11:0 unit 0 family ethernet-switching interface-mode trunk
set interfaces et-0/0/6 unit 0 family ethernet-switching interface-mode trunk
set interfaces xe-0/0/21:0 unit 0 family ethernet-switching interface-mode trunk
set protocols mstp configuration-name region1
set protocols mstp bridge-priority 8k
set protocols mstp interface xe-0/0/11:0 cost 1000
set protocols mstp interface xe-0/0/11:0 mode point-to-point
set protocols mstp interface et-0/0/6 cost 1000
set protocols mstp interface et-0/0/6 mode point-to-point
set protocols mstp interface xe-0/0/21:0 cost 1000
set protocols mstp interface xe-0/0/21:0 mode point-to-point
set protocols mstp msti 1 bridge-priority 4k
set protocols mstp msti 1 vlan [10 20]
set protocols mstp msti 2 bridge-priority 16k
set protocols mstp msti 2 vlan [30 40]
```

NOTE: For non-ELS switches, instead of the following command used above for ELS switches that sets an interface into trunk mode using the **interface-mode** statement:

set interfaces *interface-name* unit 0 family ethernet-switching interface-mode trunk

substitute the following command for those lines in the configuration, which uses the non-ELS **port-mode** statement to set an interface into trunk mode:

set interfaces *interface-name* unit 0 family ethernet-switching port-mode trunk

Step-by-Step Procedure

To configure interfaces and MSTP on Switch 3:

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch3# set voice-vlan description “Voice VLAN”
user@switch3# set voice-vlan vlan-id 10
user@switch3# set employee-vlan description “Employee VLAN”
user@switch3# set employee-vlan vlan-id 20
user@switch3# set guest-vlan description “Guest VLAN”
user@switch3# set guest-vlan vlan-id 30
user@switch3# set camera-vlan description “Camera VLAN”
user@switch3# set guest-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet Switching protocol:

```
[edit interfaces]
user@switch3# set xe-0/0/11:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch3# set et-0/0/6 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch3# set xe-0/0/21:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch3# set xe-0/0/11:0 unit 0 family ethernet-switching interface-mode trunk
user@switch3# set et-0/0/6 unit 0 family ethernet-switching interface-mode trunk
user@switch3# set xe-0/0/21:0 unit 0 family ethernet-switching interface-mode trunk
```

> **NOTE:** For non-ELS switches, instead of the following command used above for ELS switches that sets an interface into trunk mode using the **interface-mode** statement:
>
> **set interfaces *interface-name* unit 0 family ethernet-switching interface-mode trunk**
>
> substitute the following command for those lines in the configuration, which uses the non-ELS **port-mode** statement to set an interface into trunk mode:
>
> **set interfaces *interface-name* unit 0 family ethernet-switching port-mode trunk**

4. Configure MSTP on the switch, including the two MSTIs:

```
[edit protocols]
```

```
user@switch3# mstp configuration-name region1
user@switch3# mstp bridge-priority 8k
user@switch3# mstp interface xe-0/0/11:0 cost 1000
user@switch3# mstp interface xe-0/0/11:0 mode point-to-point
user@switch3# mstp interface et-0/0/6 cost 1000
user@switch3# mstp interface et-0/0/6 mode point-to-point
user@switch3# mstp interface xe-0/0/21:0 cost 1000
user@switch3# mstp interface xe-0/0/21:0 mode point-to-point
user@switch3# mstp msti 1 bridge-priority 4k
user@switch3# mstp msti 1 vlan [10 20]
user@switch3# mstp msti 2 bridge-priority 16k
user@switch3# mstp msti 2 vlan [30 40]
```

Results

Check the results of the configuration:

```
user@switch3> show configuration
  interfaces {
    xe-0/0/11:0 {
      unit 0 {
        family ethernet-switching {
          interface-mode trunk;
          vlan {
            members 10;
            members 20;
            members 30;
            members 40;
          }
        }
      }
    }
    et-0/0/6 {
      unit 0 {
        family ethernet-switching {
          interface-mode trunk;
          vlan {
            members 10;
            members 20;
            members 30;
            members 40;
          }
```

```
            }
          }
        }
        xe-0/0/21:0 {
          unit 0 {
            family ethernet-switching {
              interface-mode trunk;
              vlan {
                members 10;
                members 20;
                members 30;
                members 40;
              }
            }
          }
        }
    }
}
protocols {
    mstp {
        configuration-name region1;
        bridge-priority 8k;
        interface xe-0/0/11:0 {
          cost 1000;
          mode point-to-point;
        }
        interface et-0/0/6 {
          cost 1000;
          mode point-to-point;
        }
        interface xe-0/0/21:0 {
          cost 1000;
          mode point-to-point;
        }
        msti 1 {
          bridge-priority 4k;
          vlan [10 20];
        }
        msti 2 {
          bridge-priority 16k;
          vlan [30 40];
        }
    }
}
```

```
vlans {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
```

Configuring MSTP on Switch 4

CLI Quick Configuration

To quickly configure interfaces and MSTP on Switch 4, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans voice-vlan description “Voice VLAN”
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description “Employee VLAN”
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description “Guest VLAN”
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description “Camera VLAN”
set vlans camera-vlan vlan-id 40
set interfaces xe-0/0/12:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces xe-0/0/21:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces xe-0/0/12:0 unit 0 family ethernet-switching interface-mode trunk
set interfaces xe-0/0/21:0 unit 0 family ethernet-switching interface-mode trunk
set protocols mstp configuration-name region1
set protocols mstp bridge-priority 16k
set protocols mstp interface xe-0/0/12:0 cost 1000
set protocols mstp interface xe-0/0/12:0 mode point-to-point
set protocols mstp interface xe-0/0/21:0 cost 1000
set protocols mstp interface xe-0/0/21:0 mode point-to-point
set protocols mstp msti 1 bridge-priority 16k
set protocols mstp msti 1 vlan [10 20]
set protocols mstp msti 2 bridge-priority 32k
```

```
set protocols mstp msti 2 vlan [30 40]
```

NOTE: For non-ELS switches, instead of the following command used above for ELS switches that sets an interface into trunk mode using the **interface-mode** statement:

set interfaces *interface-name* unit 0 family ethernet-switching interface-mode trunk

substitute the following command for those lines in the configuration, which uses the non-ELS **port-mode** statement to set an interface into trunk mode:

set interfaces *interface-name* unit 0 family ethernet-switching port-mode trunk

Step-by-Step Procedure

To configure interfaces and MSTP on Switch 4:

1. Configure the VLANs **voice-vlan**, **employee-vlan**, **guest-vlan**, and **camera-vlan**:

```
[edit vlans]
user@switch4# set voice-vlan description “Voice VLAN”
user@switch4# set voice-vlan vlan-id 10
user@switch4# set employee-vlan description “Employee VLAN”
user@switch4# set employee-vlan vlan-id 20
user@switch4# set guest-vlan description “Guest VLAN”
user@switch4# set guest-vlan vlan-id 30
user@switch4# set camera-vlan description “Camera VLAN”
user@switch4# set guest-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet Switching protocol:

```
[edit interfaces]
user@switch4# set xe-0/0/12:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch4# set xe-0/0/21:0 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch4# set xe-0/0/12:0 unit 0 family ethernet-switching interface-mode trunk
user@switch4# set xe-0/0/21:0 unit 0 family ethernet-switching interface-mode trunk
```

NOTE: For non-ELS switches, instead of the following command used above for ELS switches that sets an interface into trunk mode using the **interface-mode** statement:

set interfaces *interface-name* unit 0 family ethernet-switching interface-mode trunk

substitute the following command for those lines in the configuration, which uses the non-ELS **port-mode** statement to set an interface into trunk mode:

set interfaces *interface-name* unit 0 family ethernet-switching port-mode trunk

4. Configure MSTP on the switch, including the two MSTIs:

```
[edit protocols]
user@switch4# mstp configuration-name region1
user@switch4# mstp bridge-priority 16k
user@switch4# mstp interface xe-0/0/12:0 cost 1000
user@switch4# mstp interface xe-0/0/12:0 mode point-to-point
user@switch4# mstp interface xe-0/0/21:0 cost 1000
user@switch4# mstp interface xe-0/0/21:0 mode point-to-point
user@switch4# mstp msti 1 bridge-priority 16k
user@switch4# mstp msti 1 vlan [10 20]
user@switch4# mstp msti 2 bridge-priority 32k
user@switch4# mstp msti 2 vlan [30 40]
```

Results

Check the results of the configuration:

```
user@switch4> show configuration
interfaces {
    xe-0/0/12:0 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members 10;
                    members 20;
                    members 30;
                    members 40;
```

```
            }
          }
        }
      }
      xe-0/0/21:0 {
        unit 0 {
          family ethernet-switching {
            interface-mode trunk;
            vlan {
              members 10;
              members 20;
              members 30;
              members 40;
            }
          }
        }
      }
    }
    protocols {
      mstp {
        configuration-name region1;
        bridge-priority 16k;
        interface xe-0/0/12:0 {
          cost 1000;
          mode point-to-point;
        }
        interface xe-0/0/21:0 {
          cost 1000;
          mode point-to-point;
        }
        msti 1 {
          bridge-priority 16k;
          vlan [10 20];
        }
        msti 2 {
          bridge-priority 32k;
          vlan [30 40];
        }
      }
    }
    vlans {
      voice-vlan {
        vlan-id 10;
      }
```

```
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Verifying MSTP Configuration on Switch 1

Purpose

Verify the MSTP configuration on Switch 1.

Action

Issue the operational mode commands **show spanning-tree interface** and **show spanning-tree bridge**:

```
user@switch1> show spanning-tree interface
```

```
Spanning tree interface parameters for instance 0

Interface                   Port ID    Designated         Designated         Port
   State  Role
                                        port ID           bridge ID          Cost
xe-0/0/9:0                128:1010     128:1010  16384.544b8c432703         1000
```

```
   FWD    DESG
xe-0/0/12:0              128:1011     128:1011  16384.40a677792303         1000
   BLK    ALT
xe-0/0/11:0              128:1012     128:1010   8192.544b8c44c103         1000
   FWD    ROOT

Spanning tree interface parameters for instance 1

Interface                  Port ID    Designated         Designated         Port
   State  Role
                                       port ID           bridge ID          Cost
xe-0/0/9:0               128:1010     128:1010  16385.544b8c432703         1000
   FWD    DESG
xe-0/0/12:0              128:1011     128:1011  16385.40a677792303         1000
   BLK    ALT
xe-0/0/11:0              128:1012     128:1010   4097.544b8c44c103         1000
   FWD    ROOT

Spanning tree interface parameters for instance 2

Interface                  Port ID    Designated         Designated         Port
   State  Role
                                       port ID           bridge ID          Cost
xe-0/0/9:0               128:1010     128:1012   4098.88a25e8c7603         1000
   FWD    ROOT
xe-0/0/12:0              128:1011     128:1011   8194.544b8c432703         1000
   FWD    DESG
xe-0/0/11:0              128:1012     128:1012   8194.544b8c432703         1000
   FWD    DESG
```

user@switch1> **show spanning-tree bridge**

```
STP bridge parameters
Routing instance name              : GLOBAL
Context ID                         : 0
Enabled protocol                   : MSTP

STP bridge parameters for CIST
  Root ID                          : 8192.54:4b:8c:44:c1:03
  Root cost                        : 0
  Root port                        : xe-0/0/11:0
  CIST regional root               : 8192.54:4b:8c:44:c1:03
```

```
  CIST internal root cost          : 1000
  Hello time                       : 2 seconds
  Maximum age                      : 20 seconds
  Forward delay                    : 15 seconds
  Hop count                        : 19
  Message age                      : 0
  Number of topology changes       : 3
  Time since last topology change  : 675 seconds
  Local parameters
    Bridge ID                      : 16384.54:4b:8c:43:27:03

STP bridge parameters for MSTI 1
  MSTI regional root               : 4097.54:4b:8c:44:c1:03
  Root cost                        : 1000
  Root port                        : xe-0/0/11:0
  Hello time                       : 2 seconds
  Maximum age                      : 20 seconds
  Forward delay                    : 15 seconds
  Hop count                        : 19
  Number of topology changes       : 3
  Time since last topology change  : 675 seconds
  Local parameters
    Bridge ID                      : 16385.54:4b:8c:43:27:03

STP bridge parameters for MSTI 2
  MSTI regional root               : 4098.88:a2:5e:8c:76:03
  Root cost                        : 1000
  Root port                        : xe-0/0/9:0
  Hello time                       : 2 seconds
  Maximum age                      : 20 seconds
  Forward delay                    : 15 seconds
  Hop count                        : 19
  Number of topology changes       : 3
  Time since last topology change  : 675 seconds
  Local parameters
    Bridge ID                      : 8194.54:4b:8c:43:27:03
```

Meaning

The operational mode command **show spanning-tree interface** displays spanning-tree domain information such as the designated port and the port roles.

The operational mode command **show spanning-tree bridge** displays the spanning-tree domain information at either the bridge level or the interface level. If the optional interface name is omitted, all interfaces in the spanning-tree domain are displayed.

Verifying MSTP Configuration on Switch 2

Purpose

Verify the MSTP configuration on Switch 2.

Action

Issue the operational mode commands **show spanning-tree interface** and **show spanning-tree bridge**:

```
user@switch2> show spanning-tree bridge
```

```
Spanning tree interface parameters for instance 0

Interface                 Port ID    Designated         Designated         Port
   State  Role
                                       port ID           bridge ID          Cost
et-0/0/3                128:1010     128:1011   8192.544b8c44c103         1000
   FWD    ROOT
xe-0/0/9:0              128:1012     128:1010  16384.544b8c432703         1000
   BLK    ALT

Spanning tree interface parameters for instance 1

Interface                 Port ID    Designated         Designated         Port
   State  Role
                                       port ID           bridge ID          Cost
et-0/0/3                128:1010     128:1011   4097.544b8c44c103         1000
   FWD    ROOT
xe-0/0/9:0              128:1012     128:1010  16385.544b8c432703         1000
   BLK    ALT

Spanning tree interface parameters for instance 2

Interface                 Port ID    Designated         Designated         Port
   State  Role
                                       port ID           bridge ID          Cost
et-0/0/3                128:1010     128:1010   4098.88a25e8c7603         1000
   FWD    DESG
xe-0/0/9:0              128:1012     128:1012   4098.88a25e8c7603         1000
   FWD    DESG
```

```
user@switch2> show spanning-tree bridge
```

```
STP bridge parameters
Routing instance name               : GLOBAL
Context ID                          : 0
Enabled protocol                    : MSTP

STP bridge parameters for CIST
  Root ID                           : 8192.54:4b:8c:44:c1:03
  Root cost                         : 0
  Root port                         : et-0/0/3
  CIST regional root                : 8192.54:4b:8c:44:c1:03
  CIST internal root cost           : 1000
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Hop count                         : 19
  Message age                       : 0
  Number of topology changes        : 2
  Time since last topology change   : 659 seconds
  Local parameters
    Bridge ID                       : 32768.88:a2:5e:8c:76:03

STP bridge parameters for MSTI 1
  MSTI regional root                : 4097.54:4b:8c:44:c1:03
  Root cost                         : 1000
  Root port                         : et-0/0/3
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Hop count                         : 19
  Number of topology changes        : 2
  Time since last topology change   : 659 seconds
  Local parameters
    Bridge ID                       : 32769.88:a2:5e:8c:76:03

STP bridge parameters for MSTI 2
  MSTI regional root                : 4098.88:a2:5e:8c:76:03
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Number of topology changes        : 3
  Time since last topology change   : 655 seconds
  Local parameters
```

```
    Bridge ID                      : 4098.88:a2:5e:8c:76:03
```

Meaning

The operational mode command **show spanning-tree interface** displays spanning-tree domain information such as the designated port and the port roles. The spanning-tree interface parameters for instance 2 show that both ports are designated ports, which means Switch 2 is the root bridge for this instance.

The operational mode command **show spanning-tree bridge** displays the spanning-tree domain information at either the bridge level or interface level. If the optional interface name is omitted, all interfaces in the spanning-tree domain are displayed.

Verifying MSTP Configuration on Switch 3

Purpose

Verify the MSTP configuration on Switch 3.

Action

Issue the operational mode commands **show spanning-tree interface** and **show spanning-tree bridge**:

```
user@switch3> show spanning-tree interface
```

```
Spanning tree interface parameters for instance 0

Interface                 Port ID    Designated         Designated         Port
   State  Role
                                       port ID           bridge ID          Cost
xe-0/0/11:0              128:1010     128:1010   8192.544b8c44c103         1000
   FWD    DESG
et-0/0/6                 128:1011     128:1011   8192.544b8c44c103         1000
   FWD    DESG
xe-0/0/21:0              128:1012     128:1012   8192.544b8c44c103         1000
   FWD    DESG

Spanning tree interface parameters for instance 1

Interface                 Port ID    Designated         Designated         Port
   State  Role
                                       port ID           bridge ID          Cost
xe-0/0/11:0              128:1010     128:1010   4097.544b8c44c103         1000
   FWD    DESG
et-0/0/6                 128:1011     128:1011   4097.544b8c44c103         1000
```

```
   FWD    DESG
xe-0/0/21:0              128:1012     128:1012   4097.544b8c44c103         1000
   FWD    DESG

Spanning tree interface parameters for instance 2

Interface                  Port ID    Designated         Designated         Port
   State  Role
                                        port ID           bridge ID          Cost
xe-0/0/11:0              128:1010     128:1012   8194.544b8c432703         1000
   BLK    ALT
et-0/0/6                 128:1011     128:1010   4098.88a25e8c7603         1000
   FWD    ROOT
xe-0/0/21:0              128:1012     128:1012  16386.544b8c44c103         1000
   FWD    DESG
```

user@switch3> **show spanning-tree bridge**

```
STP bridge parameters
Routing instance name               : GLOBAL
Context ID                          : 0
Enabled protocol                    : MSTP

STP bridge parameters for CIST
  Root ID                           : 8192.54:4b:8c:44:c1:03
  CIST regional root                : 8192.54:4b:8c:44:c1:03
  CIST internal root cost           : 0
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Number of topology changes        : 2
  Time since last topology change   : 786 seconds
  Local parameters
    Bridge ID                       : 8192.54:4b:8c:44:c1:03

STP bridge parameters for MSTI 1
  MSTI regional root                : 4097.54:4b:8c:44:c1:03
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Number of topology changes        : 1
```

```
  Time since last topology change   : 786 seconds
  Local parameters
    Bridge ID                       : 4097.54:4b:8c:44:c1:03

STP bridge parameters for MSTI 2
  MSTI regional root                : 4098.88:a2:5e:8c:76:03
  Root cost                         : 1000
  Root port                         : et-0/0/6
  Hello time                        : 2 seconds
  Maximum age                       : 20 seconds
  Forward delay                     : 15 seconds
  Hop count                         : 19
  Number of topology changes        : 1
  Time since last topology change   : 786 seconds
  Local parameters
    Bridge ID                       : 16386.54:4b:8c:44:c1:03
```

Meaning

The operational mode command **show spanning-tree interface** displays spanning-tree domain information such as the designated port and the port roles. Switch 3 is the root bridge for instance 0, which is the CIST, as well as for instance 1. In both instances, all ports on Switch 3 are designated ports.

The operational mode command **show spanning-tree bridge** displays the spanning-tree domain information at either the bridge level or the interface level. If the optional interface name is omitted, all interfaces in the spanning-tree domain are displayed.

Verifying MSTP Configuration on Switch 4

Purpose

Verify the MSTP configuration on Switch 4.

Action

Issue the operational mode commands **show spanning-tree interface** and **show spanning-tree bridge**:

```
user@switch4> show spanning-tree interface
```

```
Spanning tree interface parameters for instance 0

Interface                 Port ID    Designated         Designated         Port
   State  Role
                                       port ID           bridge ID          Cost
```

```
xe-0/0/12:0              128:1011     128:1011  16384.40a677792303         1000
   FWD    DESG
xe-0/0/21:0              128:1012     128:1012   8192.544b8c44c103         1000
   FWD    ROOT

Spanning tree interface parameters for instance 1

Interface                  Port ID    Designated         Designated         Port
   State  Role
                                       port ID           bridge ID          Cost
xe-0/0/12:0              128:1011     128:1011  16385.40a677792303         1000
   FWD    DESG
xe-0/0/21:0              128:1012     128:1012   4097.544b8c44c103         1000
   FWD    ROOT

Spanning tree interface parameters for instance 2

Interface                  Port ID    Designated         Designated         Port
   State  Role
                                       port ID           bridge ID          Cost
xe-0/0/12:0              128:1011     128:1011   8194.544b8c432703         1000
   FWD    ROOT
xe-0/0/21:0              128:1012     128:1012  16386.544b8c44c103         1000
   BLK    ALT
```

user@switch4> **show spanning-tree bridge**

```
STP bridge parameters
Routing instance name              : GLOBAL
Context ID                         : 0
Enabled protocol                   : MSTP

STP bridge parameters for CIST
  Root ID                          : 8192.54:4b:8c:44:c1:03
  Root cost                        : 0
  Root port                        : xe-0/0/21:0
  CIST regional root               : 8192.54:4b:8c:44:c1:03
  CIST internal root cost          : 1000
  Hello time                       : 2 seconds
  Maximum age                      : 20 seconds
  Forward delay                    : 15 seconds
```

```
  Hop count                          : 19
  Message age                        : 0
  Number of topology changes         : 2
  Time since last topology change    : 823 seconds
  Local parameters
    Bridge ID                        : 16384.40:a6:77:79:23:03

STP bridge parameters for MSTI 1
  MSTI regional root                 : 4097.54:4b:8c:44:c1:03
  Root cost                          : 1000
  Root port                          : xe-0/0/21:0
  Hello time                         : 2 seconds
  Maximum age                        : 20 seconds
  Forward delay                      : 15 seconds
  Hop count                          : 19
  Number of topology changes         : 2
  Time since last topology change    : 823 seconds
  Local parameters
    Bridge ID                        : 16385.40:a6:77:79:23:03

STP bridge parameters for MSTI 2
  MSTI regional root                 : 4098.88:a2:5e:8c:76:03
  Root cost                          : 2000
  Root port                          : xe-0/0/12:0
  Hello time                         : 2 seconds
  Maximum age                        : 20 seconds
  Forward delay                      : 15 seconds
  Hop count                          : 18
  Number of topology changes         : 2
  Time since last topology change    : 823 seconds
  Local parameters
    Bridge ID                        : 32770.40:a6:77:79:23:03
```

Meaning

The operational mode command **show spanning-tree interface** displays spanning-tree domain information such as the designated port and the port roles.

The operational mode command **show spanning-tree bridge** displays the spanning-tree domain information at either the bridge level or the interface level. If the optional interface name is omitted, all interfaces in the spanning-tree domain are displayed.

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]**

SEE ALSO

Configuring VSTP Protocol

IN THIS SECTION

Virtual Spanning-Tree Protocol works with VLANs that require device compatibility.

Understanding VSTP

IN THIS SECTION

When using VSTP, we recommend that you enable VSTP on all VLANs that can receive VSTP bridge protocol data units (BPDUs).

Benefits of VSTP

VSTP has the following benefits:

- Connects devices that are not part of the network
- Compatible with Cisco PVST+
- VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a device.

VSTP Restrictions

VSTP has these restrictions:

- The EX Series switches EX4300, EX4600 and the QFX platforms QFX5100,QFX3500,QFX3600 support 510 Vlans on VSTP.
- VSTP is not supported on the SRX platform - just STP/RSTP/MSTP are supported on SRX Series.
- On EX Series (except EX9200) and QFX Series switches running Junos OS that supports ELS—VSTP can support up to 510 VLANs.
- On EX9200 switches—VSTP can support up to 4000 VLANs.
- On an EX Series switch running Junos OS that does not support ELS—VSTP can support up to 253 VLANs.

Recommended Uses of VSTP

You can use Juniper Networks switches with VSTP and Cisco switches with PVST+ and Rapid-PVST+ in the same network. Cisco supports a proprietary Per-VLAN Spanning Tree (PVST) protocol, which maintains

a separate spanning tree instance per each VLAN. One Spanning Tree per VLAN allows fine grain load balancing but requires more BPDU CPU processing as the number of VLANs increases. PVST runs on Cisco proprietary ISL trunks which is not supported by Juniper. Juniper switches only inter-operate with PVST+ and Rapid-PVST+. For more information, see VSTP and RPVST+ convergence on native-vlan 1 for EX Switches .

> **TIP:** If your device interoperates with a Cisco device running Rapid per VLAN Spanning Tree (Rapid PVST+), we recommend that you enable both VSTP and RSTP on the EX Series or QFX Series interface.

VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a device. The maximum number of VLANs that can be supported by VSTP on a switch depends upon whether you are using Junos OS for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style or Junos OS that does not support ELS. For ELS details, see *Using the Enhanced Layer 2 Software CLI*. For additional VLANs, use RSTP.

The maximum number of VLANs supported by VSTP on a switch depends upon whether you are using Junos OS for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style or Junos OS that does not support ELS.

Global and Specific VSTP Configurations for Switches

IN THIS SECTION

Juniper Networks EX Series Ethernet Switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP). The default factory configuration for EX Series switches uses RSTP. This topic describes options for configuring VSTP on an EX Series or QFX Series switch.

> **NOTE:** On EX Series (other than EX9200) and QFX switches running Junos OS that supports ELS—VSTP can support up to 510 VLANs. However, on EX9200 switches, VSTP can support only up to 253 VLANs.

> **NOTE:** When you configure VSTP, we recommend that you enable VSTP on all VLANs that can receive VSTP bridge protocol data units (BPDUs).

Where Can I Configure VSTP?

You can configure VSTP at the global level:

- For all interfaces on the switch
- For all interfaces within all VLANs
- For all interfaces within a specified VLAN
- For all interfaces within a specified VLAN group

You can configure or disable VSTP for specific interfaces:

- For a specific interface on the switch
- For a specific interface within all VLANs
- For a specific interface within a specified VLAN
- For a specific interface within a specified VLAN group

NOTE:

- If you configure VSTP on an interface at both the global and the specific VLAN level, the interface configuration that is defined at the specific VLAN level overrides the interface configuration that is defined at the global level.
- If you specify VSTP to be configured on an interface that is not configured to belong to the VLAN (or VLANs), an error message is displayed.
- On EX Series (other than EX9200) and QFX switches running Junos OS that supports ELS—VSTP can support up to 510 VLANs. However, on EX9200 switches, VSTP can support only up to 253 VLANs.
- When you configure VSTP, we recommend that you enable VSTP on all VLANs that can receive VSTP bridge protocol data units (BPDUs).

  You must enable RSTP if you used the **set vstp vlan all** statement to enable VSTP and if the switch has more than 253 VLANs. If you use the **set vstp vlan all** statement to enable VSTP on a switch with more than 253 VLANs, the configuration cannot be committed.

VSTP Commands to Configure All Interfaces

Command to configure VSTP on an individual interface on a switch:

```
[edit protocols vstp]
user@switch@ set interface interface-name
```

Command to configure all VSTP interfaces on a switch:

```
[edit protocols vstp]
user@switch# set interface all
```

Command to configure all VSTP interfaces for all VLANs:

NOTE: When you issue the **set protocols vstp vlan all interface all** command, you might not receive an error message when you have exceed the limit of 5119 vports.

```
[edit protocols vstp]
user@switch# set vlan all interface all
```

Command to configure all VSTP interfaces within a specified VLAN:

```
[edit protocols vstp]
user@switch# set vlan (vlan-id  |vlan-range |open-set-of-values) interface all  interface all
```

> **NOTE:** When you configure VSTP with the **set protocol vstp vlan *vlan-id* interface *interface-name*** command, the VLAN named **default** is excluded. You must manually configure a VLAN with the name **default** to run VSTP.

Command to configure all VSTP interfaces within a specified VLAN group:

```
[edit protocols vstp]
user@switch# set vlan-group vlan-group-name vlan (vlan-id  |vlan-range |open-set-of-values) interface all
```

VSTP Commands to Configure Specific Interfaces

Command to configure a specific interface on a switch:

```
[edit protocols vstp]
user@switch# set interface interface-name
```

Command to configure a specific interface within all VLANs:

```
[edit protocols vstp]
user@switch# set vlan all interface interface-name
```

> **CAUTION:** Ensure that the interface is a member of all VLANs before you add the interface to the VSTP configuration. If the interface is not a member of all VLANs, this VSTP configuration will fail when you try to commit it.

Command to configure a specific interface within a specific VLAN:

```
[edit protocols vstp]
user@switch# set vlan vlan-id-or-vlan-range interface interface-name
```

Command to configure a specific interface within a specific VLAN group:

```
[edit protocols vstp]
user@switch#  set vlan-group vlan-group-name vlan (vlan-id  |vlan-range |open-set-of-values) interface
interface-name
```

VSTP Commands to Disable Interfaces

Command to disable VSTP on an individual interface on a switch:

```
[edit protocols vstp]
user@switch@  set interface interface-name disable
```

Command to disable VSTP on a specific interface within a specific VLAN on a switch:

```
[edit protocols vstp]
user@switch@  set vlan vlan-id  interface interface-name disable
```

Command to disable one specific VSTP interface on all the VLANs on the switch:

```
[edit protocols vstp]
user@switch@  set vlan all interface interface-name disable
```

Command to disable a specific VSTP interface within a specific VLAN group:

```
[edit protocols vstp]
user@switch@  set vlan-group group group-name vlan (vlan-id  |vlan-range | open-set-of-values) interface
interface-name disable
```

NOTE: You *cannot* disable the VSTP VLAN parameters for *all* VSTP interfaces.

Example: Configuring VSTP on a Trunk Port with Tagged Traffic

IN THIS SECTION

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.

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.

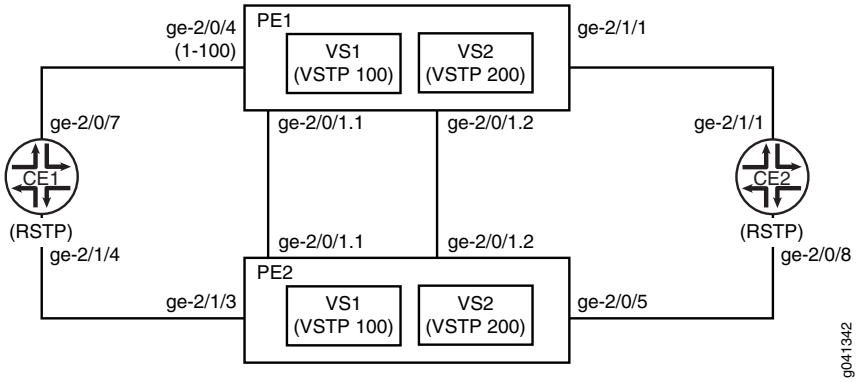
Topology

Figure 4 on page 150 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 4: 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

IN THIS SECTION

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.

SEE ALSO

access-trunk | 293

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.

SEE ALSO

.

RELATED DOCUMENTATION

Connecting and Configuring an EX Series Switch (CLI Procedure)

4

CHAPTER

BPDU Protection for Spanning-Tree Protocols

BPDU Protection for Spanning-Tree Protocols

IN THIS SECTION

Understanding BPDU Protection for Spanning-Tree Instance Interfaces

MX Series routers, ACX Series routers, and EX Series switches support spanning-tree protocols that prevent loops in a network by creating a tree topology (spanning-tree) of the entire bridged network. All spanning-tree protocols use a special type of frame called bridge protocol data units (BPDUs) to communicate with each other. Other devices in the network, such as PCs, generate their own BPDUs that are not compatible with the spanning-tree BPDUs. When BPDUs generated by other devices are transmitted to switches on which spanning-tree protocols are configured, a misconfiguration can occur in the spanning tree and a network outage can occur. Therefore, it is necessary to protect an interface in a spanning-tree topology from BPDUs generated from other devices.

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 ACX Series routers, MX Series routers, and 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**
- **vlan-bridge**
- **extended-vlan-vpls**

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

Enable BPDU protection on interfaces that are configured as edge ports by using the **bpdu-block-on-edge** command. If you have not configured a port as an edge port, you can still configure BPDU protection on the interface by using the **bpdu-block** command under the **set ethernet-switching-options** hierarchy. You can also use the **bpdu-block** command to configure BPDU protection on interfaces configured for a spanning-tree.

SEE ALSO

Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network | 259

Understanding VPLS Multihoming | 254

Understanding BPDU Protection for STP, RSTP, and MSTP

IN THIS SECTION

Networks frequently use multiple protocols simultaneously to achieve different goals and in some cases those protocols might conflict with each other. One such case is when spanning-tree protocols are active on the network, where a special type of switching frame called a bridge protocol data unit (BPDU) can conflict with BPDUs generated on other devices such as PCs. The different kinds of BPDUs are not compatible, but they can still be recognized by other devices that use BPDUs and cause network outages. You need to protect any device that recognizes BPDUs from picking up incompatible BPDUs.

Different Kinds of BPDUs

Spanning-tree protocols such as Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), and Multiple Spanning Tree Protocol (MSTP) generate their own BPDUs. These peer STP applications use their BPDUs to communicate, and ultimately, the exchange of BPDUs determines which interfaces block traffic and which interfaces become root ports and forward traffic.

User bridge applications running on a PC can also generate BPDUs. If these BPDUs are picked up by STP applications running on the switch, they can trigger STP miscalculations, and those miscalculations can lead to network outages. Similarly, BPDUs generated by STP protocols can cause problems if they are picked up by devices such as PCs that are not using STP. Some mechanism for BPDU protection must be implemented in these cases.

Protecting Switches from Incompatible BPDUs

To protect the state of spanning-tree protocols on switches from outside BPDUs, enable BPDU protection on the interfaces of a switch on which spanning-tree protocols are configured and are connected to user devices (such as PCs)—for example, on edge ports connected to PCs. Use the same strategy when a device on which STP is not configured is connected to a switch through a trunk interface that forwards BPDUs generated by spanning-tree protocols. In this case, you protect the device from BPDUs generated by the STP on the switch.

To prevent a switch from forwarding BPDUs generated by spanning-tree protocols to a device, you can enable **bpdu-block** on an interface.

- On Juniper Networks EX Series Ethernet Switches that run Juniper Networks Junos operating system (Junos OS) that supports the Enhanced Layer 2 Software (ELS) configuration style, enable **bpdu-block** at the **[edit protocols layer2-control]** hierarchy level. To clear the BPDU error, use **clear error bpdu interface**.
- On EX Series switches that run Junos OS that does not support the ELS configuration style, enable **bpdu-block** at the **[edit ethernet-switching-options**] hierarchy level. To clear the BPDU error, use **clear ethernet-switching bpdu-error interface**.

When an interface configured with BPDU protection encounters an incompatible BPDU, it drops that BPDU and then, either shuts down or continues to receive packets other than spanning-tree protocol BPDUs depending on the configuration defined in the **bpdu-block** statement. If the interface continues to be open after dropping all incompatible BPDUs, all packets except incompatible BPDUs continue to ingress and egress through the interface.

If the interface shuts down after dropping all BPDUs, you can re-enable the interface as follows:

- On Juniper Networks EX Series and QFX Series switches running Juniper Networks Junos operating system (Junos OS) that supports the Enhanced Layer 2 Software (ELS) configuration style:
  - Include the **disable-timeout** statement at the **[edit protocols layer2-control bpdu-block]** hierarchy level to enable the interfaces to automatically return to service when the specified timer expires.
  - Issue the operational mode command **clear error bpdu interface** on the switch.
- On EX Series switches running Junos OS that does not support the ELS configuration style:
  - Include the **disable-timeout** statement at the [edit ethernet-switching-options bpdu-block] hierarchy level to enable the interfaces to automatically return to service when the specified timer expires.
  - Issue the operational mode command **clear ethernet-switching bpdu-error interface** on the switch.

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 the link failure to the root bridge has failed and initiates a topology reconvergence.

> **TIP:** The maximum age timer should be longer than the configured hello timer.

Hello Time for Root Bridge to Transmit Hello BPDUs

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

SEE ALSO

- Configuring BPDU Protection on Switch Spanning Tree Interfaces | 179
- Configuring Rapid Spanning Tree Protocol | 45
- Configuring Multiple Spanning Tree Protocol | 105
- *Configuring VLAN Spanning Tree Protocol*
- max-age | 332
- hello-time | 320

Configuring 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**.

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 5G Universal Routing Platforms.

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.

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)

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;
```

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.

Understanding BPDU Protection for STP, RSTP, and MSTP

IN THIS SECTION

Networks frequently use multiple protocols simultaneously to achieve different goals and in some cases those protocols might conflict with each other. One such case is when spanning-tree protocols are active on the network, where a special type of switching frame called a bridge protocol data unit (BPDU) can conflict with BPDUs generated on other devices such as PCs. The different kinds of BPDUs are not compatible, but they can still be recognized by other devices that use BPDUs and cause network outages. You need to protect any device that recognizes BPDUs from picking up incompatible BPDUs.

Different Kinds of BPDUs

Spanning-tree protocols such as Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP) generate their own BPDUs. These peer STP applications use their BPDUs to communicate, and ultimately, the exchange of BPDUs determines which interfaces block traffic and which interfaces become root ports and forward traffic.

User bridge applications running on a PC can also generate BPDUs. If these BPDUs are picked up by STP applications running on the device, they can trigger STP miscalculations, and those miscalculations can lead to network outages. Similarly, BPDUs generated by STP protocols can cause problems if they are picked up by devices such as PCs that are not using STP. Some mechanism for BPDU protection must be implemented in these cases.

Protecting Devices from Incompatible BPDUs

To protect the state of spanning-tree protocols on devices from outside BPDUs, enable BPDU protection on the interfaces of a device on which spanning-tree protocols are configured and are connected to user devices (such as PCs)—for example, on edge ports connected to PCs. Use the same strategy when a device on which STP is not configured is connected to a device through a trunk interface that forwards BPDUs generated by spanning-tree protocols. In this case, you protect the device from BPDUs generated by the STP on the device.

To prevent a device from forwarding BPDUs generated by spanning-tree protocols to a device, you can enable **bpdu-block** on an interface.

- On Juniper Networks SRX Series devices that run Juniper Networks Junos operating system (Junos OS) that supports the Enhanced Layer 2 Software (ELS) configuration style, enable **bpdu-block** at the **[edit protocols layer2-control]** hierarchy level. To clear the BPDU error, use **clear error bpdu interface**.

When an interface configured with BPDU protection encounters an incompatible BPDU, it drops that BPDU and then, either shuts down or continues to receive packets other than spanning-tree protocol BPDUs depending on the configuration defined in the **bpdu-block** statement. If the interface continues to be open after dropping all incompatible BPDUs, all packets except incompatible BPDUs continue to ingress and egress through the interface.

If the interface shuts down after dropping all BPDUs, you can re-enable the interface as follows:

- On Juniper Networks SRX Series devices running Juniper Networks Junos operating system (Junos OS) that supports the Enhanced Layer 2 Software (ELS) configuration style:
  - Include the **disable-timeout** statement at the **[edit protocols layer2-control bpdu-block]** hierarchy level to enable the interfaces to automatically return to service when the specified timer expires.
  - Issue the operational mode command **clear error bpdu interface** on the device.

Understanding BPDU Protection for EVPN-VXLAN

IN THIS SECTION

EVPN-VXLAN data center fabrics have a number of built-in Ethernet loop prevention mechanisms, such as split-horizon and designated forwarder and non-designated forwarder election. In some existing data center environments where a new IP EVPN fabric is being deployed, you might need to configure BPDU protection at the leaf-to-server interface in order to avoid network outages due to xSTP miscalculations. Incorrect cabling between the server and leaf interfaces, or any back-door layer 2 link between two or more ESI-LAG interfaces, might cause miscalculations and then result in Ethernet loops. Without BPDU protection, BPDUs might not be recognized and will be flooded as unknown Layer 2 packets on the VXLAN interfaces. With BPDU protection, when a BPDU is received on an edge port in an EVPN-VXLAN environment, the edge port is disabled and stops forwarding all traffic. You can also configure BPDU protection to drop BPDU traffic but have all other traffic forwarded on the interfaces without having to configure a spanning-tree protocol.

Enabling BPDU Protection on Edge Ports on Access and Leaf Devices with STP, MSTP, and RSTP Configured

In this procedure, RSTP is being configured, but it works the same way for STP and MSTP.

1. o enable edge port blocking for RSTP:

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

2. Configure RSTP on edge ports that are either access or trunk interfaces.

   NOTE: Edge ports can be access or trunk ports.

   To configure RSTP on edge ports:

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

   For example:

   ```
   [edit]
   user@host#  set protocols rstp interface ae0 edge
   ```

   In this example, **ae0** is an ESI-LAG interface.

Enabling BPDU Protection on Access and Leaf Devices without STP, MSTP, or RSTP Configured

1. To enable BPDU protection on access and leaf devices without STP, MSTP, or RSTP configured:

   ```
   [edit]
   user@host#  set protocols layer2-control bpdu-block interface interface-name
   ```

   For example:

   ```
   [edit]
   user@host#  set protocols layer2-control bpdu-block interface xe-0/0/5.0
   ```

Enabling BPDU Protection on Access and Leaf devices without STP, MSTP, or RSTP Configured and Forward other Traffic

1. To enable BPDU protection on access and leaf devices without STP, MSTP, or RSTP:

   ```
   [edit]
   user@host#  set protocols layer2-control bpdu-block interface interface-name drop
   ```

   For example:

   ```
   [edit]
   user@host#  set protocols layer2-control bpdu-block interface xe-0/0/5.0 drop
   ```

Automatically Unblocking an Interface Using an Expiry timer on Access and Leaf Devices

1. To automatically unblock an interface using an expiry timer on access and leaf devices:

   NOTE: The range of seconds is between 10 and 3600.

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

   For example:

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

Manually Unblocking an Interface on Access and Leaf Devices

1. To manually unblock an interface on access and leaf devices:

```
[edit]
user@host# run clear error bpdu interface all
```

SEE ALSO

Understanding BPDU Protection for STP, RSTP, and MSTP | 169

Using a Default Layer 3 Gateway to Route Traffic in an EVPN-VXLAN Overlay Network

EVPN Multihoming Overview

Configuring BPDU Protection on Switch Spanning Tree Interfaces

All spanning-tree protocols use a special type of frame called bridge protocol data units (BPDUs) to communicate with each other. Other devices in the network, such as PCs, generate their own BPDUs that are not compatible with the spanning-tree BPDUs. When BPDUs generated by other devices are transmitted to switches on which spanning-tree protocols are configured, a misconfiguration can occur in the spanning tree and a network outage can occur. Therefore, it is necessary to protect an interface in a spanning-tree topology from BPDUs generated from other devices.

On the ACX Series routers, MX Series routers QFX Series switches, and EX Series switches, you can configure BPDU protection to ignore BPDU received on interfaces where none are 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.

> **NOTE:** This topic applies to Junos OS for EX Series and QFX switches with support for the Enhanced Layer 2 Software (ELS) configuration style. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

You can configure BPDU protection to ignore BPDU received on interfaces where none are 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 spanning-tree instance interfaces:

- On a specific spanning-tree interface:

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

     ```
     [edit protocols layer2-control bpdu-block ]
     user@switcht# set 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-control bpdu-block interface interface-name]
     user@switch# 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 a Gigabit Ethernet.
           encapsulation (ethernet-bridge | ethernett-vpls | extended-vlan-bridge | extended-vlan-vpls | vlan-bridge|
              vlan-vpls);
        }
        xe-fpc/pic/port { # VLAN encapsulation on 10-Gigabit Ethernet.
           encapsulation (ethernet-bridge | ethernett-vpls | extended-vlan-bridge | extended-vlan-vpls | vlan-bridge|
              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;
        }
    }
```

- To disable BPDU protection for a specific spanning-tree interface

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

Configuring BPDU Protection on ACX Router, EX Switch and MX Router Edge Ports

On ACX Series routers, 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.

TIP: You can configure BPDU protection for RSTP, STP or MSTP topologies at the [**edit protocols (mstp|rstp|vstp)**] hierarchy level.

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;
   }
}
```

Configuring BPDU protection For Edge Interfaces

In a spanning-tree topology, if a switch is an access switch then interfaces on that switch will be connected to end devices such as PCs, servers, routers, or hubs, that are not connected to other switches. You configure these interfaces as edge interfaces because they directly connect to end devices.

Interfaces that are configured as edge interfaces can transition to a forwarding state immediately because they cannot create network loops. A switch detects edge ports by noting the absence of communication from the end stations. As edge ports are connected to end devices, it is imperative that you configure BPDU protection on edge ports to protect the switch from outside BPDUs. If BPDU protection is enabled on an edge interface, the interface shuts down on encountering an outside BPDU thereby preventing any traffic from passing through the interface. You can re-enable the interface either by using the **disable-timeout** command while configuring BPDU protection, or by issuing the **clear ethernet-switching bpdu-error** operational mode command. The **clear ethernet-switching bpdu-error** command will only re-enable an interface but the BPDU configuration for the interface will continue to exist unless you explicitly remove the BPDU configuration.

To configure BPDU protection on an edge interface of a switch:

NOTE: Ensure that the switch is connected to an end device.

1. Configure any spanning-tree protocol on the switch if not configured already. RSTP is configured in this procedure.

   NOTE: The Rapid Spanning Tree Protocol (RSTP) is configured by default on a switch.

   ```
   [edit protocols]
   user@switch# set rstp
   ```

2. Enable RSTP on a specific interface and set a priority for the interface—for example, **ge-0/0/0.0**:

```
[edit protocols]
user@switch# set rstp interface ge-0/0/0.0 priority 16
```

3. Configure the **ge-0/0/0.0** interface as an edge interface and enable BPDU protection on that interface:

```
[edit protocols]
user@switch# set rstp bpdu-block-on-edge interface ge-0/0/0.0 edge
```

4. Commit the configuration:

```
[edit]
user@switch# commit
```

5. Verify that BPDU protection is configured properly on the edge interface (**ge-0/0/0.0**):

   - Run the **show ethernet-switching interfaces** operational mode command to ensure that BPDU protection is configured on the edge interface:

     ```
     user@switch> show ethernet-switching interfaces
     ```

     ```
     Interface    State  VLAN members     Tag   Tagging     Blocking
     ge-0/0/0.0   down   default               untagged   Disabled by bpdu-control
     me0.0        up     mgmt                   untagged   unblocked
     ```

     In this output, you note that the **ge-0/0/0.0** interface is down because it has received BPDUs from the end device. Also, note that the state of the **Blocking** field is **Disabled by bpdu-control**, which indicates that the port is disabled because of BPDU protection.

   - Run the **show spanning-tree interfaces** operational mode command to ensure that the **ge-0/0/0.0** interface is not displayed in the output.

SEE ALSO

Configuring BPDU for Interface Protection With Port Shutdown Mode

In a spanning-tree topology, if a switch is an access switch then interfaces on that switch will be connected to end devices such as PCs, servers, routers, or hubs, that are not connected to other switches. You configure these interfaces as edge interfaces because they directly connect to end devices. Interfaces that are configured as edge interfaces can transition to a forwarding state immediately because they cannot create network loops. A switch detects edge ports by noting the absence of communication from the end stations. As edge ports are connected to end devices, it is imperative that you configure BPDU protection

on edge ports to protect the switch from outside BPDUs. If BPDU protection is enabled on an edge interface, the interface shuts down on encountering an outside BPDU thereby preventing any traffic from passing through the interface. You can re-enable the interface either by using the **disable-timeout** command while configuring BPDU protection, or by issuing the **clear ethernet-switching bpdu-error** operational mode command. The **clear ethernet-switching bpdu-error** command will only re-enable an interface but the BPDU configuration for the interface will continue to exist unless you explicitly remove the BPDU configuration.

To configure BPDU protection on an edge interface of a switch:

> **NOTE:** Ensure that the switch is connected to an end device.

1. Configure any spanning-tree protocol on the switch if not configured already. RSTP is configured in this procedure.

   > **NOTE:** The Rapid Spanning Tree Protocol (RSTP) is configured by default on a switch.

   ```
   [edit protocols]
   user@switch# set rstp
   ```

2. Enable RSTP on a specific interface and set a priority for the interface—for example, **ge-0/0/0.0**:

   ```
   [edit protocols]
   user@switch# set rstp interface ge-0/0/0.0 priority 16
   ```

3. Configure the **ge-0/0/0.0** interface as an edge interface and enable BPDU protection on that interface:

   ```
   [edit protocols]
   user@switch# set rstp bpdu-block-on-edge interface ge-0/0/0.0 edge
   ```

4. Commit the configuration:

   ```
   [edit]
   user@switch# commit
   ```

5. Verify that BPDU protection is configured properly on the edge interface (**ge-0/0/0.0**):

   - Run the **show ethernet-switching interfaces** operational mode command to ensure that BPDU protection is configured on the edge interface:

     ```
     user@switch> show ethernet-switching interfaces
     ```

```
Interface    State  VLAN members     Tag   Tagging     Blocking
ge-0/0/0.0   down   default                untagged   Disabled by bpdu-control
me0.0        up     mgmt                    untagged   unblocked
```

In this output, you note that the **ge-0/0/0.0** interface is down because it has received BPDUs from the end device. Also, note that the state of the **Blocking** field is **Disabled by bpdu-control**, which indicates that the port is disabled because of BPDU protection.

- Run the **show spanning-tree interfaces** operational mode command to ensure that the **ge-0/0/0.0** interface is not displayed in the output.

SEE ALSO

Configuring BPDU for Interface Protection With BPDU Drop Mode

For certain access switches, you might want interfaces on the switch not to shutdown on encountering incompatible BPDU packets; instead, only drop incompatible BPDU packets while allowing the remaining traffic to pass through. Such an interface must not have a spanning-tree protocol configured on it, so that packets that pass through the interface will not cause STP misconfiguration and consequent network outages.

To configure BPDU protection for an interface to only drop incompatible BPDU packets and to allow the remaining traffic to pass through, while retaining the interface status as up:

NOTE: Ensure that the switch on which you are configuring BPDU protection is connected to a peer device.

1. Delete or disable any spanning-tree protocol (for instance, RSTP as in this procedure) configured on the switch or on any interface.

   - To delete a spanning-tree protocol on the entire switch:

     ```
     [edit]
     user@switch# delete protocols rstp
     ```

     Or,

     ```
     [edit]
     user@switch# set protocols rstp disable
     ```

   - To delete a spanning-tree protocol on a specific interface (for example, **ge-0/0/0.0**) on the switch:

     ```
     [edit]
     user@switch# set protocols rstp interface ge-0/0/0.0 disable
     ```

     NOTE: As RSTP is configured on a switch by default, ensure that you delete or disable RSTP even though you had not configured it explicitly.

2. Ensure that the interface on which you want to enable the BPDU protection, is up and unblocked. For example, if you want to configure the BPDU protection on the **ge-0/0/0.0** interface, following is the output of the **show ethernet-switching interfaces** command if the interface is up and unblocked:

   ```
   user@switch> show ethernet-switching interfaces
   ```

   ```
   Interface    State  VLAN members        Tag   Tagging  Blocking
   ge-0/0/0.0   up     default                   untagged unblocked
   ```

   In this output, note that the state of the **ge-0/0/0.0** interface is **up** and the value for the **Blocking** field is **unblocked**.

3. Enable the BPDU protection on the interface (**ge-0/0/0.0** in this procedure) to drop BPDU packets:

   ```
   [edit]
   user@switch set ethernet-switching-options bpdu-block interface ge-0/0/0.0 drop
   ```

4. Commit the configuration:

   ```
   [edit]
   ```

```
user@switch# commit
```

5. Verify that the BPDU protection is configured on the interface:

   - Run the **show ethernet-switching interfaces** operational mode command to ensure that the BPDU protection is configured on the interface:

     ```
     user@switch> show ethernet-switching interfaces
     ```

     ```
     Interface    State  VLAN members     Tag   Tagging  Blocking
     ge-0/0/0.0   up     default               untagged unblocked-xSTP bpdu
                                                      filter enabled
     ```

     In this output, note that the **ge-0/0/0.0** interface is up even though it has received incompatible BPDU packets because the **drop** feature is configured for this interface. Also, note that the state of the **Blocking** field is **unblocked-xSTP bpdu filter enabled**, which indicates that the BPDU **drop** feature is enabled on this interface.

   - Run the **show spanning-tree interfaces** operational mode command to ensure that the **ge-0/0/0.0** interface is displayed in the output and that the **State** of the interface is **DIS**, which indicates that the interface discards all incompatible BPDUs:

     ```
     user@switch> 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   16:513    8192.841888af0681  20000   DIS    DIS
     ```

SEE ALSO

Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations

IN THIS SECTION

NOTE: This example uses Junos OS for SRX Series devices with support for the Enhanced Layer 2 Software (ELS) configuration style. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

Spanning-tree protocols support loop-free network communication through the exchange of a special type of frame called a bridge protocol data unit (BPDU). However, when BPDUs generated by spanning-tree protocols are communicated to devices on which spanning-tree protocols are not configured, these devices recognize the BPDUs, which can lead to network outages. You can, however, enable BPDU protection on device interfaces to prevent BPDUs generated by spanning-tree protocols from passing through those interfaces. When BPDU protection is enabled, an interface shuts down when any incompatible BPDU is encountered, thereby preventing the BPDUs generated by spanning-tree protocols from reaching the device.

This example configures BPDU protection on STP device downstream interfaces that connect to two PCs:

Requirements

This example uses the following software and hardware components:

- One SRX Series device in an RSTP
- One SRX Series device that is not in any spanning-tree
- Junos OS Release 15.1X49-D70 or later

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

- Ensured that RSTP is operating on device 1.

- Disabled RSTP on device 2

Overview

SRX Series devices provide Layer 2 loop prevention through Rapid Spanning Tree protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). All spanning-tree protocols use a special type of frame called a BPDU to communicate. Other devices also use BPDUs—PC bridging applications, for example, 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 devices within a spanning-tree topology receive BPDUs from other devices, network outages can occur because of the miscalculations caused by the outside BPDUs. Therefore, you must configure BPDU protection on interfaces in a spanning-tree to avoid network outages.

This example explains how to block outside BPDUs from reaching a device interface connected to devices that are not part of the STP. In this scenario, an interface is shutdown when it encounters an outside BPDU.

This example configures downstream BPDU protection on device 2 interfaces **ge-0/0/5** and **ge-0/0/6**. When BPDU protection is enabled, the device interfaces will shut down if BPDUs generated by the laptops attempt to access device 2.

CAUTION: When configuring BPDU protection on an interface without spanning trees connected to a device with spanning trees, be careful that you do not configure BPDU protection on **all** interfaces. Doing so could prevent BPDUs being received on device interfaces (such as a trunk interface) that you intended to have receive BPDUs from a device with spanning trees.

Configuration

To configure BPDU protection on the interfaces:

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

> **NOTE:** This example configures BPDU protection on specific interfaces. For, SRX Series devices with support for the Enhanced Layer 2 Software (ELS) configuration style, you can configure BPDU protection globally on all spanning tree interfaces. See *Configuring BPDU Protection on Spanning Tree Interfaces* for additional information.

```
set protocols layer2-control bpdu-block interface ge-0/0/5
set protocols layer2-control bpdu-block interface ge-0/0/6
```

Step-by-Step Procedure

To configure BPDU protection for automatic shutdown.

1. To shutdown the BPDU interface on the downstream interface **ge-0/0/5** on device 2:

```
[edit protocol layer 2]
user@host# set bpdu-block interface ge-0/0/5
```

2. To shutdown the BPDU interface on the downstream interface **ge-0/0/6** on device 2:

```
[edit protocol layer 2]
user@host# set bpdu-block interface ge-0/0/6
```

Results

Check the results of the configuration:

```
user@host> show protocol layer 2
bpdu-block {
    interface ge-0/0/5 {
    interface ge-0/0/6 {
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Displaying the Interface State Before BPDU Protection Is Triggered

Purpose

Before any BPDUs can be received on device 2 on either interface **ge-0/0/5** or interface **ge-0/0/6**, confirm the state of those interfaces.

Action

Use the operational mode command **show interfaces extensive <interface name>**:

```
user@host> show interfaces extensive ge-0/0/5
```

```
Physical interface: ge-0/0/5, Enabled, Physical link is Down
  Interface index: 141, SNMP ifIndex: 516, Generation: 144
  Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Link-mode: Full-duplex,
Speed: 1000mbps, BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
Source filtering: Disabled,
  Flow control: Disabled, Auto-negotiation: Enabled, Remote fault: Online
  Device flags   : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 30:7c:5e:44:b1:c6, Hardware address: 30:7c:5e:44:b1:c6
  Last flapped   : 2017-01-16 20:23:55 PST (05:44:46 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :                   0                   0 bps
   Output bytes  :                   0                   0 bps
   Input  packets:                   0                   0 pps
   Output packets:                   0                   0 pps
  Dropped traffic statistics due to STP State:
   Input  bytes  :                   0
   Output bytes  :                   0
   Input  packets:                   0
   Output packets:                   0
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3
incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0,
Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
```

```
FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
  Active alarms  : LINK
  Active defects : LINK
  MAC statistics:                      Receive         Transmit
    Total octets                             0                0
    Total packets                            0                0
    Unicast packets                          0                0
    Broadcast packets                        0                0
    Multicast packets                        0                0
    CRC/Align errors                         0                0
    FIFO errors                              0                0
    MAC control frames                       0                0
    MAC pause frames                         0                0
    Oversized frames                         0
    Jabber frames                            0
    Fragment frames                          0
    VLAN tagged frames                       0
    Code violations                          0
  Filter statistics:
    Input packet count                       0
    Input packet rejects                     0
    Input DA rejects                         0
    Input SA rejects                         0
    Output packet count                                       0
    Output packet pad count                                   0
    Output packet error count                                 0
    CAM destination filters: 1, CAM source filters: 0
  Autonegotiation information:
    Negotiation status: Incomplete
  Packet Forwarding Engine configuration:
    Destination slot: 0
  CoS information:
    Direction : Output
    CoS transmit queue               Bandwidth              Buffer Priority
Limit
                                 %           bps     %           usec
    0 best-effort            95      950000000    95              0      low
none
    3 network-control         5       50000000     5              0      low
none
  Interface transmit statistics: Disabled
  MACSec statistics:
    Output
        Secure Channel Transmitted
```

```
        Protected Packets              : 0
        Encrypted Packets              : 0
        Protected Bytes                : 0
        Encrypted Bytes                : 0
     Input
        Secure Channel Received
        Accepted Packets               : 0
        Validated Bytes                : 0
        Decrypted Bytes                : 0
```

Meaning

The output from the operational mode command **show interfaces extensive** shows that **ge-0/0/5** a is enabled.

Verifying That BPDU Shutdown Protection Is Working Correctly

Purpose

Verify that BPDU protection is working correctly in the network by checking to see whether BPDUs have been blocked appropriately.

Action

Issue **show interfaces extensive <interface name>** to see what happened when the BPDUs reached the two interfaces configured for BPDU protection on device 2:

`user@host>` **show interfaces extensive ge-0/0/5**

```
Physical interface: ge-0/0/5, Enabled, Physical link is Down
  Interface index: 659, SNMP ifIndex: 639, Generation: 161
  Link-level type: Ethernet, MTU: 1514, MRU: 0, Link-mode: Auto, Speed: Auto,
  BPDU Error: Detected, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled,
  Remote fault: Online, Media type: Copper,
  IEEE 802.3az Energy Efficient Ethernet: Disabled
  Device flags   : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 12 supported, 12 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
```

Meaning

When the BPDUs sent from laptops reached interface **ge-0/0/5** on device 2, the interface transitioned to a BPDU inconsistent state, shutting down the interface to prevent BPDUs from reaching the laptops.

You need to reenable the blocked interface. There are two ways to do this. If you included the statement **disable-timeout(Spanning Trees)** in the BPDU configuration, the interface returns to service after the timer expires. Otherwise, use the operational mode command **clear error bpdu interface *interface-name*** to unblock and reenable **ge-0/0/5**. This command will only reenable an interface but the BPDU configuration for the interface will continue to exist unless you remove the BPDU configuration explicitly.

If BPDUs reach the downstream interface on device 2 again, BPDU protection is triggered again and the interface shuts down. In such cases, you must find and repair the misconfiguration that is sending BPDUs to interface **ge-0/0/5** .

SEE ALSO

Configuring BPDU Protection on Spanning Tree Interfaces

Understanding BPDU Protection for STP, RSTP, and MSTP | **173**

Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations | **200**

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

IN THIS SECTION

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 5 on page 196 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 5: BPDU Protection Topology

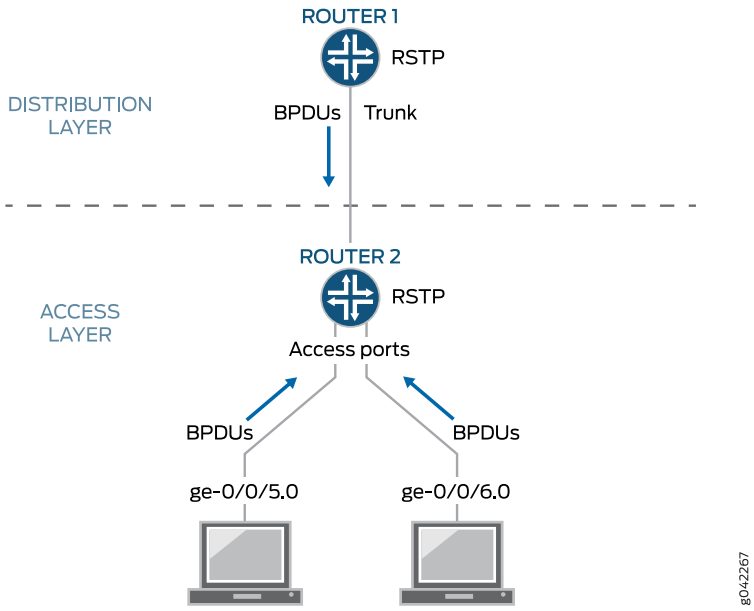


Table 9 on page 196 describes the components that are configured for BPDU protection.

Table 9: 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

IN THIS SECTION

Verify that the configuration is working properly.

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.

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

IN THIS SECTION

SRX Series devices provide Layer 2 loop prevention through 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 devices within a spanning-tree topology receive BPDUs from other devices, network outages can occur because of STP miscalculations.

This example configures BPDU protection on a SRX Series device that uses 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 software and hardware components:

- Two SRX Series devices in an RSTP topology
- Junos OS Release 15.1X49-D70 or later

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

- RSTP enabled on the devices.

Overview

The devices, being in an RSTP, support a loop-free network through the exchange of BPDUs. Receipt of outside BPDUs in an RSTP or MSTP, however, can lead to network outages by triggering an STP misconfiguration. To prevent such outages, enable BPDU protection on spanning tree 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 spanning tree interface.

In this example, device 1 and device 2 are configured for RSTP. The interfaces on device 2 are edge access ports—edge access ports frequently receive outside BPDUs generated by PC applications.

This example configures interface **ge-0/0/5** and interface **ge-0/0/6** as edge ports on device 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 device 2.

Configuration

To configure BPDU protection on two access interfaces:

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, copy and paste the commands into the CLI at the **[edit]** hierarchy level, and then enter **commit** from configuration mode.

> **NOTE:** This example configures BPDU protection on specific interfaces. SRX Series devices with support for the Enhanced Layer 2 Software (ELS) configuration style, you can also configure BPDU protection globally on all spanning tree interfaces. See *Configuring BPDU Protection on Spanning Tree Interfaces* for additional information.

```
set protocols rstp interface ge-0/0/5 edge
set protocols rstp interface ge-0/0/6 edge
set protocols rstp bpdu-block-on-edge
```

Step-by-Step Procedure

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

1. Configure RSTP on interface **ge-0/0/5** and interface **ge-0/0/6**, and configure them as edge ports:

```
[edit protocols rstp]
user@host# set interface ge-0/0/5 edge
user@host# set interface ge-0/0/6 edge
```

2. Configure BPDU protection on all edge ports on this device:

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

Results

Check the results of the configuration:

```
user@host> show configuration protocols rstp
interface ge-0/0/5 {
    edge;
}
interface ge-0/0/6 {
    edge;
}
bpdu-block-on-edge;
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly:

Displaying the Interface State Before BPDU Protection Is Triggered

Purpose

Before BPDUs can be received from PCs connected to interface **ge-0/0/5** and interface **ge-0/0/6**, confirm the interface state.

Action

Use the operational mode command:

`user@host>` **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     128:513      128:513  32768.0019e2503f00     20000  BLK    DIS
```

```
ge-0/0/1     128:514      128:514  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/2     128:515      128:515  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/3     128:516      128:516  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/4     128:517      128:517  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/5     128:518      128:518  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/6     128:519      128:519  32768.0019e2503f00     20000  FWD    DESG
[output truncated]
```

Meaning

The output from the operational mode command **show spanning-tree interface** shows that **ge-0/0/5** and interface **ge-0/0/6** are ports in a forwarding state.

Verifying That BPDU Protection Is Working Correctly

Purpose

In this example, the PCs connected to device 2 start sending BPDUs to interface **ge-0/0/5** and interface **ge-0/0/6**. Verify that BPDU protection is working on the interfaces.

Action

Use the operational mode command:

`user@host>` **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     128:513      128:513  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/1     128:514      128:514  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/2     128:515      128:515  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/3     128:516      128:516  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/4     128:517      128:517  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/5     128:518      128:518  32768.0019e2503f00     20000  BLK    DIS
(Bpdu—Incon)
ge-0/0/6     128:519      128:519  32768.0019e2503f00     20000  BLK    DIS
(Bpdu—Incon)
ge-0/0/7     128:520        128:1  16384.00aabbcc0348     20000  FWD    ROOT
ge-0/0/8     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** and interface **ge-0/0/6** on device 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 reenable the interface. However, if the **disable-timeout (Spanning Trees)** 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** to unblock and reenable the interface.

If the PCs connected to device 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 is sending BPDUs to device 2.

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

IN THIS SECTION

EX Series and QFX Series switches provide Layer 2 loop prevention through 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 switches within a spanning-tree topology receive BPDUs from other devices, network outages can occur because of STP miscalculations.

This example configures BPDU protection on an EX Series switch that uses 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 software and hardware components:

- Two EX Series switches in an RSTP topology
- Junos OS Release 13.2X50-D10 or later or later for EX Series or QFX Series switches

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

- RSTP enabled on the switches.

> **NOTE:** By default, RSTP is enabled on all EX Series switches.

Overview and Topology

The switches, being in an RSTP topology, support a loop-free network through the exchange of BPDUs. Receipt of outside BPDUs in an RSTP or MSTP topology, however, can lead to network outages by triggering an STP misconfiguration. To prevent such outages, enable BPDU protection on spanning tree 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 spanning tree interface.

Figure 6 on page 206 shows the topology for this example. In this example, Switch 1 and Switch 2 are configured for RSTP and create a loop-free topology. The interfaces on Switch 2 are edge access ports—edge access ports frequently receive outside BPDUs generated by PC applications.

This example configures interface **ge-0/0/5** and interface **ge-0/0/6** as edge ports on Switch 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 Switch 2.

Figure 6: BPDU Protection Topology

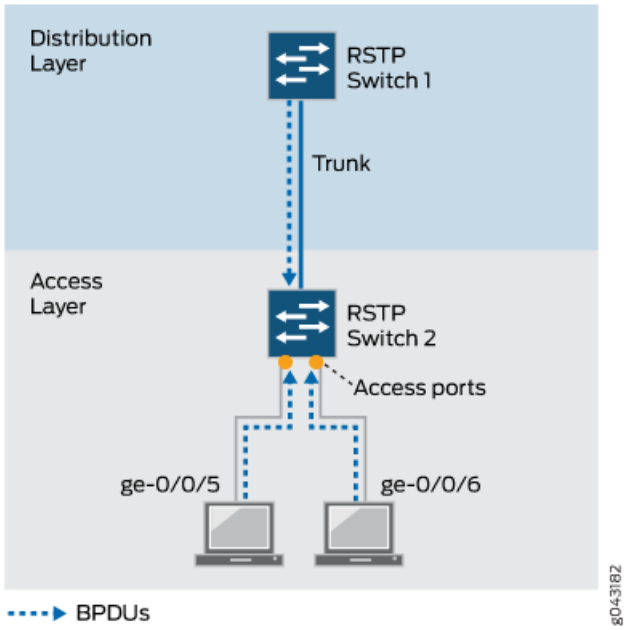


Table 10 on page 206 shows the components that will be configured for BPDU protection.

Table 10: Components of the Topology for Configuring BPDU Protection on EX Series Switches

Property	Settings
Switch 1 (Distribution Layer)	Switch 1 is connected to Switch 2 on a trunk interface.
Switch 2 (Access Layer)	Switch 2 has these access ports that require BPDU protection: • **ge-0/0/5** • **ge-0/0/6**

This configuration example uses RSTP topology. You also can configure BPDU protection for MSTP topologies at the [**edit protocols mstp**] hierarchy level.

Configuration

To configure BPDU protection on two access interfaces:

CLI Quick Configuration

Quickly configure RSTP on the two Switch 2 interfaces, and then configure BPDU protection on all edge ports on Switch 2 by copying the following commands and pasting them into the switch terminal window:

> **NOTE:** This example configures BPDU protection on specific interfaces. Starting with Junos OS Release 15.1 for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can also configure BPDU protection globally on all spanning tree interfaces. See "Configuring BPDU Protection on Switch Spanning Tree Interfaces" on page 179 for additional information.

```
[edit]
```

set protocols rstp interface ge-0/0/5 edge
set protocols rstp interface ge-0/0/6 edge
set protocols rstp bpdu-block-on-edge

Step-by-Step Procedure

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

1. Configure RSTP on interface **ge-0/0/5** and interface **ge-0/0/6**, and configure them as edge ports:

   ```
   [edit protocols rstp]
   user@switch# set interface ge-0/0/5 edge
   user@switch# set interface ge-0/0/6 edge
   ```

2. Configure BPDU protection on all edge ports on this switch:

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

Results

Check the results of the configuration:

```
user@switch> show configuration protocols rstp
interface ge-0/0/5 {
    edge;
}
interface ge-0/0/6 {
    edge;
}
bpdu-block-on-edge;
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly:

Displaying the Interface State Before BPDU Protection Is Triggered

Purpose

Before BPDUs can be received from PCs connected to interface **ge-0/0/5** and interface **ge-0/0/6**, confirm the interface state.

Action

Use the operational mode command:

```
user@switch> 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     128:513      128:513  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/1     128:514      128:514  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/2     128:515      128:515  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/3     128:516      128:516  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/4     128:517      128:517  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/5     128:518      128:518  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/6     128:519      128:519  32768.0019e2503f00     20000  FWD    DESG
[output truncated]
```

Meaning

The output from the operational mode command **show spanning-tree interface** shows that **ge-0/0/5** and interface **ge-0/0/6** are ports in a forwarding state.

Verifying That BPDU Protection Is Working Correctly

Purpose

In this example, the PCs connected to Switch 2 start sending BPDUs to interface **ge-0/0/5** and interface **ge-0/0/6**. Verify that BPDU protection is working on the interfaces.

Action

Use the operational mode command:

```
user@switch>  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     128:513      128:513  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/1     128:514      128:514  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/2     128:515      128:515  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/3     128:516      128:516  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/4     128:517      128:517  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/5     128:518      128:518  32768.0019e2503f00     20000  BLK    DIS
(Bpdu—Incon)
ge-0/0/6     128:519      128:519  32768.0019e2503f00     20000  BLK    DIS
(Bpdu—Incon)
ge-0/0/7     128:520        128:1  16384.00aabbcc0348     20000  FWD    ROOT
ge-0/0/8     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** and interface **ge-0/0/6** on Switch 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 reenable 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** to unblock and reenable the interface.

If the PCs connected to Switch 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 is sending BPDUs to Switch 2.

Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches

IN THIS SECTION

EX Series switches provide Layer 2 loop prevention through 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 switches within a spanning-tree topology receive BPDUs from other devices, network outages can occur because of STP miscalculations.

This example configures BPDU protection on an EX Series switch that uses 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 EX Series switches in an RSTP topology
- Junos OS Release 9.1 or later for EX Series switches

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

- RSTP enabled on the switches.

> **NOTE:** By default, RSTP is enabled on all EX Series switches.

Overview and Topology

The switches, 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 7 on page 211 shows the topology for this example. In this example, Switch 1 and Switch 2 are configured for RSTP and create a loop-free topology. The interfaces on Switch 2 are edge access ports—edge access ports 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 Switch 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 Switch 2.

Figure 7: BPDU Protection Topology

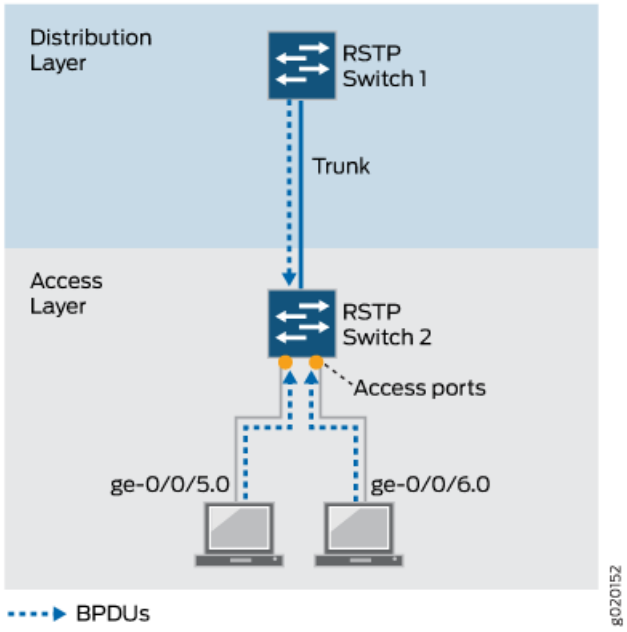


Table 11 on page 211 shows the components that will be configured for BPDU protection.

Table 11: Components of the Topology for Configuring BPDU Protection on EX Series Switches

Property	Settings
Switch 1 (Distribution Layer)	Switch 1 is connected to Switch 2 on a trunk interface.

Table 11: Components of the Topology for Configuring BPDU Protection on EX Series Switches *(continued)*

Property	Settings
Switch 2 (Access Layer)	Switch 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** | **stp**)] hierarchy level.

Configuration

To configure BPDU protection on two access interfaces:

CLI Quick Configuration

Quickly configure RSTP on the two Switch 2 interfaces, and then configure BPDU protection on all edge ports on Switch 2 by copying the following commands and pasting them into the switch terminal window:

```
[edit]
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
```

Step-by-Step Procedure

To configure RSTP on the two Switch 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@switch# set interface ge-0/0/5.0 edge
   user@switch# set interface ge-0/0/6.0 edge
   ```

2. Configure BPDU protection on all edge ports on this switch:

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

Results

Check the results of the configuration:

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

Verification

IN THIS SECTION

To confirm that the configuration is working properly:

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:

```
user@switch>  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 operational mode command **show spanning-tree interface** shows that **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 Switch 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:

```
user@switch>  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 Switch 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 ethernet-switching bpdu-error interface** to unblock and re-enable the interface.

If the PCs connected to Switch 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 is sending BPDUs to Switch 2.

Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches

IN THIS SECTION

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches" on page 221. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

Spanning-tree protocols support loop-free network communication through the exchange of a special type of frame called a bridge protocol data unit (BPDU). However, when BPDUs generated by spanning-tree protocols are communicated to devices on which spanning-tree protocols are not configured, these devices recognize the BPDUs, which can lead to network outages. You can, however, enable BPDU protection on switch interfaces to prevent BPDUs generated by spanning-tree protocols from passing through those interfaces. When BPDU protection is enabled, an interface shuts down when any incompatible BPDU is encountered, thereby preventing the BPDUs generated by spanning-tree protocols from reaching the switch.

This example configures BPDU protection on STP switch downstream interfaces that connect to two PCs:

Requirements

This example uses the following software and hardware components:

- One EX Series switch in an RSTP topology
- One EX Series switch that is not in any spanning-tree topology
- Junos OS Release 13.2X50-D10 or later or later for EX Series switches

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

- Ensured that RSTP is operating on Switch 1.
- Disabled RSTP on Switch 2

> **NOTE:** By default, RSTP is enabled on all EX Series switches.

Overview and Topology

EX Series switches provide Layer 2 loop prevention through Rapid Spanning Tree protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). All spanning-tree protocols use a special type of frame called a BPDU to communicate. Other devices also use BPDUs—PC bridging applications, for example, 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 switches within a spanning-tree topology receive BPDUs from other devices, network outages can occur because of the miscalculations caused by the outside BPDUs. Therefore, you must configure BPDU protection on interfaces in a spanning-tree topology to avoid network outages.

This example explains how to block outside BPDUs from reaching a switch interface connected to devices that are not part of the STP topology. In this scenario, an interface is shutdown when it encounters an outside BPDU.

Figure 8 on page 217 shows the topology for this example. Switch 1 and Switch 2 are connected through a trunk interface. Switch 1 is configured for RSTP and Switch 2 does not have a spanning-tree protocol configured on it.

This example configures downstream BPDU protection on Switch 2 interfaces **ge-0/0/5** and **ge-0/0/6**. When BPDU protection is enabled, the switch interfaces will shut down if BPDUs generated by the laptops attempt to access Switch 2.

CAUTION: When configuring BPDU protection on an interface without spanning trees connected to a switch with spanning trees, be careful that you do not configure BPDU protection on **all** interfaces. Doing so could prevent BPDUs being received on switch interfaces (such as a trunk interface) that you intended to have receive BPDUs from a switch with spanning trees.

Figure 8: BPDU Protection Topology

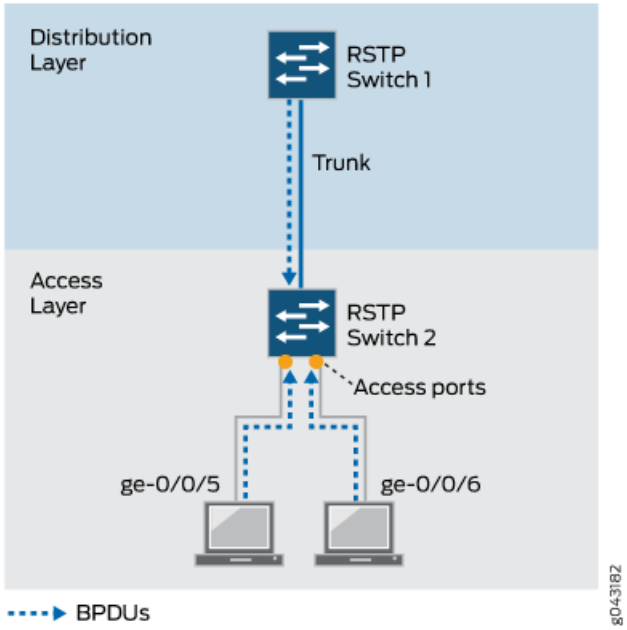


Table 12 on page 217 shows the components that will be configured for BPDU protection.

Table 12: Components of the Topology for Configuring BPDU Protection on EX Series Switches

Property	Settings
Switch 1 (Distribution Layer)	Switch 1 is connected to Switch 2 through a trunk interface. Switch 1 is configured for RSTP.
Switch 2 (Access Layer)	Switch 2 has two downstream access ports connected to laptops: • **ge-0/0/5** • **ge-0/0/6**

Configuration

To configure BPDU protection on the interfaces:

CLI Quick Configuration

This configuration causes the interface to automatically shutdown if it receives BPDUs. To quickly configure BPDU protection on Switch 2 , copy the following commands and paste them into the switch terminal window:

> **NOTE:** This example configures BPDU protection on specific interfaces. However, starting with Junos OS Release 15.1 for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can configure BPDU protection globally on all spanning tree interfaces. See "Configuring BPDU Protection on Switch Spanning Tree Interfaces" on page 179 for additional information.

```
[edit]
user@switch# set protocols layer2-control bpdu-block interface ge-0/0/5

[edit]
user@switch# set protocols layer2-control bpdu-block interface ge-0/0/6
```

Step-by-Step Procedure

To configure BPDU protection for automatic shutdown.

1. To shutdown the BPDU interface on the downstream interface **ge-0/0/5** on Switch 2:

   ```
   [edit protocol layer 2]
   user@switch# set bpdu-block interface ge-0/0/5
   ```

2. To shutdown the BPDU interface on the downstream interface **ge-0/0/6** on Switch 2:

   ```
   [edit protocol layer 2]
   user@switch# set bpdu-block interface ge-0/0/6
   ```

Results

Check the results of the configuration:

```
user@switch> show protocol layer 2
bpdu-block {
   interface ge-0/0/5 {
```

```
    interface ge-0/0/6 {
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Displaying the Interface State Before BPDU Protection Is Triggered

Purpose

Before any BPDUs can be received on Switch 2 on either interface **ge-0/0/5** or interface **ge-0/0/6**, confirm the state of those interfaces.

Action

Use the operational mode command **show interfaces extensive <interface name>**:

`user@switch>` **show interfaces extensive ge-0/0/5**

```
Physical interface: ge-0/0/5, Enabled, Physical link is Down
  Interface index: 659, SNMP ifIndex: 639, Generation: 161
  Link-level type: Ethernet, MTU: 1514, MRU: 0, Link-mode: Auto, Speed: Auto,
  BPDU Error: Detected, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled,
  Remote fault: Online, Media type: Copper,
  IEEE 802.3az Energy Efficient Ethernet: Disabled
  Device flags   : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 12 supported, 12 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
```

Meaning

The output from the operational mode command **show interfaces extensive** shows that **ge-0/0/5** a is enabled.

Verifying That BPDU Shutdown Protection Is Working Correctly

Purpose

Verify that BPDU protection is working correctly in the network by checking to see whether BPDUs have been blocked appropriately.

Action

Issue **show interfaces extensive <interface name>** to see what happened when the BPDUs reached the two interfaces configured for BPDU protection on Switch 2:

```
user@switch>  show interfaces extensive ge-0/0/5
```

```
Physical interface: ge-0/0/5, Enabled, Physical link is Down
  Interface index: 659, SNMP ifIndex: 639, Generation: 161
  Link-level type: Ethernet, MTU: 1514, MRU: 0, Link-mode: Auto, Speed: Auto,
  BPDU Error: Detected, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled,
  Remote fault: Online, Media type: Copper,
  IEEE 802.3az Energy Efficient Ethernet: Disabled
  Device flags   : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 12 supported, 12 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
```

Meaning

When the BPDUs sent from laptops reached interface **ge-0/0/5** on Switch 2, the interface transitioned to a BPDU inconsistent state, shutting down the interface to prevent BPDUs from reaching the laptops.

You need to reenable the blocked interface. There are two ways to do this. If you included the statement **disable-timeout(Spanning Trees)** in the BPDU configuration, the interface returns to service after the timer expires. Otherwise, use the operational mode command **clear error bpdu interface *interface-name*** to unblock and reenable **ge-0/0/5**. This command will only reenable an interface but the BPDU configuration for the interface will continue to exist unless you remove the BPDU configuration explicitly.

If BPDUs reach the downstream interface on Switch 2 again, BPDU protection is triggered again and the interface shuts down. In such cases, you must find and repair the misconfiguration that is sending BPDUs to interface **ge-0/0/5** .

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;
}
```

SEE ALSO

Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network | **259**

Checking the Status of Spanning-Tree Instance Interfaces | **281**

Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches

IN THIS SECTION

NOTE: This example uses Junos OS for EX Series switches without support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see "Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches" on page 215. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

Spanning-tree protocols support loop-free network communication through the exchange of a special type of frame called a bridge protocol data unit (BPDU). However, when BPDUs generated by spanning-tree protocols are communicated to devices on which spanning-tree protocols are not configured, these devices recognize the BPDUs, which can lead to network outages. You can, however, enable BPDU protection on switch interfaces to prevent BPDUs generated by spanning-tree protocols from passing through those interfaces. When BPDU protection is enabled, an interface shuts down or drops BPDU packets when any incompatible BPDU is encountered, thereby preventing the BPDUs generated by spanning-tree protocols from reaching the switch. When an interface is configured to drop BPDU packets, all traffic except the incompatible BPDUs can pass through the interface.

> **NOTE:** The BPDU drop feature can be specified only on interfaces on which no spanning-tree protocol is configured.

This example configures BPDU protection on STP switch downstream interfaces that connect to two PCs:

Requirements

This example uses the following hardware and software components:

- One EX Series switch in an RSTP topology
- One EX Series switch that is not in any spanning-tree topology
- Junos OS Release 9.1 or later for EX Series switches

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

- Ensured that RSTP is operating on Switch 1.
- Disabled or enabled RSTP on Switch 2 (depending on the configuration that you plan to implement.)

  If you want to enable the BPDU shutdown feature, then it is optional to disable spanning-tree protocols on the interface.

> **NOTE:** By default, RSTP is enabled on all EX Series switches.

Overview and Topology

EX Series switches provide Layer 2 loop prevention through 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 BPDU to communicate. Other devices also use BPDUs—PC bridging applications, for example, 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 switches within a spanning-tree topology receive BPDUs from other devices, network outages can occur because of the miscalculations caused by the outside BPDUs. Therefore, you must configure BPDU protection on interfaces in a spanning-tree topology to avoid network outages.

This example explains how to block outside BPDUs from reaching a switch interface connected to devices that are not part of the STP topology. This example addresses two scenarios. In the first scenario, an interface is shutdown when it encounters an outside BPDU. In the second scenario, an interface drops only BPDU packets while retaining the status of the interface as up and allowing all other traffic to pass through the interface.

Figure 9 on page 224 shows the topology for this example. Switch 1 and Switch 2 are connected through a trunk interface. Switch 1 is configured for RSTP while Switch 2 has a spanning-tree protocol configured on it for the first scenario, and does not have a spanning-tree protocol configured on it for the second scenario.

In the first scenario, this example configures downstream BPDU protection on Switch 2 interfaces **ge-0/0/5.0** and **ge-0/0/6.0** when the default spanning-tree protocol (RSTP) is not disabled on these interfaces. When BPDU protection is enabled with the **shutdown** statement, the switch interfaces will shut down if BPDUs generated by the laptops attempt to access Switch 2.

In the second scenario, this example configures downstream BPDU protection on Switch 2 interfaces **ge-0/0/5.0** and **ge-0/0/6.0** when the default spanning-tree protocol (RSTP) is disabled on these interfaces. When BPDU protection is enabled with the **drop** statement, the switch interfaces drop only the BPDUs while allowing remaining traffic to pass through and retaining their status as up if BPDUs generated by the laptops attempt to access Switch 2.

CAUTION: When configuring BPDU protection on an interface without spanning trees connected to a switch with spanning trees, be careful that you do not configure BPDU protection on **all** interfaces. Doing so could prevent BPDUs being received on switch interfaces (such as a trunk interface) that you intended to have receive BPDUs from a switch with spanning trees.

Figure 9: BPDU Protection Topology

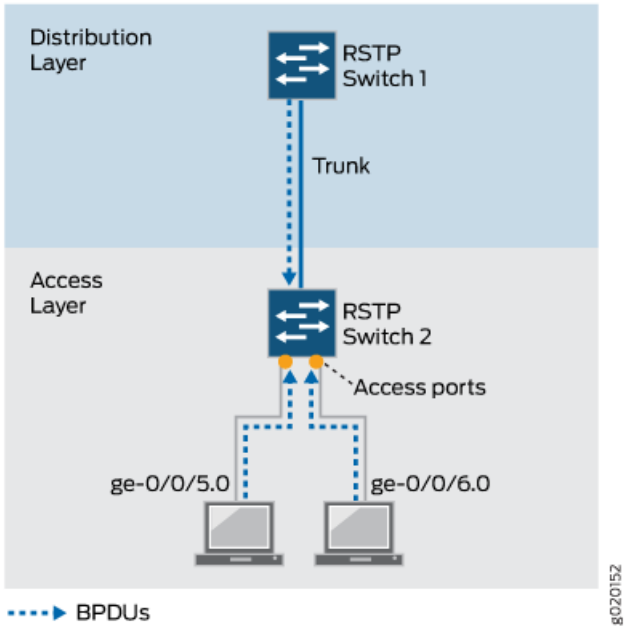


Table 13 on page 224 shows the components that will be configured for BPDU protection.

Table 13: Components of the Topology for Configuring BPDU Protection on EX Series Switches

Property	Settings
Switch 1 (Distribution Layer)	Switch 1 is connected to Switch 2 through a trunk interface. Switch 1 is configured for RSTP.
Switch 2 (Access Layer)	Switch 2 has two downstream access ports connected to laptops: • **ge-0/0/5.0** • **ge-0/0/6.0**

Configuration

To configure BPDU protection on the interfaces:

CLI Quick Configuration

This is the first scenario that explains configuration for the **shutdown** statement. To quickly configure BPDU protection on Switch 2 for the **shutdown** statement, copy the following commands and paste them into the switch terminal window:

```
[edit]
```

```
user@switch# set ethernet-switching-options bpdu-block interface ge-0/0/5.0 shutdown

[edit]
user@switch# set ethernet-switching-options bpdu-block interface ge-0/0/6.0 shutdown
```

Step-by-Step Procedure

To configure BPDU protection for the **shutdown** statement:

1. Configure the BPDU **shutdown** statement on the downstream interface **ge-0/0/5.0** on Switch 2:

   ```
   [edit ethernet-switching-options]
   user@switch# set bpdu-block interface ge-0/0/5.0 shutdown
   ```

2. Configure the BPDU **shutdown** statement on the downstream interface **ge-0/0/6.0** on Switch 2:

   ```
   [edit ethernet-switching-options]
   user@switch# set bpdu-block interface ge-0/0/6.0 shutdown
   ```

Results

Check the results of the configuration:

```
user@switch> show ethernet-switching-options
bpdu-block {
    interface ge-0/0/5.0 {
        shutdown;
        }
    interface ge-0/0/6.0 {
        shutdown;
        }
}
```

CLI Quick Configuration

This is the second scenario that explains configuration for the **drop** statement. To quickly configure BPDU protection on Switch 2 for the **drop** statement, copy the following commands and paste them into the switch terminal window:

```
[edit]
user@switch# set protocols rstp interface ge-0/0/5.0 disable
user@switch# set protocols rstp interface ge-0/0/6.0 disable
user@switch# set ethernet-switching-options bpdu-block interface ge-0/0/5.0 drop
user@switch# set ethernet-switching-options bpdu-block interface ge-0/0/6.0 drop
```

> **NOTE:** You can also disable RSTP globally using the **delete protocols rstp**, the **set protocols rstp disable**, or the **set protocols rstp interface all disable** command.

Step-by-Step Procedure

To configure BPDU protection for the **drop** statement:

1. Disable RSTP on both the interfaces **ge-0/0/5.0** and **ge-0/0/6.0** interfaces:

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

2. Configure the BPDU **drop** statement on the downstream interface **ge-0/0/5.0** on Switch 2:

```
[edit ethernet-switching-options]
user@switch# set bpdu-block interface ge-0/0/5.0 drop
```

3. Configure the BPDU **drop** statement on the downstream interface **ge-0/0/6.0** on Switch 2:

```
[edit ethernet-switching-options]
user@switch# set bpdu-block interface ge-0/0/6.0 drop
```

Results

Check the results of the configuration:

```
user@switch> show protocols rstp
interface ge-0/0/5.0 {
    disable;
}
interface ge-0/0/6.0 {
    disable;
}
user@switch> show ethernet-switching-options
bpdu-block {
    interface ge-0/0/5.0 {
        drop;
        }
    interface ge-0/0/6.0 {
        drop;
        }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Displaying the Interface State Before BPDU Protection Is Triggered

Purpose

Before any BPDUs can be received on Switch 2 on either interface **ge-0/0/5.0** or interface **ge-0/0/6.0**, confirm the state of those interfaces.

Action

Use the operational mode command **show ethernet-switching interfaces**:

```
user@switch>  show ethernet-switching interfaces
```

```
Interface    State  VLAN members     Tag   Tagging    Blocking
ge-0/0/5.0   up     default               untagged   unblocked
ge-0/0/6.0   up     default               untagged   unblocked
```

Meaning

The output from the operational mode command **show ethernet-switching interfaces** shows that **ge-0/0/5.0** and interface **ge-0/0/6.0** are **up** and unblocked.

Verifying That BPDU Shutdown Protection Is Working Correctly

Purpose

Verify that BPDU protection is working correctly in the network by checking to see whether BPDUs have been blocked appropriately.

Action

Issue **show ethernet-switching interfaces** to see what happened when the BPDUs reached the two interfaces configured for BPDU protection on Switch 2:

```
user@switch>  show ethernet-switching interfaces
```

```
Interface    State  VLAN members     Tag   Tagging     Blocking
ge-0/0/5.0   down   default                 untagged    Disabled by bpdu-control
ge-0/0/6.0   down   default                 untagged    Disabled by bpdu-control
```

Meaning

When the BPDUs sent from laptops reached interfaces **ge-0/0/5.0** and **ge-0/0/6.0** on Switch 2, the interfaces transitioned to a BPDU inconsistent state, shutting down the two interfaces to prevent BPDUs from reaching the laptops.

You need to re-enable the blocked interfaces. There are two ways to do this. If you included the statement **disable-timeout** in the BPDU configuration, the interface returns to service after the timer expires. Otherwise, use the operational mode command **clear ethernet-switching bpdu-error interface** to unblock and re-enable **ge-0/0/5.0** and **ge-0/0/5.0**. This command will only re-enable an interface but the BPDU configuration for the interface will continue to exist unless you remove the BPDU configuration explicitly.

If BPDUs reach the downstream interfaces on Switch 2 again, BPDU protection is triggered again and the interfaces shut down. In such cases, you must find and repair the misconfiguration that is sending BPDUs to interfaces **ge-0/0/5.0** and **ge-0/0/6.0**.

Verifying That BPDU Drop Protection Is Working Correctly

Purpose

Verify that BPDU drop protection is working correctly in the network by checking to see whether BPDUs have been blocked appropriately.

Action

Issue **show ethernet-switching interfaces** to see what happened when the BPDUs reached the two interfaces configured for BPDU protection on Switch 2:

```
user@switch>  show ethernet-switching interfaces
```

```
Interface    State  VLAN members     Tag   Tagging  Blocking
ge-0/0/5.0   up     default               untagged unblocked-xSTP bpdu
                                                  filter enabled
ge-0/0/6.0   up     default               untagged unblocked-xSTP bpdu
                                                  filter enabled
```

Meaning

When the BPDUs sent from laptops reached interfaces **ge-0/0/5.0** and **ge-0/0/6.0** on Switch 2, the interfaces dropped those BPDUs to prevent them from reaching Switch 2, and the state of both the interfaces is **up**.

5
CHAPTER

Loop Protection for Spanning-Tree Protocols

Loop Protection for Spanning-Tree Protocols

IN THIS SECTION

Understanding Loop Protection for Spanning-Tree Instance Interfaces

IN THIS SECTION

Loop protection increases the efficiency of STP, RSTP, and MSTP by preventing ports from moving into a forwarding state that would result in a loop opening up in the network. 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.

How Does Loop Protection Work?

A loop-free network in spanning-tree topologies is supported through the exchange of a special type of frame called bridge protocol data unit (BPDU). Peer STP applications running on the switch interfaces use BPDUs to communicate. Ultimately, the exchange of BPDUs determines which interfaces block traffic (preventing loops) and which interfaces become root ports and forward traffic.

However, a blocking interface can transition to the forwarding state in error if the interface stops receiving BPDUs from its designated port on the segment. Such a transition error can occur when there is a hardware error on the switch or software configuration error between the switch and its neighbor.

When loop protection is enabled, the spanning-tree topology detects root ports and blocked ports and makes sure both keep receiving BPDUs. If a loop-protection-enabled interface stops receiving BPDUs from its designated port, it reacts as it would react to a problem with the physical connection on this interface. It does not transition the interface to a forwarding state, but instead transitions it to a loop-inconsistent state. The interface recovers and then it transitions back to the spanning-tree blocking state as soon as it receives a BPDU.

Benefits of Loop Protection on STP Protocols

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.

What Action Causes a Loop?

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.

What Can Loop Protection Do When BPDUs Don't Arrive?

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.

When Should I Use Loop Protection?

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.

We recommend that you enable loop protection on all switch interfaces that have a chance of becoming root or designated ports. Loop protection is most effective when enabled in the entire switched network. When you enable loop protection, you must configure at least one action (log, block, or both).

> **NOTE:** An interface can be configured for either loop protection or root protection, but not for both.

What Happens if I Do Not Use Loop Protection?

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.

Eliminating Bridge Loops in Ethernet LANs with Spanning Tree Protocol

IN THIS SECTION

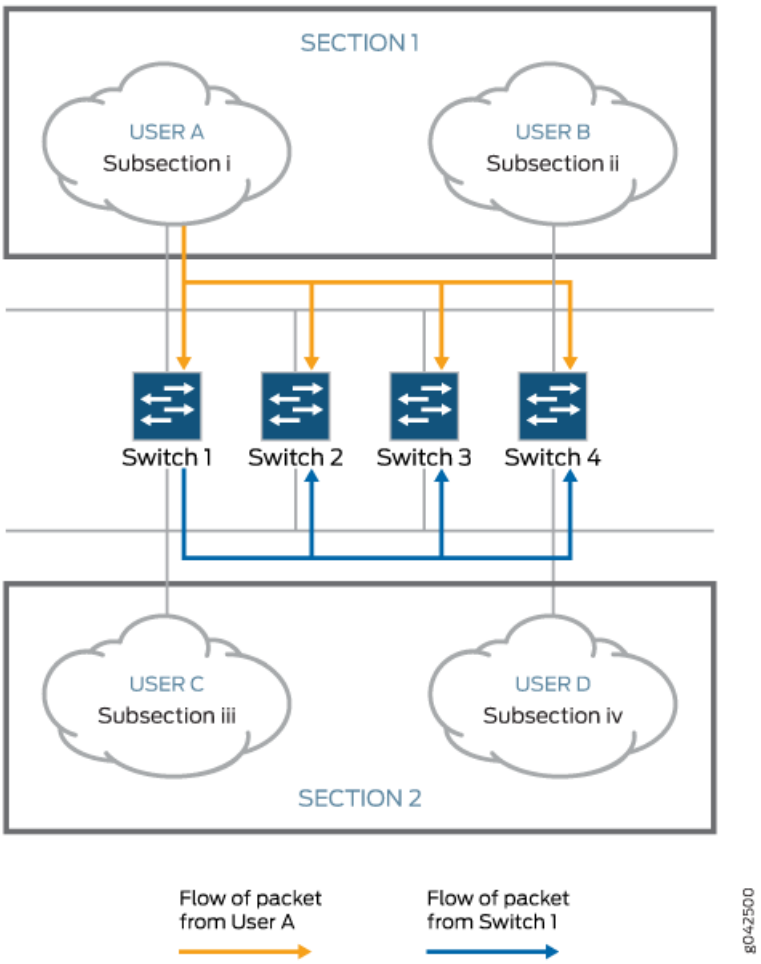
The Spanning Tree Protocol (STP) is a network protocol that is used to eliminate bridge loops in Ethernet LANs. STP prevents network loops and associated network outage by blocking redundant links or paths. The redundant paths can be used to keep the network operational if the primary link fails.

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 10 on page 235). 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 10: 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:

Table 14: Switches Make Entries in Respective Bridging Tables

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:

Table 15: Bridging Tables Updated with Incorrect Information

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 10 on page 235, 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:

Table 16: Switch 1 Updates Its Bridging 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.

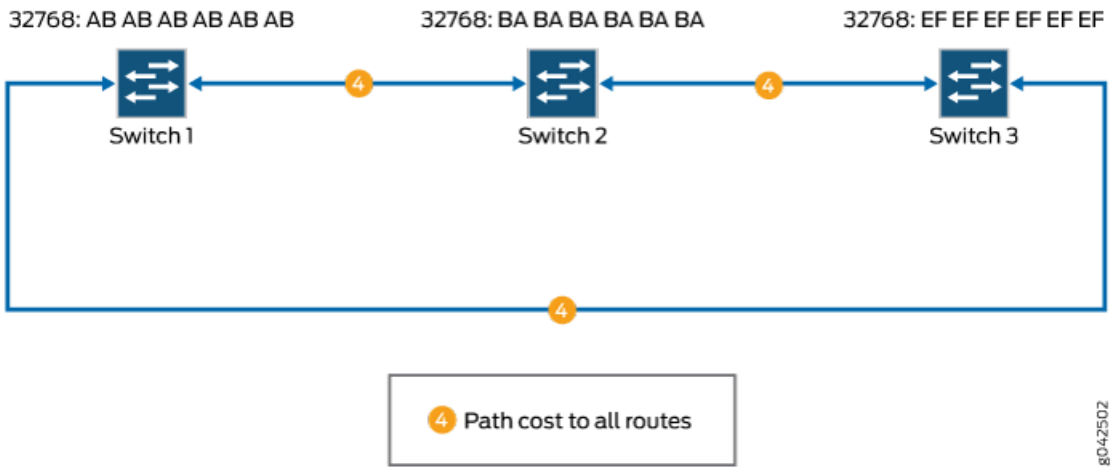
How STP Helps Eliminate Loops

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 11 on page 237). 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.

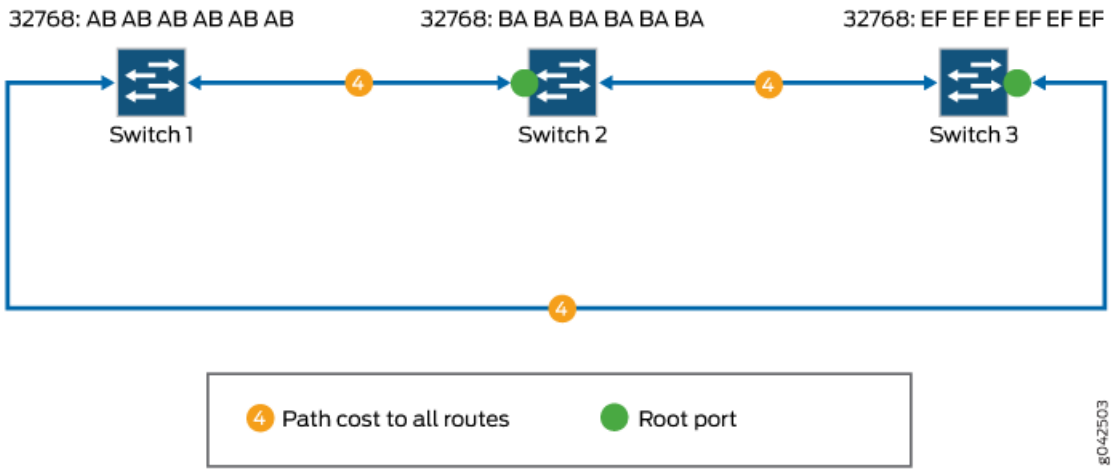
Figure 11: Simple Network with Redundant Links



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

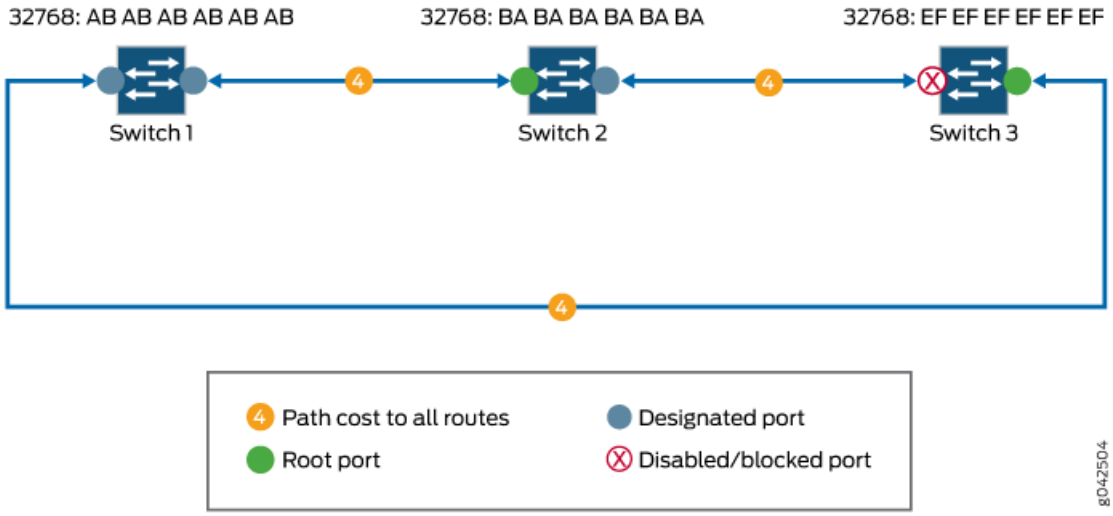
1. *Elects a root bridge (or switch).* To elect a root switch, STP uses the bridge ID. The bridge ID is 8 bytes in length and consists of two parts. The first part is 2 bytes of information known as bridge priority. The default bridge priority is 32,768. In this example, the default value is used for 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 12 on page 238. Similarly, for Switch 3, the root port is the one that uses the direct path from Switch 1.

Figure 12: 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 13 on page 238, the designated ports are marked.

Figure 13: 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 5G Universal Routing Platforms 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.

NOTE: All virtual switch routing instances configured on an MX Series router are supported using only one spanning-tree process. The Layer 2 control protocol process is named l2cpd.

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.

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.

Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on non-ELS EX Series Switches

IN THIS SECTION

EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). Loop protection increases the efficiency of STP, RSTP, and MSTP by preventing interfaces from moving into a forwarding state that would result in a loop opening up in the network.

This example describes how to configure loop protection for an interface on an EX Series switch in an RSTP topology:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- Three EX Series switches in an RSTP topology

Before you configure the interface for loop protection, be sure you have:

- RSTP operating on the switches.

> **NOTE:** By default, RSTP is enabled on all EX Series switches.

Overview and Topology

A loop-free network in spanning-tree topologies is supported through the exchange of a special type of frame called bridge protocol data unit (BPDU). Peer STP applications running on the switch interfaces use BPDUs to communicate. Ultimately, the exchange of BPDUs determines which interfaces block traffic (preventing loops) and which interfaces become root ports and forward traffic.

A blocking interface can transition to the forwarding state in error if the interface stops receiving BPDUs from its designated port on the segment. Such a transition error can occur when there is a hardware error on the switch or software configuration error between the switch and its neighbor. When this happens, a loop opens up in the spanning tree. Loops in a Layer 2 topology cause broadcast, unicast, and multicast frames to continuously circle the looped network. As a switch processes a flood of frames in a looped network, its resources become depleted and the ultimate result is a network outage.

> **CAUTION:** An interface can be configured for either loop protection or root protection, but not for both.

Three EX Series switches are displayed in Figure 14 on page 244. In this example, they are configured for RSTP and create a loop-free topology. Interface **ge-0/0/6** is blocking traffic between Switch 3 and Switch 1; thus, traffic is forwarded through interface **ge-0/0/7** on Switch 2. BPDUs are being sent from the root bridge on Switch 1 to both of these interfaces.

This example shows how to configure loop protection on interface **ge-0/0/6** to prevent it from transitioning from a blocking state to a forwarding state and creating a loop in the spanning-tree topology.

Figure 14: Network Topology for Loop Protection

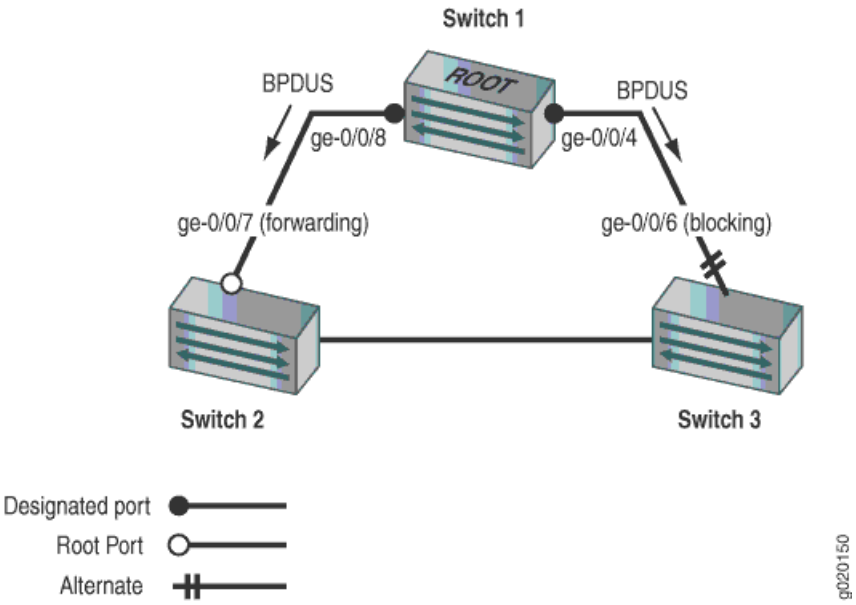


Table 17 on page 244 shows the components that will be configured for loop protection.

Table 17: Components of the Topology for Configuring Loop Protection on EX Series Switches

Property	Settings
Switch 1	Switch 1 is the root bridge.
Switch 2	Switch 2 has the root port **ge-0/0/7**.
Switch 3	Switch 3 is connected to Switch 1 through interface **ge-0/0/6**.

A spanning-tree topology contains ports that have specific roles:

- The *root port* is responsible for forwarding data to the root bridge.
- The *alternate port* is a standby port for the root port. When a root port goes down, the alternate port becomes the active root port.
- The *designated port* forwards data to the downstream network segment or device.

This configuration example uses an RSTP topology. However, you also can configure loop protection for STP or MSTP topologies at the [**edit protocols** (**mstp** | **stp**)] hierarchy level.

Configuration

To configure loop protection on an interface:

CLI Quick Configuration

To quickly configure loop protection on interface **ge-0/0/6**:

```
[edit]
set protocols rstp interface ge-0/0/6 bpdu-timeout-action block
```

Step-by-Step Procedure

To configure loop protection:

1. Configure interface **ge-0/0/6** on Switch 3:

```
[edit protocols rstp]
user@switch# set interface ge-0/0/6 bpdu-timeout-action block
```

Results

Check the results of the configuration:

```
user@switch> show configuration protocols rstp
interface ge-0/0/6.0 {
    bpdu-timeout-action {
        block;
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Displaying the Interface State Before Loop Protection Is Triggered

Purpose

Before loop protection is triggered on interface **ge-0/0/6**, confirm that the interface is blocking.

Action

Use the operational mode command:

```
user@switch>  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        128:2  16384.00aabbcc0348     20000  BLK    ALT
[output truncated]
```

Meaning

The output from the operational mode command **show spanning-tree interface** shows that **ge-0/0/6.0** is the alternate port and in a blocking state.

Verifying That Loop Protection Is Working on an Interface

Purpose

Verify the loop protection configuration on interface **ge-0/0/6**. RSTP has been disabled on interface **ge-0/0/4** on Switch 1. This will stop BPDUs from being sent to interface **ge-0/0/6** and trigger loop protection on the interface.

Action

Use the operational mode command:

```
user@switch>  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  BLK    DIS
(Loop-Incon)
[output truncated]
```

Meaning

The operational mode command **show spanning-tree interface** shows that interface **ge-0/0/6.0** has detected that BPDUs are no longer being forwarded to it and has moved into a loop-inconsistent state. The loop-inconsistent state prevents the interface from transitioning to a forwarding state. The interface recovers and transitions back to its original state as soon as it receives BPDUs.

Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches With ELS

IN THIS SECTION

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on non-ELS EX Series Switches" on page 231. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). Loop protection increases the efficiency

of STP, RSTP, and MSTP by preventing interfaces from moving into a forwarding state that would result in a loop opening up in the network.

This example describes how to configure loop protection for an interface on an EX Series switch in an RSTP topology:

Requirements

This example uses the following software and hardware components:

- Junos OS Release 13.2X50-D10 or later or later for EX Series switches
- Three EX Series switches in an RSTP topology

Before you configure the interface for loop protection, be sure you have:

- RSTP operating on the switches.

> **NOTE:** By default, RSTP is enabled on all EX Series switches.

Overview and Topology

A loop-free network in spanning-tree topologies is supported through the exchange of a special type of frame called bridge protocol data unit (BPDU). Peer STP applications running on the switch interfaces use BPDUs to communicate. Ultimately, the exchange of BPDUs determines which interfaces block traffic (preventing loops) and which interfaces become root ports and forward traffic.

A blocking interface can transition to the forwarding state in error if the interface stops receiving BPDUs from its designated port on the segment. Such a transition error can occur when there is a hardware error on the switch or software configuration error between the switch and its neighbor. When this happens, a loop opens up in the spanning tree. Loops in a Layer 2 topology cause broadcast, unicast, and multicast frames to continuously circle the looped network. As a switch processes a flood of frames in a looped network, its resources become depleted and the ultimate result is a network outage.

> **CAUTION:** An interface can be configured for either loop protection or root protection, but not for both.

Three EX Series switches are displayed in Figure 15 on page 249. In this example, they are configured for RSTP and create a loop-free topology. Interface **ge-0/0/6** is blocking traffic between Switch 3 and Switch 1; thus, traffic is forwarded through interface **ge-0/0/7** on Switch 2. BPDUs are being sent from the root bridge on Switch 1 to both of these interfaces.

This example shows how to configure loop protection on interface **ge-0/0/6** to prevent it from transitioning from a blocking state to a forwarding state and creating a loop in the spanning-tree topology.

Figure 15: Network Topology for Loop Protection

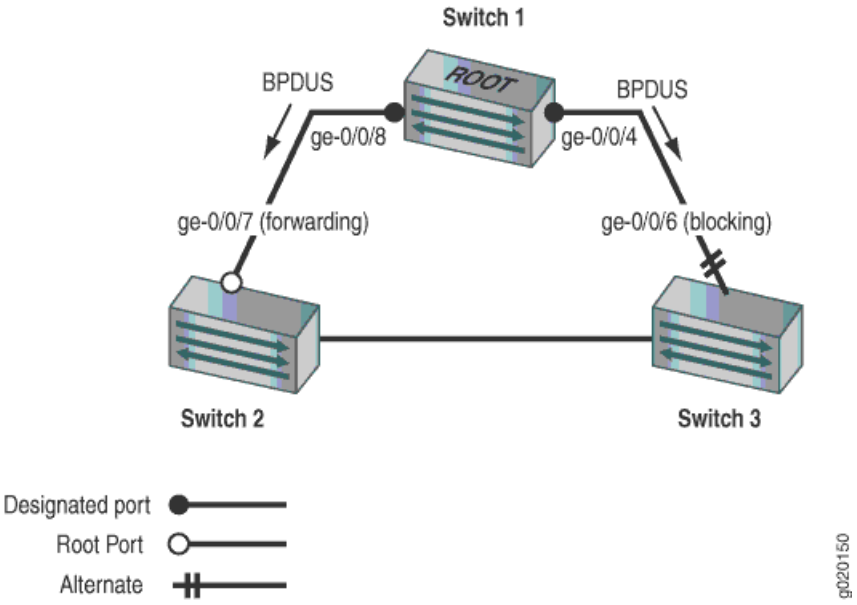


Table 18 on page 249 shows the components that will be configured for loop protection.

Table 18: Components of the Topology for Configuring Loop Protection on EX Series Switches

Property	Settings
Switch 1	Switch 1 is the root bridge.
Switch 2	Switch 2 has the root port **ge-0/0/7**.
Switch 3	Switch 3 is connected to Switch 1 through interface **ge-0/0/6**.

A spanning-tree topology contains ports that have specific roles:

- The *root port* is responsible for forwarding data to the root bridge.
- The *alternate port* is a standby port for the root port. When a root port goes down, the alternate port becomes the active root port.
- The *designated port* forwards data to the downstream network segment or device.

This configuration example uses an RSTP topology. However, you also can configure loop protection for MSTP topologies at the [**edit protocols mstp**] hierarchy level.

Configuration

To configure loop protection on an interface:

CLI Quick Configuration

To quickly configure loop protection on interface **ge-0/0/6**:

```
[edit]
set protocols rstp interface ge-0/0/6 bpdu-timeout-action block
```

Step-by-Step Procedure

To configure loop protection:

1. Configure interface **ge-0/0/6** on Switch 3:

```
[edit protocols rstp]
user@switch# set interface ge-0/0/6 bpdu-timeout-action block
```

Results

Check the results of the configuration:

```
user@switch> show configuration protocols rstp
interface ge-0/0/6 {
    bpdu-timeout-action {
        block;
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform these tasks:

Displaying the Interface State Before Loop Protection Is Triggered

Purpose

Before loop protection is triggered on interface **ge-0/0/6**, confirm that the interface is blocking.

Action

Use the operational mode command:

```
user@switch>  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     128:513      128:513  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/1     128:514      128:514  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/2     128:515      128:515  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/3     128:516      128:516  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/4     128:517      128:517  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/5     128:518      128:518  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/6     128:519        128:2  16384.00aabbcc0348     20000  BLK    ALT
[output truncated]
```

Meaning

The output from the operational mode command **show spanning-tree interface** shows that **ge-0/0/6** is the alternate port and in a blocking state.

Verifying That Loop Protection Is Working on an Interface

Purpose

Verify the loop protection configuration on interface **ge-0/0/6**. RSTP has been disabled on interface **ge-0/0/4** on Switch 1. This will stop BPDUs from being sent to interface **ge-0/0/6** and trigger loop protection on the interface.

Action

Use the operational mode command:

```
user@switch>  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     128:513      128:513  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/1     128:514      128:514  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/2     128:515      128:515  32768.0019e2503f00     20000  BLK    DIS
ge-0/0/3     128:516      128:516  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/4     128:517      128:517  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/5     128:518      128:518  32768.0019e2503f00     20000  FWD    DESG
ge-0/0/6     128:519      128:519  32768.0019e2503f00     20000  BLK    DIS
(Loop-Incon)
[output truncated]
```

Meaning

The operational mode command **show spanning-tree interface** shows that interface **ge-0/0/6** has detected that BPDUs are no longer being forwarded to it and has moved into a loop-inconsistent state. The loop-inconsistent state prevents the interface from transitioning to a forwarding state. To clear the BPDU error, issue the operational mode command **clear error bpdu interface** on the switch. The interface recovers and transitions back to its original state as soon as it receives BPDUs.

SEE ALSO

Example: Configuring Faster Convergence and Network Stability on ELS Switches with RSTP | 49

CHAPTER 6

Root Protection for VPLS Multihome Environments

Root Protection for VPLS Multihome Environments

IN THIS SECTION

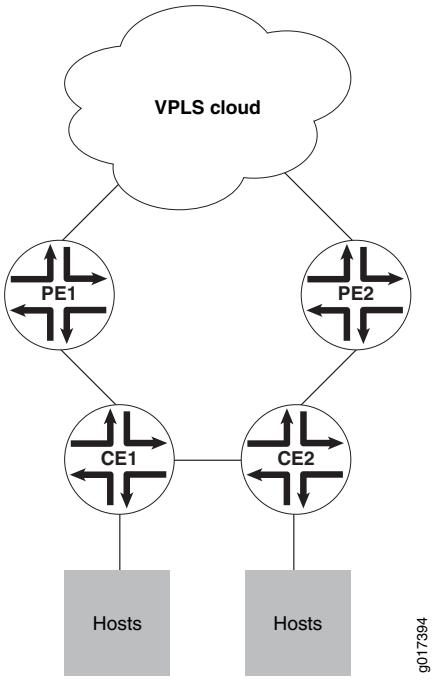
Understanding VPLS Multihoming

IN THIS SECTION

Redundancy is built into many networks through the use of alternate links and paths, which often take the shape of rings. When multiple hosts are attached to customer edge (CE) routers and provider edge (PE) routers to secure virtual private LAN service (VPLS), this technique is often called *multihoming*.

Figure 16 on page 255 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 16: Layer 2 Ring and MPLS Infrastructure Topology



Benefits of Multihoming

Multihoming multihoming is basically giving your computing device or network a presence on more than one network. When both links are up, both links are fully utilized, increasing overall throughput. If one of the links fails, the other still carries traffic so you have redundancy.

Multihoming is used in network bridges, repeaters, range extenders, firewalls, proxy servers, gateways, and when using a virtual machine, configured to use network address translation (NAT).

How Does Multihoming Work?

The two PE routers have their own links to a VPLS network service as shown in Figure 16 on page 255, 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.

The 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).

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.

VPLS Multihoming Hold Time Before Switching to Primary Priority

At a global level, each type of spanning-tree protocol has 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.

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

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.

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.

VPLS Multihoming Bridge Flush of MAC Cache on Topology Change

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 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.

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*.

VPLS Multihoming System Identifiers for Bridges in the Ring

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

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.

VPLS Multihoming Priority of the Backup Bridge

When an MX Series router or 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 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.

Understanding 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 MSTP 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.

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

IN THIS SECTION

Peer STP applications running on interfaces use BPDUs to communicate. Ultimately, the exchange of BPDUs determines which interfaces block traffic and which interfaces become root ports and forward traffic.

A root port elected through this process has the possibility of being wrongly elected. A user bridge application running on a PC can generate BPDUs, too, and interfere with root port election. This is when root protection is useful.

Benefits of Spanning Tree Protocol Root Protection

Root protection allows network administrators to manually enforce the root bridge placement in a Layer 2 switched network.

How Root Protection Works

When root protection is enabled on an interface, it is enabled for all the STP instances on that interface. 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. The interface is blocked only for instances for which it receives superior BPDUs. Otherwise, it participates in the spanning-tree topology.

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.

By default, root protect is disabled.

> **NOTE:** An interface can be configured for either root protection or loop protection, but not for both.

Where Should I Enable Root Protection?

Enable root protection on interfaces that should not receive superior bridge protocol data units (BPDUs) from the root bridge and must not be elected as the root port.

Interfaces that become designated ports are typically located on an administrative boundary. If the bridge receives superior STP BPDUs on a port that has root protection enabled, that port transitions to a root-prevented STP state (inconsistency state) and the interface is blocked. This blocking prevents a bridge that should not be the root bridge from being elected the root bridge. After the bridge stops receiving superior STP BPDUs on the interface with root protection, the interface returns to a listening state, followed by a learning state, and ultimately back to a forwarding state. Recovery back to the forwarding state is automatic.

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.

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.

Configuring VPLS Root Protection Topology Change Actions to Control Individual 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;
        }
    }
}
```

Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches

IN THIS SECTION

EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). Root protection increases the efficiency of STP, RSTP, and MSTP by allowing network administrators to manually enforce the root bridge placement in the network.

This example describes how to configure root protection on an interface on an EX Series switch:

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- Four EX Series switches in an RSTP topology

Before you configure the interface for root protection, be sure you have:

- RSTP operating on the switches.

> **NOTE:** By default, RSTP is enabled on all EX Series switches.

Overview and Topology

Peer STP applications running on switch interfaces exchange a special type of frame called a bridge protocol data unit (BPDU). Switches communicate interface information using BPDUs to create a loop-free topology that ultimately determines the root bridge and which interfaces block or forward traffic in the spanning tree.

However, a root port elected through this process has the possibility of being wrongly elected. A user bridge application running on a PC can generate BPDUs, too, and interfere with root port election.

To prevent this from happening, enable root protection on interfaces that should not receive superior BPDUs from the root bridge and should not be elected as the root port. These interfaces are typically located on an administrative boundary and are designated ports.

When root protection is enabled on an interface:

- The interface is blocked from becoming the root port.
- Root protection is enabled for all STP instances on that interface.
- The interface is blocked only for instances for which it receives superior BPDUs. Otherwise, it participates in the spanning-tree topology.

CAUTION: An interface can be configured for either root protection or loop protection, but not for both.

Four EX Series switches are displayed in Figure 17 on page 266. In this example, they are configured for RSTP and create a loop-free topology. Interface **ge-0/0/7** on Switch 1 is a designated port on an administrative boundary. It connects to Switch 4. Switch 3 is the root bridge. Interface **ge-0/0/6** on Switch 1 is the root port.

This example shows how to configure root protection on interface **ge-0/0/7** to prevent it from transitioning to become the root port.

Figure 17: Network Topology for Root Protection

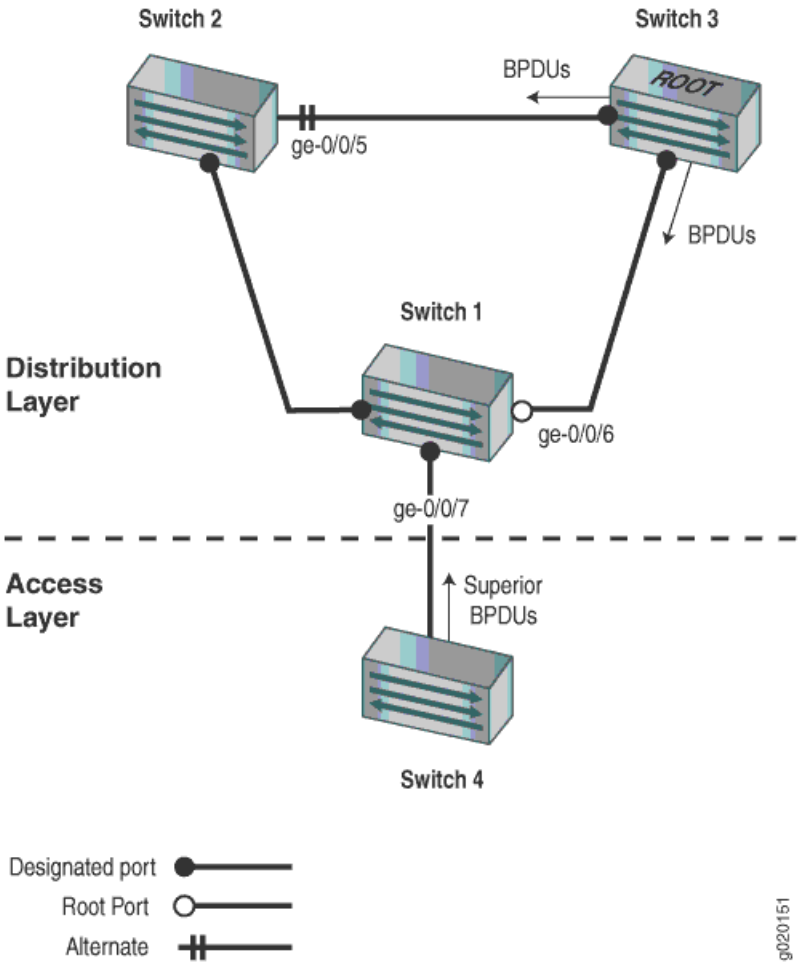


Table 19 on page 266 shows the components that will be configured for root protection.

Table 19: Components of the Topology for Configuring Root Protection on EX Series Switches

Property	Settings
Switch 1	Switch 1 is connected to Switch 4 through interface **ge-0/0/7**.
Switch 2	Switch 2 is connected to Switch 1 and Switch 3. Interface **ge-0/0/4** is the alternate port in the RSTP topology.
Switch 3	Switch 3 is the root bridge and is connected to Switch 1 and Switch 2.
Switch 4	Switch 4 is connected to Switch 1. After root protection is configured on interface **ge-0/0/7**, Switch 4 will send superior BPDUs that will trigger root protection on interface **ge-0/0/7**.

A spanning tree topology contains ports that have specific roles:

- The *root port* is responsible for forwarding data to the root bridge.
- The *alternate port* is a standby port for the root port. When a root port goes down, the alternate port becomes the active root port.
- The *designated port* forwards data to the downstream network segment or device.

This configuration example uses an RSTP topology. However, you also can configure root protection for STP or MSTP topologies at the [**edit protocols** (**mstp** | **stp**)] hierarchy level.

Configuration

To configure root protection on an interface:

CLI Quick Configuration

To quickly configure root protection on interface **ge-0/0/7**, copy the following command and paste it into the switch terminal window:

```
[edit]
set protocols rstp interface ge-0/0/7 no-root-port
```

Step-by-Step Procedure

To configure root protection:

1. Configure interface **ge-0/0/7**:

   ```
   [edit protocols rstp]
   user@switch#
   set interface ge-0/0/7 no-root-port
   ```

Results

Check the results of the configuration:

```
user@switch> show configuration protocols rstp
interface ge-0/0/7.0 {
    no-root-port;
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly:

Displaying the Interface State Before Root Protection Is Triggered

Purpose

Before root protection is triggered on interface **ge-0/0/7**, confirm the interface state.

Action

Use the operational mode command:

```
user@switch> 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        128:2  16384.00aabbcc0348     20000  BLK    ALT
ge-0/0/6.0     128:519        128:1  16384.00aabbcc0348     20000  FWD    ROOT
ge-0/0/7.0     128:520      128:520  32768.0019e2503f00     20000  FWD    DESG
[output truncated]
```

Meaning

The output from the operational mode command **show spanning-tree interface** shows that **ge-0/0/7.0** is a designated port in a forwarding state.

Verifying That Root Protection Is Working on the Interface

Purpose

A configuration change takes place on Switch 4. A smaller bridge priority on the Switch 4 causes it to send superior BPDUs to interface **ge-0/0/7**. Receipt of superior BPDUs on interface **ge-0/0/7** will trigger root protection. Verify that root protection is operating on interface **ge-0/0/7**.

Action

Use the operational mode command:

```
user@switch> 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        128:2  16384.00aabbcc0348     20000  BLK    ALT
ge-0/0/6.0     128:519        128:1  16384.00aabbcc0348     20000  FWD    ROOT
ge-0/0/7.0     128:520      128:520  32768.0019e2503f00     20000  BLK    DIS
(Root—Incon)
[output truncated]
```

Meaning

The operational mode command **show spanning-tree interface** shows that interface **ge-0/0/7.0** has transitioned to a root inconsistent state. The root inconsistent state makes the interface block, discarding any received BPDUs, and prevents the interface from becoming a candidate for the root port. When the root bridge no longer receives superior STP BPDUs from the interface, the interface will recover and transition back to a forwarding state. Recovery is automatic.

Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on EX Series Switches With ELS

IN THIS SECTION

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

EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). Root protection increases the efficiency of STP, RSTP, and MSTP by allowing network administrators to manually enforce the root bridge placement in the network.

This example describes how to configure root protection on an interface on an EX Series switch:

Requirements

This example uses the following software and hardware components:

- Junos OS Release 13.2X50-D10 or later or later for EX Series switches
- Four EX Series switches in an RSTP topology

Before you configure the interface for root protection, be sure you have:

- RSTP operating on the switches.

NOTE: By default, RSTP is enabled on all EX Series switches.

Overview and Topology

Peer STP applications running on switch interfaces exchange a special type of frame called a bridge protocol data unit (BPDU). Switches communicate interface information using BPDUs to create a loop-free topology that ultimately determines the root bridge and which interfaces block or forward traffic in the spanning tree.

However, a root port elected through this process has the possibility of being wrongly elected. A user bridge application running on a PC can generate BPDUs, too, and interfere with root port election.

To prevent this from happening, enable root protection on interfaces that must not receive superior BPDUs from the root bridge and must not be elected as the root port. These interfaces are typically located on an administrative boundary and are designated ports.

When root protection is enabled on an interface:

- The interface is blocked from becoming the root port.
- Root protection is enabled for all STP instances on that interface.
- The interface is blocked only for instances for which it receives superior BPDUs. Otherwise, it participates in the spanning-tree topology.

CAUTION: An interface can be configured for either root protection or loop protection, but not for both.

Four EX Series switches are displayed in Figure 18 on page 272. In this example, they are configured for RSTP and create a loop-free topology. Interface **ge-0/0/7** on Switch 1 is a designated port on an administrative boundary. It connects to Switch 4. Switch 3 is the root bridge. Interface **ge-0/0/6** on Switch 1 is the root port.

This example shows how to configure root protection on interface **ge-0/0/7** to prevent it from transitioning to become the root port.

Figure 18: Network Topology for Root Protection

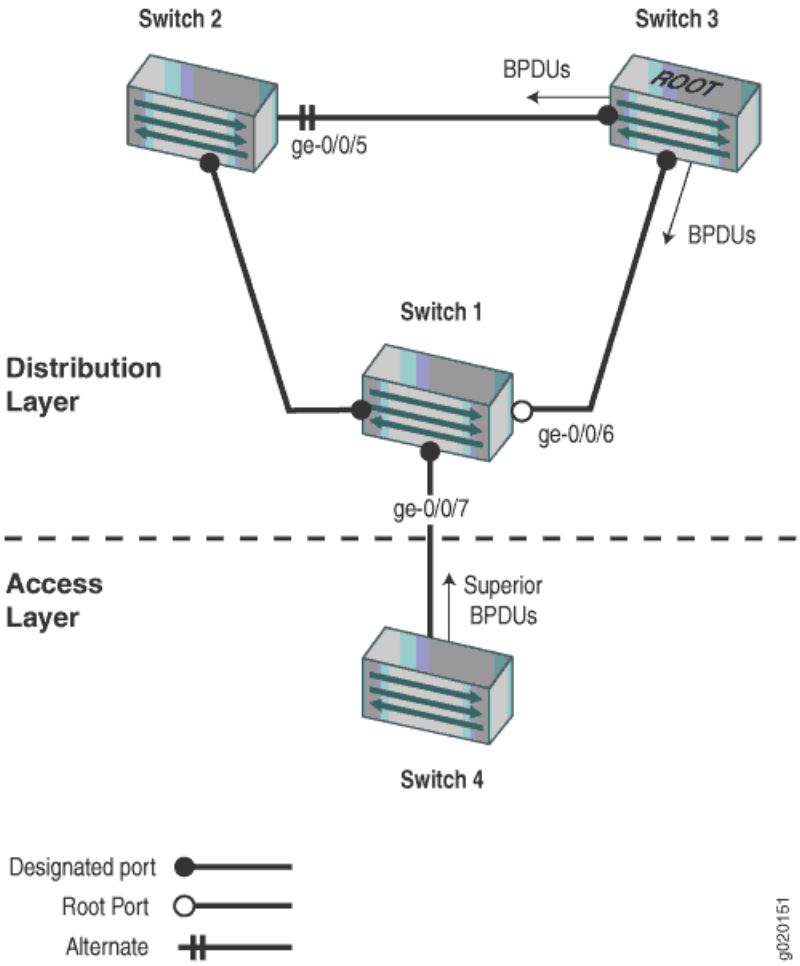


Table 20 on page 272 shows the components that will be configured for root protection.

Table 20: Components of the Topology for Configuring Root Protection on EX Series Switches

Property	Settings
Switch 1	Switch 1 is connected to Switch 4 through interface **ge-0/0/7**.
Switch 2	Switch 2 is connected to Switch 1 and Switch 3. Interface **ge-0/0/4** is the alternate port in the RSTP topology.
Switch 3	Switch 3 is the root bridge and is connected to Switch 1 and Switch 2.
Switch 4	Switch 4 is connected to Switch 1. After root protection is configured on interface **ge-0/0/7**, Switch 4 will send superior BPDUs that will trigger root protection on interface **ge-0/0/7**.

A spanning tree topology contains ports that have specific roles:

- The *root port* is responsible for forwarding data to the root bridge.
- The *alternate port* is a standby port for the root port. When a root port goes down, the alternate port becomes the active root port.
- The *designated port* forwards data to the downstream network segment or device.

This configuration example uses an RSTP topology. However, you also can configure root protection for STP or MSTP topologies at the [**edit protocols mstp**] hierarchy level.

Configuration

To configure root protection on an interface:

CLI Quick Configuration

To quickly configure root protection on interface **ge-0/0/7**, copy the following command and paste it into the switch terminal window:

```
[edit]
set protocols rstp interface ge-0/0/7 no-root-port
```

Step-by-Step Procedure

To configure root protection:

1. Configure interface **ge-0/0/7**:

   ```
   [edit protocols rstp]
   user@switch#
   set interface ge-0/0/7 no-root-port
   ```

Results

Check the results of the configuration:

```
user@switch> show configuration protocols rstp
interface ge-0/0/7 {
    no-root-port;
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly:

Displaying the Interface State Before Root Protection Is Triggered

Purpose

Before root protection is triggered on interface **ge-0/0/7**, confirm the interface state.

Action

Use the operational mode command:

```
user@switch>  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     128:513      128:513  32768.0019e2503f00
20000   BLK    DIS
                    ge-0/0/1     128:514      128:514  32768.0019e2503f00
20000   BLK    DIS
                    ge-0/0/2     128:515      128:515  32768.0019e2503f00
20000   BLK    DIS
                    ge-0/0/3     128:516      128:516  32768.0019e2503f00
20000   FWD    DESG
                    ge-0/0/4     128:517      128:517  32768.0019e2503f00
20000   FWD    DESG
                    ge-0/0/5     128:518        128:2  16384.00aabbcc0348
20000   BLK    ALT
                    ge-0/0/6     128:519        128:1  16384.00aabbcc0348
20000   FWD    ROOT
                    ge-0/0/7     128:520      128:520  32768.0019e2503f00
20000   FWD    DESG
```

```
                    [output truncated]
```

Meaning

The output from the operational mode command **show spanning-tree interface** shows that **ge-0/0/7** is a designated port in a forwarding state.

Verifying That Root Protection Is Working on the Interface

Purpose

A configuration change takes place on Switch 4. A smaller bridge priority on the Switch 4 causes it to send superior BPDUs to interface **ge-0/0/7**. Receipt of superior BPDUs on interface **ge-0/0/7** will trigger root protection. Verify that root protection is operating on interface **ge-0/0/7**.

Action

Use the operational mode command:

```
user@switch> 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     128:513      128:513  32768.0019e2503f00
20000  BLK    DIS
                    ge-0/0/1     128:514      128:514  32768.0019e2503f00
20000  BLK    DIS
                    ge-0/0/2     128:515      128:515  32768.0019e2503f00
20000  BLK    DIS
                    ge-0/0/3     128:516      128:516  32768.0019e2503f00
20000  FWD    DESG
                    ge-0/0/4     128:517      128:517  32768.0019e2503f00
20000  FWD    DESG
                    ge-0/0/5     128:518        128:2  16384.00aabbcc0348
20000  BLK    ALT
                    ge-0/0/6     128:519        128:1  16384.00aabbcc0348
20000  FWD    ROOT
                    ge-0/0/7     128:520      128:520  32768.0019e2503f00
20000  BLK    DIS (Root—Incon)
                    [output truncated]
```

Meaning

The operational mode command **show spanning-tree interface** shows that interface **ge-0/0/7** has transitioned to a root inconsistent state. The root inconsistent state makes the interface block, discarding any received BPDUs, and prevents the interface from becoming a candidate for the root port. When the root bridge no longer receives superior STP BPDUs from the interface, the interface will recover and transition back to a forwarding state. Recovery is automatic.

7

CHAPTER

Monitoring and Troubleshooting

Monitoring and Troubleshooting Spanning Tree Protocols

IN THIS SECTION

Monitoring Spanning Tree Protocols on Switches

Purpose

> **NOTE:** This topic applies only to the J-Web Application package.

Use the monitoring feature to view status and information about the spanning-tree protocol parameters on your EX Series switch.

Action

To display spanning-tree protocol parameter details in the J-Web interface, select **Monitor** > **Switching** > **STP**.

To display spanning-tree protocol parameter details in the CLI, enter the following commands:

- **show spanning-tree interface**

- **show spanning-tree bridge**

Meaning

Table 21 on page 279 summarizes the spanning-tree protocol parameters.

Table 21: Summary of Spanning Tree Protocols Output Fields

Field	Values
Bridge Parameters	
Routing instance name **NOTE:** The option is supported only on EX4300 switches.	Displays bridge information for the specified routing instance.
Context ID	An internally generated identifier.
Enabled Protocol	Spanning-tree protocol type enabled.
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.
Bridge ID	Locally configured bridge ID.
Hello time	The time for which the bridge interface remains in the listening or learning state.
Forward delay	The time for which the bridge interface remains in the listening or learning state before transitioning to the forwarding state.
Extended System ID	The system ID.
Inter Instance ID	An internally generated instance identifier.
Maximum age	Maximum age of received bridge protocol data units (BPDUs).
Number of topology changes	Total number of spanning-tree protocol topology changes detected since the switch last booted.

Table 21: Summary of Spanning Tree Protocols Output Fields *(continued)*

Field	Values
Time since last topology change **NOTE:** This option is supported only on EX4300 switches.	Number of seconds elapsed since the last topology change.
Spanning Tree Interface Details	
Interface Name	Interface configured to participate in the spanning-tree protocol instance.
Port ID	Logical interface identifier configured to participate in the spanning-tree protocol instance.
Designated Port ID	Port ID of the designated port for the LAN segment to which the interface is attached.
Designated Bridge ID	ID of the designated bridge to which the interface is attached.
Port Cost	Configured cost for the interface.
Port State	Spanning-tree protocol port state: • Forwarding (FWD) • Blocking (BLK) • Listening • Learning • Disabled
Role	MSTP or RSTP port role, Designated (DESG), backup (BKUP), alternate (ALT), or root.
Spanning Tree Statistics of Interface	
Interface	Interface for which statistics is being displayed.
BPDUs Sent	Total number of BPDUs sent.
BPDUs Received	Total number of BPDUs received.
Next BPDU Transmission	Number of seconds until the next BPDU is scheduled to be sent.

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.

   TIP: If an interface is blocked, see Troubleshooting section.

Understanding 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 for Routing Devices.

Configuring 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>;
            }
        }
    }
...
```

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;
        }
    }
}
```

Unblocking a Switch Interface That Receives BPDUs in Error (CLI Procedure)

EX Series and QFX Series switches use bridge protocol data unit (BPDU) protection on interfaces to prevent them from receiving BPDUs that could trigger a spanning-tree misconfiguration. If BPDUs are received on a BPDU-protected interface, the interface either shuts down or transitions to a blocking state and stops forwarding frames. In the latter scenario, after the misconfiguration that triggered the BPDUs being sent to an interface is fixed in the topology, the interface can be unblocked and returned to service.

> **NOTE:** This topic applies to Junos OS for EX Series and QFX switches with support for the Enhanced Layer 2 Software (ELS) configuration style. For switches that do not support ELS, see "Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error (CLI Procedure)" on page 285. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

To unblock an interface and return it to service using the CLI:

- Automatically unblock an interface by configuring a timer that expires:

  ```
  [edit protocol layer 2]
  user@switch# set protocols layer2-control bpdu-block disable-timeout 30
  ```

  All interfaces on the switch will be reenabled (unblocked) after the timer expires. However, once an interface on the switch receives a new spanning-tree protocol BPDU, the interface returns to the blocked state.

- Manually unblock an interface using the operational mode command:

  ```
  user@switch> clear error bpdu interface ge-0/0/6
  ```

  This command will only reenable an interface but the BPDU configuration for the interface will continue to exist unless you remove the BPDU configuration explicitly.

Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error (CLI Procedure)

EX Series switches use bridge protocol data unit (BPDU) protection on interfaces to prevent them from receiving BPDUs that could trigger a spanning-tree misconfiguration. If BPDUs are received on a BPDU-protected interface, the interface either shuts down or transitions to a blocking state and stops forwarding frames. In the latter scenario, after the misconfiguration that triggered the BPDUs being sent to an interface is fixed in the topology, the interface can be unblocked and returned to service.

To unblock an interface and return it to service using the CLI:

- Automatically unblock an interface by configuring a timer that expires:

  ```
  [edit ethernet-switching-options]
  user@switch# set bpdu-block disable-timeout 30
  ```

  All interfaces on the switch will be re-enabled (unblocked) after the timer expires. However, once an interface on the switch receives a new spanning-tree protocol BPDU, the interface returns to the blocked state.

- Manually unblock an interface using the operational mode command:

  ```
  user@switch> clear ethernet-switching bpdu-error interface ge-0/0/6.0
  ```

  This command will only re-enable an interface but the BPDU configuration for the interface will continue to exist unless you remove the BPDU configuration explicitly.

Clearing the Blocked Status of a Spanning-Tree Instance Interface

To clear the blocked status of a spanning-tree instance interface on routers or on switches running Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style:

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

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

- To clear the blocked status of a spanning-tree instance interface on switches running Junos OS that does not support ELS, use the **clear ethernet-switching bpdu-error interface** command. See "Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error (CLI Procedure)" on page 285 for details.

  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**).

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

To check whether an interface or 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.

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-name
  ```

Clearing a MAC Rewrite Error on an Interface with Layer 2 Protocol Tunneling

On devices with Layer 2 protocol tunneling (L2PT) configured, customer-facing ports should not receive packets with the L2PT MAC address as the destination address unless you have a network topology or configuration error. Under these conditions, when an interface with L2PT enabled receives an L2PT packet, the interface state becomes disabled due to a MAC rewrite error, and you must subsequently re-enable it to continue operation.

1. To check whether an interface with L2PT enabled has become disabled due to a MAC rewrite error condition, use the **show interfaces** operational command:

   ```
   user@switch> show interfaces interface-name
   ```

   If the interface status includes **Disabled, Physical link is Down** or **Enabled, Physical link is Down** and the **MAC-REWRITE Error** field is **Detected**, then the device detected a MAC rewrite error that contributed to the interface being down. When the device did not detect any MAC rewrite errors, the **MAC-REWRITE Error** field is **None**.

   For example, the following output shows the device detected a MAC rewrite error on the given interface:

   `user@switch>` **show interfaces ge-0/0/2**

   ```
   Physical interface: ge-0/0/2, Disabled, Physical link is Down
     Interface index: 150, SNMP ifIndex: 531
     Link-level type: Ethernet, MTU: 1514, LAN-PHY mode, Speed: 1000mbps, BPDU
   Error: None,
    Loop Detect PDU Error: None, Ethernet-Switching Error: None, Source filtering:
    Disabled
     Ethernet-Switching Error: None, MAC-REWRITE Error: Detected, Loopback: Disabled,

     Flow control: Enabled, Auto-negotiation: Enabled, Remote fault: Online, Media
    type: Fiber
     Device flags   : Present Running
   ```

2. On routers, QFX Series switches, and EX Series switches that use the Enhanced Layer 2 Software configuration style, you can clear a MAC rewrite error from the Junos CLI.

   To clear a MAC rewrite error from an interface that has L2PT enabled, use the **clear error mac-rewrite** operational command:

   ```
   user@switch> clear error mac-rewrite interface-name
   ```

Understanding 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.

8

CHAPTER

Configuration Statements

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

arp-on-stp

Syntax

```
arp-on-stp;
```

Hierarchy Level

```
[edit protocols mstp interface (all | interface-name)],
[edit protocols rstp interface (all | interface-name)],
[edit protocols stp interface (all | interface-name)],
[edit protocols vstp (all |vlan--id | vlan--name) interface (all | interface-name)]
```

Release Information

Statement introduced in Junos OS Release 11.2 for EX Series switches.

Description

Configure the Address Resolution Protocol (ARP) in a spanning-tree network so that when a spanning-tree protocol topology change notification (TCN) is issued, the VLAN with a broken link can relearn MAC addresses from another, redundant VLAN in the network. The network must include a routed VLAN interface (RVI).

When a link fails in a spanning-tree network (RSTP, STP, MSTP, or VSTP), a message called a TCN is issued that causes all affected Ethernet switching table entries to be flushed. The network must then relearn the MAC addresses using flooding. If you have configured an RVI on the network, you have the option of having the VLAN with the broken link relearn MAC addresses from another VLAN using ARP, thereby avoiding excessive flooding on the VLAN with the broken link.

Default

ARP on STP is disabled.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring STP on EX Series Switches (CLI Procedure) | 42

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 Multihoming | 254

Configuring VPLS Root Protection Topology Change Actions to Control Individual VLAN Spanning-Tree Behavior | 262

block (Spanning Trees)

Syntax

```
block;
```

Hierarchy Level

```
[edit protocols mstp interface (all | interface-name) bpdu-timeout-action],
[edit protocols rstp interface (all | interface-name) bpdu-timeout-action],
[edit protocols stp interface (all | interface-name) bpdu-timeout-action],
[edit protocolsvstp vlan vlan-id interface (all | interface-name) bpdu-timeout-action]
```

Release Information

Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configures loop protection on a specific interface.

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 STP, RSTP, VSTP, and MSTP*
- *Understanding VSTP*
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- *Example: Configuring Faster Convergence and Improving Network Stability with RSTP*
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | **72**
- *Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree*
- Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on non-ELS EX Series Switches | **231**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

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 | 172

Understanding Provider Bridge Participation in RSTP or MSTP Instances

Configuring Rapid Spanning Tree Protocol | 45

Configuring Multiple Spanning Tree Protocol | 105

bpdu-block

Syntax

```
bpdu-block {
    interface (interface-name disable | all);
    disable-timeout seconds;
}
```

Hierarchy Level

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

```
[edit ethernet-switching-options]
```

Release Information

Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configures bridge protocol data unit (BPDU) protection on a specified interface or on all interfaces. If the interface receives incompatible BPDUs, it is disabled.

If the **disable-timeout** statement is included in the BPDU configuration, the interface is automatically reenabled after the timer expires. Otherwise, you must use the operational mode command **clear ethernet-switching bpdu-error interface** to unblock and reenable the interface.

The remaining statements are explained separately. See CLI Explorer.

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 | **168**
- Configuring BPDU Protection for Individual Spanning-Tree Instance Interfaces | **171**
- Understanding BPDU Protection for STP, RSTP, and MSTP | **169**
- Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches | **221**

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 9.1 for EX Series switches.
Statement introduced in Junos OS Release 9.4 for additional devices.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support. Statement updated in Junos OS Release 11.1 for EX Series switches to change blocking behavior to port shutdown.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 17.1 for ACX Series routers.

Description

Configure bridge protocol data unit (BPDU) protection on all edge ports of a switch. When the **bpdu-block-on-edge** statement is configured and the interface encounters an incompatible BPDU, the interface shuts down.

If the **disable-timeout** statement is included in the BPDU configuration, the interface is automatically reenabled after the timer expires. Otherwise, you must use the operational mode command **clear ethernet-switching bpdu-error interface** to unblock and reenable the interface.

Default

Not enabled.

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 | 168

Understanding BPDU Protection for STP, RSTP, and MSTP | 169

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 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*]

[edit protocols **mstp**],
[edit protocols **mstp msti** *msti-id*],
[edit protocols **rstp**],
[edit protocols **stp**],
[edit protocols **vstp vlan** *vlan-id*]

Release Information

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configures the bridge priority, which determines 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.

Default

32,768

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

- Understanding MSTP | **97**
- Understanding VSTP | **143**
- Understanding Bridge Priority for Election of Root Bridge and Designated Bridge | **258**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

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

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 MSTP | 97
- Understanding BPDUs Used for Exchanging Information Among Bridges | 172
- Configuring Multiple Spanning Tree Protocol | 105
- Configuring MSTP on Switches | 101
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | 72
- show spanning-tree bridge | 403
- show spanning-tree interface | 410

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.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Support for logical systems added in Junos OS Release 9.6.

Description

For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), configure the link cost to control which bridge is the designated bridge and which interface is the designated interface.

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

- Understanding Spanning-Tree Instance Interfaces | **35**
- Understanding STP | **40**
- Understanding RSTP | **44**
- Understanding MSTP | **97**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

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 mpls],
[edit protocols mpls interface (all | interface-name)],
```

```
[edit protocols mstp],
[edit protocols mstp (all | interface-name)],
[edit protocols mstp (all | interface-name) arp-on-stp],
[edit protocols mstp msti msti-id  vlan (vlan-id | vlan-name) interface (all | interface-name)],
[edit protocols mstp msti msti-id  vlan (vlan-id | vlan-name) interface interface-name arp-on-stp],
[edit protocols rstp],
[edit protocols rstp interface (all | interface-name)],
[edit protocols rstp interface (all | interface-name) arp-on-stp],
[edit protocols stp],
[edit protocols stp interface (all | interface-name)],
[edit protocols stp interface (all | interface-name) arp-on-stp],
[edit protocols vstp],
[edit protocols vstp vlan vlan-id interface (all | interface-name)]
[edit protocols vstp vlan vlan-id interface (all | interface-name) arp-on-stp]
[edit protocols mstp interface interface-name,
[edit protocols mstp msti msti-id  vlan (all vlan-id | vlan-name) interface interface-name],
[edit protocols rstp interface interface-name],
[edit protocols vstp vlan vlan-id interface interface-name]
```

```
[edit routing-instances routing-instance-name protocols mstp]
```

```
[edit ethernet-switching-options bpdu-block interface]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.1.

Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Statement introduced in Junos OS Release 12.2 for EX Series switches.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.
Statement updated in Junos OS Release 15.1 for EX Series switches.

Description

Disable the entire MSTP, RSTP, or VSTP instance on a specific interface.

> **NOTE:** You cannot disable spanning tree parameters for all interfaces.

Default

Not enabled

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding RSTP | **44**
- Configuring Multiple Spanning Tree Protocol | **105**
- Configuring RSTP on EX Series Switches (CLI Procedure) | **48**
- Configuring MSTP on Switches | **101**
- Disabling MSTP | **142**
- Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches | **221**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- Example: Configuring Faster Convergence and Network Stability on ELS Switches with RSTP | **49**
- interface | **322**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

disable-timeout

Syntax

```
disable-timeout seconds;
```

Hierarchy Level

```
[edit protocols layer2-control bpdu-block]
```

```
[edit ethernet-switching-options bpdu-block]
```

Release Information

Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement introduced in Junos OS Release 9.4.

Description

For interfaces configured for BPDU protection, specify the amount of time an interface receiving BPDUs is disabled.

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.

Default

The disable timeout is not enabled.

Options

seconds——Amount of time, in seconds, the interface receiving BPDUs is disabled. Once the timeout expires, the interface is brought back into service.

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

RELATED DOCUMENTATION

drop (BPDU Block)

Syntax

```
drop;
```

Hierarchy Level

[edit ethernet-switching-options **bpdu-block bpdu-block** (all | [*interface-name*])]

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Drop bridge protocol data units (BPDUs) that enter any interface or a specified interface, but do not disable the interface. Configure the **drop** statement *only* on interfaces on which no spanning-tree protocol (STP, MSTP, or RSTP) is configured.

> **NOTE:** Do not configure **drop** on any interface on which a spanning-tree protocol has been configured. Doing so could cause STP misconfiguration and consequent network outages.

Default

Not enabled.

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 STP, RSTP, and MSTP | **169**
- Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches | **210**
- Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches | **221**
- bpdu-block-on-edge | **300**

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 (all | interface-name)], )arp-on-stp],
[edit protocols mstp msti msti-id interface (all | interface-name)], )arp-on-stp],
[edit protocols vstp vlan vlan-id interface (all | interface-name)], )arp-on-stp],
```

```
[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 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

For Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), configure interfaces as edge ports or edge interfaces. Edge ports do not expect to receive BPDUs. If a BPDU is received, the port becomes a nonedge port and the Edge interfaces immediately transition to a forwarding state.

> **NOTE:** Although the **edge** configuration statement appears in the [**edit protocols stp interface (all | *interface-name*)**] or [**edit protocols rstp force-version stp interface (all | *interface-name*)**] hierarchy on the switch, this statement has no effect on the switch operation if you configure it.

Default

Edge interfaces are not enabled.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding STP | **40**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

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, CDP, and other supported protocols on all logical interfaces (VLANs) configured on the interface.

NOTE: Tunneling on all logical interfaces is enabled automatically for PVST/PVST+.

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

RELATED DOCUMENTATION

Understanding Layer 2 Protocol Tunneling

protocol | **350**

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 | 45
- Configuring RSTP on EX Series Switches (CLI Procedure) | 48
- Example: Configuring Faster Convergence and Network Stability on ELS Switches with RSTP | 49
- Understanding RSTP | 44

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 9.4 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.
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

Forces the spanning-tree version to be the original IEEE 803.1D STP protocol.

Required Privilege Level

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

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 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specifies 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

- Understanding Forward Delay Before Ports Transition to Forwarding State | 289
- Understanding STP | 40
- Understanding MSTP | 97
- Understanding VSTP | 143
- Example: Configuring Network Regions for VLANs with MSTP on Switches | 111
- Example: Configuring Faster Convergence and Network Stability on ELS Switches with RSTP | 49
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | 72
- show spanning-tree bridge | 403
- show spanning-tree interface | 410

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 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Support for logical systems added in Junos OS Release 9.6.
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

For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specifies the number of seconds between transmissions of configuration BPDUs by the root bridge.

Default

2 seconds

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

- Understanding MSTP | **97**
- Understanding VSTP | **143**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- Example: Configuring Faster Convergence and Network Stability on ELS Switches with RSTP | **49**
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | **72**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

interface (BPDU Blocking)

Syntax

```
interface (all | [interface-name]);
```

Hierarchy Level

```
[edit protocols layer2-control bpdu-block]
```

```
[edit ethernet-switching-options bpdu-block]
```

Release Information

Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Applies Bridge Protocol Data Unit (BPDU) protection on all interfaces or on one or more specified interfaces.

Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP) provide Layer 2 loop prevention for EX Series switches. The spanning-tree protocols use BPDU frames to communicate. Through their exchange, spanning-tree topologies determine which interfaces block traffic and which interfaces become root ports and forward traffic. User bridge applications running on a PC can also generate BPDUs. If these BPDUs are picked up by STP applications running on the switch, they can trigger STP miscalculations that can lead to network outages.

To block outside BPDUs from reaching a switch interface connected to devices that are not part of a spanning-tree topology, configure BPDU protection on interfaces in the topology.

CAUTION: When configuring BPDU protection on an interface without spanning trees connected to a switch with spanning trees, be careful that you do not configure BPDU protection on all interfaces. Doing so could prevent BPDUs being received on switch interfaces (such as a trunk interface) that you intended to have receive BPDUs from a switch with spanning trees.

NOTE: Interfaces that are configured as edge interfaces can transition to a forwarding state immediately because they cannot create network loops. As edge ports are connected to end devices, it is imperative that you configure BPDU protection on edge ports to protect the switch from outside BPDUs. When BPDU protection is enabled on an edge interface, the interface shuts down on encountering an outside BPDU thereby preventing any traffic from passing through the interface.

Options

all—All interfaces.

[***interface-name***]—One or more Ethernet interface names.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding BPDU Protection for STP, RSTP, and MSTP | **169**
- Understanding BPDU Protection for Spanning-Tree Instance Interfaces | **168**
- Configuring BPDU Protection for Individual Spanning-Tree Instance Interfaces | **171**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | **72**
- Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches | **221**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

interface (Spanning Tree)

Syntax

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

Syntax

```
interface interface-name {
    arp-on-stp;
    bpdu-timeout-action
        block;
        log;
    cost cost;
    disable;
    edge;
    mode mode;
    no-root-port;
    priority 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 protocols (**mstp** | **rstp** | **vstp**)],
[edit protocols vstp vlan *vlan-id*],
[edit protocols vstp **vlan-group** group *group-name* vlan (vlan-id | vlan-range |open-set-of-values)

[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 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement updated in Junos OS Release 15.1 for EX Series switches to support configuration of spanning tree parameters globally on all interfaces.

NOTE: You cannot disable spanning tree parameters globally on all interfaces.

Description

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

The **edge**, **mode**, and **no-root-port** options are not available at the [**edit protocols mstp msti *msti-id***] hierarchy level.

Options

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

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding Spanning-Tree Instance Interfaces | 35
- Understanding RSTP | 44
- Understanding MSTP | 97
- Understanding VSTP | 143
- Configuring RSTP on EX Series Switches (CLI Procedure) | 48
- Configuring MSTP on Switches | 101
- Example: Configuring Network Regions for VLANs with MSTP on Switches | 111
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | 72
- show spanning-tree bridge | 403
- show spanning-tree interface | 410

layer2-control

Syntax

```
layer2-control {
    bpdu-block {
        disable-timeout seconds;
        interface interface-name;
    }
    mac-rewrite {
        interface interface-name {
            enable-all-ifl;
            protocol protocol-name;
        }
    }
    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.
Statement introduced in Junos OS Release 14.1X53-D10 for EX4300 switches.
Statement introduced in Junos OS Release 15.1X53-D50 for EX2300 and EX3400 switches.
Statement introduced in Junos OS Release 17.4R1 for EX4600 switches.
Statement introduced in Junos OS Release 19.1R1 for QFX Series switches.

Description

Configure Layer 2 control protocols to enable features such as Layer 2 protocol tunneling or nonstop bridging.

The remaining statements are explained separately. See CLI Explorer.

NOTE: For a detailed description of configuring the **nonstop-bridging** statement, see the *High Availability User Guide*. When you configure this statement 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

- *Understanding Layer 2 Protocol Tunneling*
- *Configuring Layer 2 Protocol Tunneling*
- *instance-type*

log (Spanning Trees)

Syntax

```
log;
```

Hierarchy Level

```
[edit protocols mstp interface (all | interface-name) bpdu-timeout-action],
[edit protocols rstp interface (all | interface-name) bpdu-timeout-action],
[edit protocols stp interface (all | interface-name) bpdu-timeout-action],
[edit protocols vstp vlan vlan-id interface (all | interface-name) bpdu-timeout-action]
```

Release Information

Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

Description

For interfaces configured for loop protection, configure the software to generate a message to be sent to the system log file **/var/log/messages** to record the loop-protection event.

Required Privilege Level

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

RELATED DOCUMENTATION

- show spanning-tree bridge | 403
- show spanning-tree interface | 410
- Example: Configuring Network Regions for VLANs with MSTP on Switches | 111
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | 72
- Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on non-ELS EX Series Switches | 231

mac-rewrite

Syntax

```
mac-rewrite {
   interface interface-name {
      enable-all-ifl;
      protocol protocol-name;
      }
   }
}
```

Hierarchy Level

[edit protocols layer2-control]

Release Information

Statement introduced in Junos OS Release 9.1.
enable-all-if statement added in Junos OS Release 13.3.
Support for PVSTP protocol introduced in Junos OS Release 13.3 for MX Series routers and EX9200 switches.
Statement introduced in Junos OS Release 14.1X53-D10 and 17.3R1 for EX4300 switches.
Statement introduced in Junos OS Release 15.1X53-D55 and 18.2R1 for EX2300 and EX3400 switches.
Statement introduced in Junos OS Release 17.4R1 for EX4600 switches.
Statement introduced in Junos OS Release 19.1R1 for QFX Series switches.

Description

Enable rewriting of the MAC address for Layer 2 protocol tunneling (L2PT).

When a service provider edge port configured for L2PT receives a control packet for a supported protocol, the device rewrites the multicast destination MAC address with the predefined multicast tunneling MAC address 01:00:0c:cd:cd:d0. The packet travels across the provider network transparently to the other end of the tunnel, and the destination device restores the original multicast destination MAC address to deliver the packet at its destination.

Refer to **protocol** for the list of protocols that you can configure for L2PT on different devices.

To see the protocols for which you enabled L2PT on an interface, enter the **show mac-rewrite interface** command.

On MX Series and ACX Series routers and EX9200 switches with L2PT configured, customer-facing ports should not receive packets with the L2PT MAC address as the destination address unless there is a network

tolopogy or configuration error. Any such interface receiving an L2PT packet becomes “Disabled”, and you must subsequently re-enable it using the **clear error mac-rewrite** command.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

- *Understanding Layer 2 Protocol Tunneling*
- *Configuring Layer 2 Protocol Tunneling*
- show mac-rewrite interface | **401**
- clear error mac-rewrite | **386**

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**],
[edit protocols **rstp**],
[edit protocols **stp**],
[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 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specifies the maximum expected arrival time of hello BPDUs.

Default

20 seconds

Options

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

seconds—The maximum age of received protocol 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

- Understanding STP | **40**
- Understanding MSTP | **97**
- Understanding VSTP | **143**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- Example: Configuring Faster Convergence and Network Stability on ELS Switches with RSTP | **49**
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | **72**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

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

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 hops20 hops

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding MSTP | **97**
- Configuring Multiple Spanning Tree Protocol | **105**
- Configuring MSTP on Switches | **101**

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 protocols mstp interface (all | interface-name) arp-on-stp],
[edit protocols mstpmsti msti-id interface interface-name) arp-on-stp],
[edit protocols rstp interface (all | interface-name) arp-on-stp],
```

```
[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]
[edit protocols stp interface (all | (all | interface-name)],
[edit protocols stp interface (all | interface-name) arp-on-stp],
[edit protocols vstp vlan vlan-id interface (all | interface-name) arp-on-stp]
```

Release Information

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), configures the 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:** For EX4300 switches, the interfaces operate in full-duplex mode only.

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

- Understanding Spanning-Tree Instance Interfaces | **35**
- Understanding STP | **40**
- Understanding VSTP | **143**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- Example: Configuring Faster Convergence and Network Stability on ELS Switches with RSTP | **49**
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | **72**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

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;
    }
}
```

Syntax

```
msti msti-id {
    vlan (vlan-id | vlan-name);
    interface interface-name {
        disable-timeout;
        cost cost;
        priority 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 9.0 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement updated in Junos OS Release 15.1 for EX Series switches to support configuration of spanning tree parameters globally on all interfaces.

NOTE: You cannot disable spanning tree parameters globally on all interfaces.

Description

Configures the Multiple Spanning Tree Instance (MSTI) identifier for Multiple Spanning Tree Protocol (MSTP). MSTI IDs are local to each region, so you can reuse the same MSTI ID in different regions.

Default

MSTI is disabled.

Options

msti-id—MSTI instance identifier.

Range: 1 through 64

Range: 1 through 4094. The Common Instance Spanning Tree (CIST) is always MSTI 0.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding MSTP | **97**
- Configuring Multiple Spanning Tree Protocol | **105**
- Configuring MSTP on Switches | **101**
- Configuring MSTP Instances on a Physical Interface | **109**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- Understanding MSTP | **97**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

mstp

List of Syntax

MX Series, QFX Series, EX Series (Enhanced Layer 2 Software (ELS) Configuration Style)

```
mstp {
    backup-bridge-priority priority;
    bpdu-block-on-edge;
    bpdu-destination-mac-address provider-bridge-group;
    bridge-priority priority;
    configuration-name configuration-name;
    disable;
    forward-delay seconds;
    hello-time seconds;
    interface ( all | interface-name ) {
        bpdu-timeout-action {
            alarm;
            block;
        }
        cost cost;
        edge;
        mode (p2p | shared);
        no-root-port;
        priority interface-priority;
    }
    max-age seconds;
    max-hops hops;
    msti msti-id {
        backup-bridge-priority priority;
        bridge-priority priority;
        interface interface-name {
            cost cost;
            priority interface-priority;
        }
        vlan vlan-id;
    }
    priority-hold-time seconds;
    revision-level revision-level;
    system-id system-id-value {
        ip-address(es);
    }
```

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

EX Series (Without Enhanced Layer 2 Software (ELS) Configuration Style)

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

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.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
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

Configures Multiple Spanning Tree Protocol (MSTP). MSTP is defined in the IEEE 802.1Q-2003 specification and is used to create a loop-free topology in networks with multiple spanning tree regions.

> **NOTE:** MX Series routers and QFX5100 switches do not support the **interface all** statement to enable MSTP on all interfaces with one command.
>
> On MX Series routers, you must enable MSTP on interfaces individually using the **set ... protocols mstp interface *interface-name*** statement.
>
> On QFX5100 switches, to apply MSTP configuration to more than one interface, you must first configure one or more interface ranges for the interfaces on which you want to configure MSTP, and then issue the **set protocols mstp interface *interface-name*** command using each interface range as the *interface-name* parameter.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

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 protocols mstp interface (all | interface-name) arp-on-stp],
[edit protocols rstp interface (all | interface-name) arp-on-stp],
[edit protocols stp interface (all | interface-name) arp-on-stp],
```

```
[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]
[edit protocols vstp vlan vlan-id interface (all | interface-name) arp-on-stp]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 17.1 for ACX Series routers.

Description

Configures an interface to be a spanning-tree designated port. If the bridge receives superior STP bridge protocol data units (BPDUs) on a root-protected interface, that interface transitions to a root-prevented STP state (inconsistency state) and the interface is blocked. This blocking prevents a bridge from being elected the root bridge. When the bridge stops receiving superior STP BPDUs on the root-protected interface, interface traffic is no longer blocked.

Required Privilege Level

routing—To view this statement in the configuration.

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

RELATED DOCUMENTATION

- Understanding VSTP | **143**
- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network | **259**
- Enabling Root Protection for a Spanning-Tree Instance Interface | **261**
- Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches | **264**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | **72**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

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 protocols mstp ;interface (all | interface-name) arp-on-stp],
[edit protocols mstpmsti msti-id interface interface-name arp-on-stp],
[edit protocols rstp interface (all | interface-name) arp-on-stp],
[edit protocols stp interface (all | interface-name) arp-on-stp],
[edit protocols vstp vlan vlan-id interface (all | interface-name) arp-on-stp]
```

```
[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 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specifies the interface priority to control which interface is elected as the root port. The interface priority must be set in increments of 16.

Default

The default value is 128.

Options

priority—(Optional) Interface priority. The interface priority must be set in increments of 16.

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

- Understanding STP | 40
- show spanning-tree bridge | 403
- show spanning-tree interface | 410

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.

protocol

List of Syntax

Syntax (MX Series Routers)

```
protocol (cdp | pvstp | stp | vtp);
```

Syntax (ACX Series Routers)

```
protocol (cdp | elmi | ieee8021x | ieee8023ah | lacp | lldp | mmrp | mvrp | stp | vtp);
```

Syntax (EX2300, EX3400, EX4300, EX4300 Multigigabit Model, EX4600, EX4650, and QFX Series Switches)

```
protocol (cdp | elmi | gvrp | ieee8021x | ieee8023ah | lacp | lldp | mmrp | mvrp | stp | udld | vstp | vtp);
```

Syntax (EX2300 Multigigabit Model Switches)

```
protocol (cdp | gvrp | ieee8023ah | lacp | lldp | mvrp | stp | vstp | vtp);
```

Syntax (EX9200 Switches)

```
protocol (cdp | elmi | gvrp | ieee8021x | ieee8023ah | lacp | lldp | mmrp | mvrp | pvstp | stp | udld | vtp);
```

Hierarchy Level

[edit logical-systems *name* protocols layer2-control **mac-rewrite** interface *interface-name*],
[edit protocols **layer2-control mac-rewrite** interface *interface-name*]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Releases 12.3X52-D10 and 13.2R1 for ACX Series Routers.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Support for PVST/PVST+ introduced in Junos OS Release 13.3 for MX Series routers and EX9200 switches.
Statement introduced in Junos OS Release 14.1X53-D10 and 17.3R1 for EX4300 switches
Statement introduced in Junos OS Release 15.1X53-D55 and 18.2R1 for EX2300 and EX3400 switches.
Support for E-LMI, IEEE 802.1X, MMRP, and UDLD introduced in Junos OS Release 17.3R1 for EX4300 switches.
Support for E-LMI, GVRP, IEEE 802.1x, IEEE 802.3AH, LACP, LLDP, MMRP, MVRP, and UDLD introduced in Junos OS Release 17.3R1 for EX9200 switches.
Statement introduced in Junos OS Release 17.4R1 for EX4600 switches.
Support for E-LMI, IEEE 802.1X, MMRP, and UDLD introduced in Junos OS Release 18.2R1 for EX2300 and EX3400 switches.
Statement introduced in Junos OS Release 19.1R1 for QFX Series switches.
Statement introduced in Junos OS Release 19.2R1 for EX4300 multigigabit switches.

Description

Configure the protocol to be tunneled on an interface using Layer 2 protocol tunneling (L2PT). To enable tunneling multiple protocols, include multiple **protocol** statements.

You can tunnel different protocols listed in the Options section on different types of devices. The Syntax and Release Information sections list the available options for the protocols that different devices can tunnel as of a particular Junos OS release (for devices that support L2PT).

When a service provider edge (PE) port configured for L2PT receives a control packet for a supported protocol, the device rewrites the multicast destination MAC address with the predefined multicast tunneling MAC address 01:00:0c:cd:cd:d0. The packet travels across the provider network transparently to the other end of the tunnel, and the destination device restores the original multicast destination MAC address to deliver the packet at its destination.

Options

cdp—Tunnel the Cisco Discovery Protocol (CDP).

elmi—Tunnel Ethernet Local Management Interface (E-LMI) packets.

gvrp—Tunnel Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) packets.

ieee8021x—Tunnel IEEE 802.1X authentication packets.

ieee8023ah—Tunnel IEEE 802.3AH Operation, Administration, and Maintenance (OAM) link fault management (LFM) packets.

lacp—Tunnel Link Aggregation Control Protocol (LACP) packets.

lldp—Tunnel Link Layer Discovery Protocol (LLDP) packets.

mmrp—Tunnel Multiple MAC Registration Protocol (MMRP) packets.

mvrp—Tunnel Multiple VLAN Registration Protocol (MVRP) packets.

pvstp—Tunnel VLAN Spanning Tree Protocol (VSTP), Per-VLAN Spanning Tree (PVST), and Per-VLAN Spanning Tree Plus (PVST+) Protocol packets.

stp—Tunnel packets for all versions of Spanning-Tree Protocols.

udld—Tunnel Unidirectional Link Detection (UDLD) packets.

vstp—Tunnel VLAN Spanning Tree Protocol (VSTP) packets.

vtp—Tunnel VLAN Trunking Protocol (VTP) packets.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Layer 2 Protocol Tunneling

Configuring Layer 2 Protocol Tunneling

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

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

Description

For Multiple Spanning Tree Protocol (MSTP), 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

- Understanding MSTP | **97**
- Configuring Multiple Spanning Tree Protocol | **105**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

rstp

List of Syntax

MX Series

```
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>;
    }
}
```

EX Series

```
rstp {
    bpdu-block-on-edge;
    bridge-priority priority; priority;
    disable;
    forward-delay seconds;
```

```
    hello-time seconds;
    interface (all | interface-name) {
        arp-on-stp;
        bpdu-timeout-action {
            block;
            log;
        }
        cost cost;
        edge;
        mode mode;
        no-root-port;
        priority priority;
    }
    max-age seconds;
    traceoptions {
        file filename <files number > <size size> <no-stamp | no-world-readable | world-readable>;
        flag flag;
    }
}
```

ELS Versions: EX Series, QFX Series, NFX Series

```
rstp {
    bpdu-block-on-edge;
    bpdu-destination-mac-address provider-bridge-group;
    bridge-priority priority;
    disable;
    extended-system-id;
    force-version stp;
    forward-delay seconds;
    hello-time seconds;
    max-age seconds;
    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.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
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.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement updated in Junos OS Release 15.1 for EX Series and QFX Series switches to support configuration of spanning tree parameters globally on all interfaces.

NOTE: You cannot disable spanning tree parameters globally on all interfaces.

Description

Configure Rapid Spanning Tree Protocol (RSTP). RSTP is defined in the IEEE 802.1D-2004 specification and is used to prevent loops in Layer 2 networks, which results in shorter convergence times than those provided by basic Spanning Tree Protocol (STP).

VSTP and RSTP can be configured concurrently. You can selectively configure up to 253 VLANs using VSTP; the remaining VLANs will be configured using RSTP. VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on the switch.

BEST PRACTICE: Configure RSTP when you configure VSTP. RSTP overhead is minimal and this configuration ensures that a spanning-tree protocol is running on all VLANs on your switch, even when your switch is supporting more than 253 VLANs.

The remaining statements are explained separately. See CLI Explorer.

Default

RSTP is enabled on all Ethernet switching interfaces.

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 | **45**
- Understanding RSTP | **44**
- Configuring RSTP on EX Series Switches (CLI Procedure) | **48**
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | **72**
- show spanning-tree bridge | **403**
- show spanning-tree interface | **410**

shutdown (BPDU Block)

Syntax

```
shutdown;
```

Hierarchy Level

```
[edit ethernet-switching-options bpdu-block interface (all | [interface-name])]
```

Release Information

Statement introduced in Junos OS Release 12.2 for EX Series switches.

Description

Shut down all or specified interfaces to prevent spanning-tree protocol BPDUs (for STP, MSTP, RSTP, and VSTP) from entering the interfaces on which BPDU protection is configured.

Default

Not enabled

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 STP, RSTP, and MSTP | 169

Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error (CLI Procedure) | 285

stp

Syntax

```
stp {
    disable;
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
        disable;
        bpdu-timeout-action {
            block;
            alarm;
        }
        cost  cost;
        edge;
        mode mode;
        no-root-port;
        priority priority;
    }
    max-age seconds;
    traceoptions {
        file name <replace> <size size> <files number> <no-stamp>
            <(world-readable | no-world-readable)>;
        flag flag <flag-modifier> <disable>;
    }
}
```

Syntax (EX Series)

```
stp {
    bpdu-block-on-edge ;
    bridge-priority priority;
    disable;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
        arp-on-stp;
        bpdu-timeout-action {
            block;
            log;
        }
```

```
        cost  cost;
        disable;
        mode mode;
        no-root-port;
        priority priority;
    }
    max-age seconds;
    traceoptions {
        file filename <files number > <size size> <no-stamp | world-readable | no-world-readable>;
        flag flag;
    }
}
```

Hierarchy Level

```
[edit protocols],
[edit protocols rstp force-version]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

When you explicitly configure STP, a switch uses the IEEE 802.1D 2004 specification, force version 0. This configuration runs a version of RSTP that is compatible with the classic, basic STP (defined in the IEEE 802.1D 1998 specification).

The remaining statements are explained separately. See CLI Explorer.

> **NOTE:** Although the **edge** configuration statement appears in the CLI on the switch, this statement has no effect on the switch operation if you configure it.

Default

STP is disabled; by default, RSTP is enabled on all Ethernet switching ports.

Required Privilege Level

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

RELATED DOCUMENTATION

Overview of Spanning-Tree Protocols

Understanding STP | **40**

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

Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches | **210**

Configuring STP on EX Series Switches (CLI Procedure) | **42**

Configuring STP

show spanning-tree bridge | **403**

show spanning-tree interface | **410**

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

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 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Sets protocol-level tracing options for for spanning-tree protocols MPLS, MVRP, STP, RSTP, MSTP, and VSTP.

Default

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

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.
- **error**—Trace all failure conditions.
- **events**—Trace events of the protocol state machine.
- **pdu**—Trace PDUs that were received and sent.
- **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.
- **socket**—Trace socket activity.
- **state-machine**—Trace state machine information.
- **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.

replace—(Optional) Replace an existing trace file if there is one.

Default: If you do not include this option, tracing output is appended to an existing trace 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

- Understanding RSTP | 44
- Understanding STP | 40
- Understanding VSTP | 143
- *Understanding Multiple VLAN Registration Protocol (MVRP)*
- Understanding Spanning-Tree Protocol Trace Options | 281
- Configuring Tracing Spanning-Tree Operations | 282
- Understanding MSTP | 97
- Example: Configuring Network Regions for VLANs with MSTP on Switches | 111
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | 72
- Example: Tracing Spanning-Tree Protocol Operations | 284
- show spanning-tree bridge | 403
- show spanning-tree interface | 410

vlan (MSTP)

Syntax

```
vlan vlan-id;
```

EX Series

```
vlan (all | vlan-id | vlan-name) {
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface interface-name {
        bpdu-timeout-action {
            block;
            log;
        }
        cost  cost;
        disable;
        edge;
        mode mode;
        no-root-port;
        priority priority;
    }
    max-age seconds;
    traceoptions {
        file filename <files number > <size size> <no-stamp | world-readable | no-world-readable>;
        flag flag;
    }
}
```

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 protocols mstpmsti msti-id]
[edit protocols vstp]
```

```
[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 9.0 for EX Series switches.
Statement updated with enhanced **?** (CLI completion feature) functionality in Junos OS Release 9.5 for EX Series switches.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure the VLANs for a Multiple Spanning Tree Instance (MSTI) or VSTP instance.

> **NOTE:** When you configure VSTP with the **set prototocol vstp vlan all** command, vlan-id 1 is excluded to be compatible with Cisco PVST+. If you want vlan-id 1 to be included in VSTP, you must set it separately with the **set protocol vstp vlan 1** command.

> **TIP:** To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type **?** after **vlan** or **vlans** in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.

Options

vlan-name—Name of the VLAN.

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

- Understanding MSTP | **97**
- Understanding VSTP | **143**
- Configuring Multiple Spanning Tree Protocol | **105**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**

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;
    }
}
```

EX Series

```
vlan (all | vlan-id | vlan-name) {
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
        bpdu-timeout-action {
            block;
            log;
        }
        cost  cost;
        disable;
        edge;
        mode mode;
        no-root-port;
        priority priority;
    }
    max-age seconds;
    traceoptions {
        file filename <files number > <size size> <no-stamp | world-readable | no-world-readable>;
        flag flag;
    }
}
```

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

Description

Configure VSTP VLAN parameters.

TIP: To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type **?** after **vlan** or **vlans** in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.

Options

all—All VLANs.

vlan-id—Numeric VLAN identifier.

vlan-range—Name of the VLAN range.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding VSTP | **143**

Configuring VLAN Spanning Tree Protocol

vlan-group

Syntax

```
vlan-group group group-name {
vlan (vlan-id |vlan-group |all) {
}
```

Hierarchy Level

```
[edit protocols vstp]
```

Release Information

Statement introduced in Junos OS Release 15.1 for EX Series switches.

Description

Configure VLAN group for Spanning Tree Protocol (VSTP). VSTP is used to prevent loops in Layer 2 networks on a per-VLAN basis.

> **BEST PRACTICE:** Configure RSTP when you configure VSTP. RSTP overhead is minimal and this configuration ensures that a spanning-tree protocol is running on all VLANs on your switch, even when your switch is supporting more than the maximum number of allowed VSTP VLANs.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- vstp | 376
- show spanning-tree bridge | 403
- show spanning-tree interface | 410

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.

vstp

List of Syntax

MX Series

```
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>;
    }
}
```

EX Series, QFX Series, QFabric

```
vstp {
    bpdu-block-on-edge;
    disable;
    force-version stp;
    vlan (all | vlan-id | vlan-name) {
        bridge-priority priority;
        forward-delay seconds;
        hello-time seconds;
        interface (all | interface-name) {
            arp-on-stp;
            bpdu-timeout-action {
                block;
                log;
            }
            cost  cost;
            disable;
            edge;
            mode mode;
            no-root-port;
            priority priority;
        }
        max-age seconds;
        traceoptions {
            file filename <files number > <size size> <no-stamp | no-world-readable | world-readable>;
            flag flag;
        }
    }
}
```

ELS versions: EX Series, QFX Series, NFX Series

```
vstp {
    bpdu-block-on-edge;
    disable;
    force-version stp;
    interface (interface-name disable | interface-range-name | all ){
        bpdu-timeout-action {
            alarm;
            block;
        }
        cost cost;
        edge;
        mode (p2p | shared);
        no-root-port;
        priority interface-priority;
    }
priority-hold-time seconds;
    vlan (vlan-id | all){
        bridge-priority priority;
        forward-delay seconds;
        hello-time seconds;
        max-age seconds;
        interface (interface-name disable | interface-range-name | all ){
            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>;
    }
    vlan-group group group-name {
        vlansvlan-name (vlan-id |vlan-range | open-set-of-values) {
            interface all;
            interface interface-name {
                disable;
            }
```

```
    }
}
```

Hierarchy Level

```
[edit protocols]
```

```
[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.
Statement introduced in Junos OS Release 9.4 for EX Series switches.
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.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement updated in Junos OS Release 15.1 for EX Series switches to support configuration of spanning tree parameters globally on all interfaces.

NOTE: You cannot disable spanning tree parameters globally on all interfaces.

Description

Configures VLAN Spanning Tree Protocol (VSTP). VSTP is used to prevent loops in Layer 2 networks on a per-VLAN basis.

You can have a maximum of 253 VSTP VLANs per switch.

If the number of VLANs on your switch exceeds the VSTP VLAN limit, you must use the **vlan** statement to specify which VLANs or VLAN groups use VSTP. You also cannot use the **vlan all** option to configure VSTP when your switch has more than the maximum allowed VSTP VLANs. To ensure all VLANs are running a spanning-tree protocol, run RSTP for networks with large numbers of VLANs .

> **NOTE:** When you configure VSTP with the **set protocol vstp vlan all** command, VLAN ID 1 is not set; it is excluded so that the configuration is compatible with Cisco PVST+. If you want VLAN ID 1 to be included in the VSTP configuration on your switch, you must set it separately with the **set protocol vstp vlan 1** command.

> **NOTE:** Option **vlan all** is not supported in Junos OS Release 13.2X50.

> **BEST PRACTICE:** Configure RSTP when you configure VSTP. RSTP overhead is minimal and this configuration ensures that some spanning tree protocol is running on all VLANs on your switch, even when your switch has more than the maximum number of allowed VSTP VLANs.

The remaining statements are explained separately. See CLI Explorer.

Default

VSTP is not enabled by default.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding VSTP | 143
- *Configuring VLAN Spanning Tree Protocol*
- *Configuring VSTP (CLI Procedure)*
- *Example: Configuring VSTP on QFX Series Switches and EX4600 Switches*
- show spanning-tree bridge | 403
- show spanning-tree interface | 410

CHAPTER 9

Operational Commands

clear error bpdu interface

List of Syntax

MX Series on page 384
QFX Series, EX Series, NFX Series on page 384

MX Series

```
clear error bpdu interface interface-name
```

QFX Series, EX Series, NFX Series

```
clear error bpdu interface (all | interface-name)
```

Release Information

Command introduced in Junos OS Release 9.4.
Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Command supports **all** option in Junos OS Release 15.1 for EX Series switches.

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 on ACX Router, EX Switch and MX Router Edge Ports | 181
Unblocking a Switch Interface That Receives BPDUs in Error (CLI Procedure) | 285

List of Sample Output

clear error bpdu interface ge-1/1/1 on page 385

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear error bpdu interface ge-1/1/1

```
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.
Command introduced in Junos OS Release 14.1X53-D10 and 17.3R1 for EX4300 switches.
Command introduced in Junos OS Release 15.1X53-D55 and 18.2R1 for EX2300 and EX3400 switches.
Command introduced in Junos OS Release 17.4R1 for EX4600 switches.
Command introduced in Junos OS Release 19.1R1 for QFX Series switches.

Description

Clear a MAC rewrite error condition on an interface receiving tunneled Layer 2 protocol packets.

On interfaces with L2PT configured, customer-facing ports should not receive packets with the L2PT MAC address as the destination address unless there is a network tolopogy or configuration error. The device sets the status of such interfaces to “Disabled”. Use this command to clear the error and re-enable the interface.

Options

interface *interface-name*—(Optional) Clear the MAC rewrite error condition for the specified interface.

Required Privilege Level

clear

RELATED DOCUMENTATION

Configuring Layer 2 Protocol Tunneling

Clearing a MAC Rewrite Error on an Interface with Layer 2 Protocol Tunneling

show mac-rewrite interface | **401**

List of Sample Output

clear error mac-rewrite interface on page 387

Output Fields

When you enter this command, the device returns feedback on the status of the request.

Sample Output

clear error mac-rewrite interface

```
user@host> clear error mac-rewrite interface ge-1/0/1
```

clear ethernet-switching bpdu-error interface

Syntax

```
clear ethernet-switching bpdu-error interface interface-name
```

Release Information

Command introduced in Junos OS Release 9.1 for EX Series switches.
Command updated in Junos OS Release 11.1 for EX Series switches—a BPDU error shuts down the interface and this command brings the interface back up.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Clear bridge protocol data unit (BPDU) errors from an interface and bring up the interface.

> **NOTE:** This command is only available on switches running Junos OS without support for the Enhanced Layer 2 Software (ELS) configuration style. To clear BPDU errors from switches that support ELS, see **clear error bpdu interface**.

Options

interface-name—Clear BPDU errors on the specified interface.

Required Privilege Level

clear

RELATED DOCUMENTATION

- show spanning-tree interface | **410**

List of Sample Output

clear ethernet-switching bpdu-error interface on page 388

Sample Output

clear ethernet-switching bpdu-error interface

```
user@switch> clear ethernet-switching bpdu-error interface xe-0/0/1.0
```

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

List of Syntax

Syntax

```
clear spanning-tree statistics
<interface interface-name>
<logical-system logical-system-name>
```

Syntax (EX Series Switches and the QFX Series)

```
clear spanning-tree statistics
<interface interface-name>
```

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

Clear Spanning Tree Protocol statistics for all interfaces or a specified interface.

Options

none—Reset STP counters for all interfaces for all routing instances.

interface *interface-name*—(Optional) Clear STP statistics for the specified interface only.

logical-system *logical-system-name*—(Optional) Clear STP statistics on a particular logical system.

> **NOTE:** The **logical-system** option is not available on QFabric systems.

Required Privilege Level

clear

RELATED DOCUMENTATION

Understanding STP | 40

show spanning-tree statistics | 425

show spanning-tree bridge | 403

show spanning-tree interface | 410

List of Sample Output

clear spanning-tree statistics on page 391

Output Fields

This command produces no output.

Sample Output

clear spanning-tree statistics

```
user@switch> clear spanning—tree statistics
```

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 392

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 393

Sample Output

clear spanning-tree stp-buffer (MX Series)

```
user@host> clear spanning-tree stp-buffer
```

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 397
show bridge mac-table (with Layer 2 Services over GRE Interfaces) on page 397
show bridge mac-table (with VXLAN enabled) on page 398
show bridge mac-table age (for GE interface) on page 398
show bridge mac-table age (for AE interface) on page 398
show bridge mac-table count on page 399
show bridge mac-table detail on page 399
show bridge mac-table instance pbb-evpn on page 400
show bridge mac-table on page 400

Output Fields

Table 22 on page 395 describes the output fields for the **show bridge mac-table** command. Output fields are listed in the approximate order in which they appear.

Table 22: 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.

Table 22: show bridge mac-table Output Fields *(continued)*

Field Name	Field Description
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.
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 and 17.3R1 for EX4300 switches.
Command introduced in Junos OS Release 15.1X53-D55 and 18.2R1 for EX2300 and EX3400 switches.
Command introduced in Junos OS Release 17.4R1 for EX4600 switches.
Command introduced in Junos OS Release 19.1R1 for QFX Series switches.

Description

Display Layer 2 protocol tunneling (L2PT) information.

Options

brief | detail—(Optional) Display the specified level of output.

interface *interface-name*—(Optional) Display L2PT information for the specified interface.

Required Privilege Level

view

RELATED DOCUMENTATION

- layer2-control | **327**
- mac-rewrite | **330**
- protocol | **350**
- *Understanding Layer 2 Protocol Tunneling*
- *Configuring Layer 2 Protocol Tunneling*

List of Sample Output

show mac-rewrite interface on page 402
show mac-rewrite interface (EX Series Switches) on page 402

Output Fields

Table 23 on page 402 lists the output fields for the **show mac-rewrite interface** command. Output fields are listed in the approximate order in which they appear.

Table 23: show mac-rewrite interface Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface on which L2PT is configured.	brief detail
Protocols	Layer 2 protocols being tunneled on this interface. All devices that support L2PT can tunnel the following protocols: Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunk Protocol (VTP). The following Layer 2 protocols can also be tunneled on some devices that support L2PT: E-LMI, GVRP, IEEE 802.1X, IEEE 802.3AH, LACP, LLDP, MMRP, MVRP, PVSTP+, UDLD, or VSTP. See protocol for more information on the supported protocols for tunneling on different devices.	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 Switches)

```
user@switch> show mac-rewrite interface
```

```
Interface       Protocols

 ge-0/0/1       802.3AH LLDP STP
```

show spanning-tree bridge

List of Syntax

Syntax

```
show spanning-tree bridge
<brief | detail>
<msti msti-id>
<routing-instance routing-instance-name>
<vlan-id vlan-id>
```

Syntax (QFX Series and EX 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 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Displays the configured or calculated spanning-tree protocol (can be either STP, RSTP, MSTP, or VSTP) 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 spanning-tree protocol bridge information for the specified MSTI or Common and Internal Spanning Tree (CIST). Specify **0** for CIST. Specify a value from **1** through **4094** for an MSTI.

routing-instance *routing-instance-name*—(Optional) Display STP bridge information for the specified routing instance.

vlan-id *vlan-id*—(Optional) Display spanning-tree protocol bridge information for the specified VLAN. Specify a VLAN tag identifier from **1** through **4094**.

Required Privilege Level
view

RELATED DOCUMENTATION

- Understanding STP | 40
- Understanding RSTP | 44
- Example: Configuring Network Regions for VLANs with MSTP on Switches | 111
- show spanning-tree interface | 410

List of Sample Output

show spanning-tree bridge routing-instance on page 405
show spanning-tree bridge msti on page 407
show spanning-tree bridge vlan-id (MSTP) on page 407
show spanning-tree bridge (RSTP) on page 408
show spanning-tree bridge vlan-id (RSTP) on page 409

Output Fields

Table 24 on page 404 lists the output fields for the **show spanning-tree bridge** command. Output fields are listed in the approximate order in which they appear.

Table 24: 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.
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.

Table 24: show spanning-tree bridge Output Fields *(continued)*

Field Name	Field Description
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 1 101 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

```
show spanning-tree interface
<brief | detail>
<msti msti-id>
<routing-instance routing-instance-name>
<vlan-id vlan-id>
```

Syntax (EX Series Switches and QFX Series Switches)

```
show spanning-tree interface
<brief | detail>
<msti msti-id>
<vlan-id vlan-id>
```

Syntax (EX Series Switches)

```
show spanning-tree interface
<brief | detail>
<interface-name interface-name>
<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 spanning-tree protocol (can be either STP, RSTP, or MSTP) parameters. In **brief** mode, will not display interfaces that are administratively disabled or do not have a physical link.

Options

none—Display brief STP interface information.

brief | detail—(Optional) Display the specified level of output.

interface-name *interface-name*—(Optional) Name of an interface.

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

RELATED DOCUMENTATION

- show spanning-tree bridge | **403**
- Example: Configuring Network Regions for VLANs with MSTP on Switches | **111**
- Understanding STP | **40**
- Understanding RSTP | **44**
- Understanding MSTP | **97**

List of Sample Output

Output Fields

Table 25 on page 412 lists the output fields for the **show spanning-tree interface** command. Output fields are listed in the approximate order in which they appear.

Table 25: show spanning-tree Interface Output Fields

Field Name	Field Description
Interface name	Interface configured to participate in the STP, RSTP, VSTP, or MSTP instance.
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**).
Edge delay while expiry count	Number of times the edge delay timer expired on that interface.
Rcvd info while expiry count	Number of times the rcvd info timer expired on that interface.

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 (EX Series)

`user@switch>` **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   8192.0019e2500340    1000   FWD    DESG
ge-0/0/2.0  128:515  128:515   8192.0019e2500340    1000   BLK    DIS
```

```
ge-0/0/4.0  128:517  128:517   8192.0019e2500340    1000   FWD    DESG
ge-0/0/23.0 128:536  128:536   8192.0019e2500340    1000   FWD    DESG


Spanning tree interface parameters for instance 1

Interface    Port ID    Designated  Designated     Port    State  Role
                         port ID    bridge ID      Cost
ge-0/0/0.0  128:513  128:513   8193.0019e2500340    1000   FWD    DESG
ge-0/0/2.0  128:515  128:515   8193.0019e2500340    1000   BLK    DIS
ge-0/0/4.0  128:517  128:517   8193.0019e2500340    1000   FWD    DESG
ge-0/0/23.0 128:536  128:536   8193.0019e2500340    1000   FWD    DESG

Spanning tree interface parameters for instance 2

Interface    Port ID    Designated  Designated     Port    State  Role
                         port ID    bridge ID      Cost
ge-0/0/0.0  128:513  128:1   8194.001b549fd000  1000  FWD    ROOT
ge-0/0/2.0  128:515  128:515  32770.0019e2500340  4000  BLK    DIS
ge-0/0/4.0  128:517  128:1    16386.001b54013080  1000  BLK    ALT
ge-0/0/23.0 128:536  128:536  32770.0019e2500340  1000  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 detail (EX Series)

`user@switch>` **show spanning-tree interface detail**

```
Spanning tree interface parameters for instance 0

Interface name     : ge-1/0/0.0
Port identifier    : 128.625
Designated port ID     : 128.625
Port cost      : 20000
Port state     : Blocking
Designated bridge ID   : 32768.00:19:e2:50:95:a0
Port role      : Disabled
Link type      : Pt-Pt/EDGE
Boundary port       : NA
Edge delay while expiry count  : 0
Rcvd info while expiry count   : 0

Interface name     : ge-1/0/1.0
Port identifier    : 128.626
Designated port ID     : 128.626
Port cost      : 20000
Port state     : Blocking
Designated bridge ID   : 32768.00:19:e2:50:95:a0
Port role      : Disabled
Link type      : Pt-Pt/NONEDGE
Boundary port       : NA
Edge delay while expiry count  : 0
Rvcd info while expiry count   : 0

Interface name     : ge-1/0/2.0
Port identifier    : 128.627
Designated port ID     : 128.627
Port cost      : 20000
Port state     : Blocking
Designated bridge ID   : 32768.00:19:e2:50:95:a0
Port role      : Disabled
Link type      : Pt-Pt/NONEDGE
Boundary port       : NA
Edge delay while expiry count  : 0
Rvcd info while expiry count   : 0
```

```
Interface name     : ge-1/0/10.0
Port identifier    : 128.635
Designated port ID     : 128.635
Port cost      : 20000
Port state     : Blocking
Designated bridge ID   : 32768.00:19:e2:50:95:a0
Port role      : Disabled
Link type      : Pt-Pt/NONEDGE
Boundary port       : NA
Edge delay while expiry count  : 0
Rvcd info while expiry count   : 0

Interface name     : ge-1/0/20.0
Port identifier    : 128.645
Designated port ID     : 128.645
Port cost      : 20000
Port state     : Blocking
Designated bridge ID   : 32768.00:19:e2:50:95:a0
Port role      : Disabled
Link type      : Pt-Pt/NONEDGE
Boundary port       : NA
Edge delay while expiry count  : 0
Rvcd info while expiry count   : 0
[output truncated]
```

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 interface brief (EX Series)

`user@switch>` **show spanning-tree interface brief**

```
Spanning tree interface parameters for instance 0

Interface    Port ID    Designated  Designated     Port    State  Role
     port ID    bridge ID  Cost
ge-1/0/0.0  128:625  128:625  32768.0019e25095a0 20000  BLK    DIS
ge-1/0/1.0  128:626  128:626  32768.0019e25095a0 20000  BLK    DIS
ge-1/0/2.0  128:627  128:627  32768.0019e25095a0 20000  BLK    DIS
ge-1/0/10.0 128:635  128:635  32768.0019e25095a0 20000  BLK    DIS
ge-1/0/20.0 128:645  128:645  32768.0019e25095a0 20000  BLK    DIS
ge-1/0/30.0 128:655  128:655  32768.0019e25095a0 20000  BLK    DIS
```

show spanning-tree interface ge-1/0/0 (EX Series)

`user@switch>` **show spanning-tree interface ge-1/0/0**

```
Interface    Port ID    Designated  Designated     Port    State  Role
     port ID    bridge ID  Cost
ge-1/0/0.0 128:625  128:625  32768.0019e25095a0 20000  BLK    DIS
```

show spanning-tree mstp configuration

List of Syntax

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

RELATED DOCUMENTATION

Understanding MSTP | 97
Example: Configuring Network Regions for VLANs with MSTP on Switches | 111
show spanning-tree bridge | 403

show spanning-tree statistics | 425
mstp | 340

List of Sample Output

show spanning-tree mstp configuration detail on page 423
show spanning-tree mstp configuration detail (QFX Series) on page 424
show spanning-tree mstp configuration (EX Series) on page 424

Output Fields

Table 26 on page 423 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 26: 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 mstp configuration (EX Series)

`user@host>` **show spanning-tree mstp configuration**

```
MSTP configuration information
Context identifier     : 0
Region name            : region1
Revision               : 0
Configuration digest   : 0xc92e7af9febb44d8df928b87f16b


MSTI     Member VLANs
   0 0-100,105-4094
   1 101-102
   2 103-104
```

show spanning-tree statistics

List of Syntax

Syntax

```
show spanning-tree statistics
<brief | detail>
<interface interface-name>
<routing-instance routing-instance-name>
```

Syntax (EX Series and QFX Series)

```
show spanning-tree statistics
<brief | detail>
<interface interface-name | vlan vlan-id>
```

Syntax (EX Series)

```
show spanning-tree statistics
interface interface-name
vlan vlan-id
<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 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 426
show spanning-tree statistics interface routing-instance detail on page 427

Output Fields
Table 27 on page 426 lists the output fields for the **show spanning-tree statistics** command. Output fields are listed in the approximate order in which they appear.

Table 27: 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.
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 428

Output Fields

Table 28 on page 428 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 28: 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 431

Output Fields

Table 29 on page 430 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 29: 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 432

Output Fields

Table 30 on page 432 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 30: 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 436
show spanning-tree stp-buffer see-all stp-instance stp-instance-id routing-instance instance-name (MX Series) on page 437
show spanning-tree stp buffer see-all vlan vlan-id routing-instance instance-name (MX Series) on page 438

Output Fields

Table 31 on page 435 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 31: 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**
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**

Table 31: show spanning-tree stp-buffer see-all Output Fields *(continued)*

Field Name	Field Description	Level of Output
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
```