JUNIPER NETWORKS | Engineering Simplicity

Spanning-Tree Protocols User Guide

Published
2024-06-12

JUNOS

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Spanning-Tree Protocols User Guide
Copyright © 2024 Juniper Networks, Inc. All rights reserved.

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

About This Guide | viii

1 Overview

Spanning Tree Protocol Overview | 2

How Spanning Tree Protocols Work | 2

Choosing a Spanning Tree Protocol | 6

2 Spanning-Tree Instances and Interfaces

Spanning Tree Instances and Interfaces | 18

Understanding Spanning-Tree Instance Interfaces | 18

Configuring a Virtual Switch Routing Instance on MX Series Routers | 20

Configuring a Spanning-Tree Instance Interface as an Edge Port for Faster Convergence | 21

3 Configuring Spanning-Tree Protocols

Configuring STP | 23

Understanding STP | 23

Understanding System Identifiers for Bridges in STP or RSTP Instances | 24

Configuring STP | 24

Configuring RSTP | 26

Understanding RSTP | 26

Configuring Rapid Spanning Tree Protocol | 27

Configuring RSTP on Devices That Support Enhanced Layer 2 Software (ELS) | 31

Example: Configuring Faster Convergence and Network Stability on ELS Devices with RSTP | 32

Requirements | 32

Overview and Topology | 33

Configuring RSTP and Nonstop Bridging on Switch 1 | 36

Configuring RSTP and Nonstop Bridging on Switch 2 | 41

Configuring RSTP and Nonstop Bridging on Switch 3 | 46

Configuring RSTP and Nonstop Bridging on Switch 4 | 51

Verification | 55

Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | 59

Requirements | 59

Overview and Topology | 60

Configuring RSTP and Nonstop Bridging on Switch 1 | 63

Configuring RSTP and Nonstop Bridging on Switch 2 | 68

Configuring RSTP and Nonstop Bridging on Switch 3 | 73

Configuring RSTP and Nonstop Bridging on Switch 4 | 78

Verification | 82

Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure) | 86

Configuring MSTP | 87

Understanding MSTP | 87

Configuring MSTP | 91

Configuring MSTP Instances on a Physical Interface | 95

Example: Configuring Network Regions for VLANs with MSTP | 97

Requirements | 97

Overview and Topology | 98

Configuring MSTP on Switch 1 | 101

Configuring MSTP on Switch 2 | 106

Configuring MSTP on Switch 3 | 111

Configuring MSTP on Switch 4 | 116

Verification | 120

Disabling MSTP | 129

Configuring VSTP | 130

Understanding VSTP | 131

Global and Specific VSTP Configurations for Switches | 132

Example: Configuring VSTP on a Trunk Port with Tagged Traffic | 136

Requirements | 137

Overview | 137

Configuration | 138

Verification | **150**

Reverting to RSTP or VSTP from Forced IEEE 802.1D STP | **153**

4 **BPDU Protection for Spanning-Tree Protocols**

BPDU Protection for Spanning-Tree Protocols | 156

Understanding BPDU Protection for Spanning-Tree Instance Interfaces | **156**

Understanding BPDU Protection for STP, RSTP, and MSTP | **158**

Configuring BPDU Protection for Individual Spanning-Tree Instance Interfaces | **158**

Understanding BPDUs Used for Exchanging Information Among Bridges | **159**

Understanding BPDU Protection for EVPN-VXLAN | **160**

Configuring Interface for BPDU Protection With Port Shutdown Mode | **160**

Configuring Interface for BPDU Protection With BPDU Drop Mode | **163**

Configuring BPDU Protection for Edge Interfaces | **166**

Example: Blocking BPDUs on an Interface for 600 Seconds | **169**

Example: Configuring BPDU Protection on Interfaces | **169**

Requirements | **170**

Overview and Topology | **170**

Configuration | **173**

5 **Loop Protection for Spanning-Tree Protocols**

Loop Protection for Spanning-Tree Protocols | 177

Understanding Loop Protection for Spanning-Tree Instance Interfaces | **177**

Eliminating Bridge Loops in Ethernet LANs with Spanning Tree Protocol | **179**

Example: Enabling Loop Protection for Spanning-Tree Protocols | **187**

Configuring Loop Protection for a Spanning-Tree Instance Interface | **187**

Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on non-ELS EX Series Switches | **189**

Requirements | **189**

Overview and Topology | **190**

Configuration | **192**

Verification | **193**

Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches With ELS | **195**

Requirements | **196**

Overview and Topology | **196**

Configuration | **198**

Verification | **199**

6 **Root Protection for VPLS Multihome Environments**

Root Protection for VPLS Multihome Environments | 203

Understanding VPLS Multihoming | **203**

Understanding Bridge Priority for Election of Root Bridge and Designated Bridge | **208**

Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network | **208**

Example: Configuring VPLS Root Topology Change Actions | **210**

Enabling Root Protection for a Spanning-Tree Instance Interface | **210**

Configuring VPLS Root Protection Topology Change Actions to Control Individual VLAN Spanning-Tree Behavior | **211**

Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches | **213**

Requirements | **213**

Overview and Topology | **213**

Configuration | **216**

Verification | **217**

Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on EX Series Switches With ELS | **220**

Requirements | **220**

Overview and Topology | **221**

Configuration | **223**

Verification | **224**

7 **Monitoring and Troubleshooting**

Monitoring and Troubleshooting Spanning Tree Protocols | 229

Monitoring Spanning Tree Protocols on Switches | **229**

Checking the Status of Spanning-Tree Instance Interfaces | **232**

Understanding Spanning-Tree Protocol Trace Options | **233**

Configuring Tracing Spanning-Tree Operations | **233**

Example: Tracing Spanning-Tree Protocol Operations | **236**

Unblocking a Switch Interface That Receives BPDUs in Error (CLI Procedure) | **236**

Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error (CLI Procedure) | **237**

Clearing the Blocked Status of a Spanning-Tree Instance Interface | **238**

Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface | **238**

Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface | **239**

Clearing a MAC Rewrite Error on an Interface with Layer 2 Protocol Tunneling | **239**

Understanding Forward Delay Before Ports Transition to Forwarding State | **240**

8 **Configuration Statements and Operational Commands**

Junos CLI Reference Overview | 242

About This Guide

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

CHAPTER 1

Overview

Spanning Tree Protocol Overview | 2

Spanning Tree Protocol Overview

IN THIS SECTION

- How Spanning Tree Protocols Work | 2
- Choosing a Spanning Tree Protocol | 6

How Spanning Tree Protocols Work

IN THIS SECTION

- Benefits of Using Spanning Tree Protocols | 3
- Spanning Tree Protocols Help Prevent Broadcast Storms | 3
- Understanding Bridge Priority for Election of Root Bridge and Designated Bridge | 3
- Port Roles Determine Participation in the Spanning Tree | 4
- Port States Determine How a Port Processes a Frame | 4
- Edge Ports Connect to Devices That Cannot Be Part of a Spanning Tree | 4
- BPDUs Maintain the Spanning-Tree | 5
- When a Root Bridge Fails | 5
- Devices Must Relearn MAC Addresses After a Link Failure | 6

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*.

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.

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 | 23

Understanding MSTP | 87

Understanding RSTP | 26

Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | 59

Example: Configuring Faster Convergence and Network Stability on ELS Devices with RSTP | 32

Configuring RSTP on Devices That Support Enhanced Layer 2 Software (ELS) | 31

Choosing a Spanning Tree Protocol

IN THIS SECTION

- Comparison of Spanning Tree Features | 7
- Switch and Router Spanning Tree Support and Limitations | 12

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 1 on page 7 describes differences between spanning-tree protocols STP, RSTP, MSTP and VSTP.

Table 1: 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 86

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 153.

Table 1: 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-—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.

Table 1: Selecting a Spanning-Tree Protocol *(Continued)*

Protocol	Advantages	Disadvantages
		• 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.
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 24.		
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 91.		

Table 1: 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.	• 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

Table 1: Selecting a Spanning-Tree Protocol *(Continued)*

Protocol	Advantages	Disadvantages
		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 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 2 on page 12.

Table 2: 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 20 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 233. 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.

Table 2: Spanning Tree Hardware Considerations *(Continued)*

Router or Switch	Considerations
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.	
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 233.

Table 2: Spanning Tree Hardware Considerations *(Continued)*

Router or Switch	Considerations
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 86. 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 2: 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 86. • 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.

Table 2: Spanning Tree Hardware Considerations *(Continued)*

Router or Switch	Considerations
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.	
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 Firewalls	• 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 Firewalls. Be sure to use the correct commands for each version. Some SRX Series Firewalls 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 | 18

Spanning Tree Instances and Interfaces

IN THIS SECTION

- Understanding Spanning-Tree Instance Interfaces | 18
- Configuring a Virtual Switch Routing Instance on MX Series Routers | 20
- Configuring a Spanning-Tree Instance Interface as an Edge Port for Faster Convergence | 21

Understanding Spanning-Tree Instance Interfaces

IN THIS SECTION

- Benefits of Spanning-Tree Instance Interface Configuration | 18
- How Many Instances Do Spanning Tree Protocols Have? | 19
- Spanning-Tree Instance Interfaces Have Priorities | 19
- What is Spanning-Tree Instance Interface Cost? | 19

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* .

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

Configuring Rapid Spanning Tree Protocol | **27**

Configuring Multiple Spanning Tree Protocol

Configuring VLAN Spanning Tree Protocol

edge

interface (Spanning Tree)

Configuring RSTP on Devices That Support Enhanced Layer 2 Software (ELS) | **31**

Configuring MSTP | **91**

3

CHAPTER

Configuring Spanning-Tree Protocols

Configuring STP | 23

Configuring RSTP | 26

Configuring MSTP | 87

Configuring VSTP | 130

Configuring STP

IN THIS SECTION

- Understanding STP | 23
- Understanding System Identifiers for Bridges in STP or RSTP Instances | 24
- Configuring STP | 24

Understanding STP

IN THIS SECTION

- Benefits of Using the Original STP | 23
- STP on Devices That Support Enhanced Layer 2 Software (ELS) | 24
- STP Operation Mode Commands | 24

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 Devices That Support Enhanced Layer 2 Software (ELS)

Devices configured to use STP run RSTP force version 0, which is compatible with STP. If you are using Junos OS for devices that support 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.

Configuring STP

The default spanning-tree protocol for devices that support Enhanced Layer 2 Software (ELS) 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

IN THIS SECTION

- Understanding RSTP | 26
- Configuring Rapid Spanning Tree Protocol | 27
- Configuring RSTP on Devices That Support Enhanced Layer 2 Software (ELS) | 31
- Example: Configuring Faster Convergence and Network Stability on ELS Devices with RSTP | 32
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches | 59
- Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure) | 86

Understanding RSTP

IN THIS SECTION

- Benefits of Using RSTP | 26
- Why is RSTP the Default Spanning-Tree Protocol? | 27

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 Series and ACX Series 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 run RSTP force version 0, which is compatible with STP.

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 232.

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 208.

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 Devices That Support Enhanced Layer 2 Software (ELS)

The default spanning-tree protocol on devices that support ELS is Rapid Spanning Tree Protocol (RSTP). RSTP provides faster convergence times than the original Spanning Tree Protocol (STP).You can configure VSTP and RSTP on a device at the same time. If you have configured MSTP on your device, you cannot configure RSTP on the device. You need to use this procedure only if another spanning-tree protocol is configured on your device.

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 Devices with RSTP

IN THIS SECTION

- Requirements | 32
- Overview and Topology | 33
- Configuring RSTP and Nonstop Bridging on Switch 1 | 36
- Configuring RSTP and Nonstop Bridging on Switch 2 | 41
- Configuring RSTP and Nonstop Bridging on Switch 3 | 46
- Configuring RSTP and Nonstop Bridging on Switch 4 | 51
- Verification | 55

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 59. 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 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

IN THIS SECTION

- Topology | 36

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 34 to create a loop-free topology with NSB applied to switches with dual Routing Engines.

Figure 1: Network Topology for RSTP

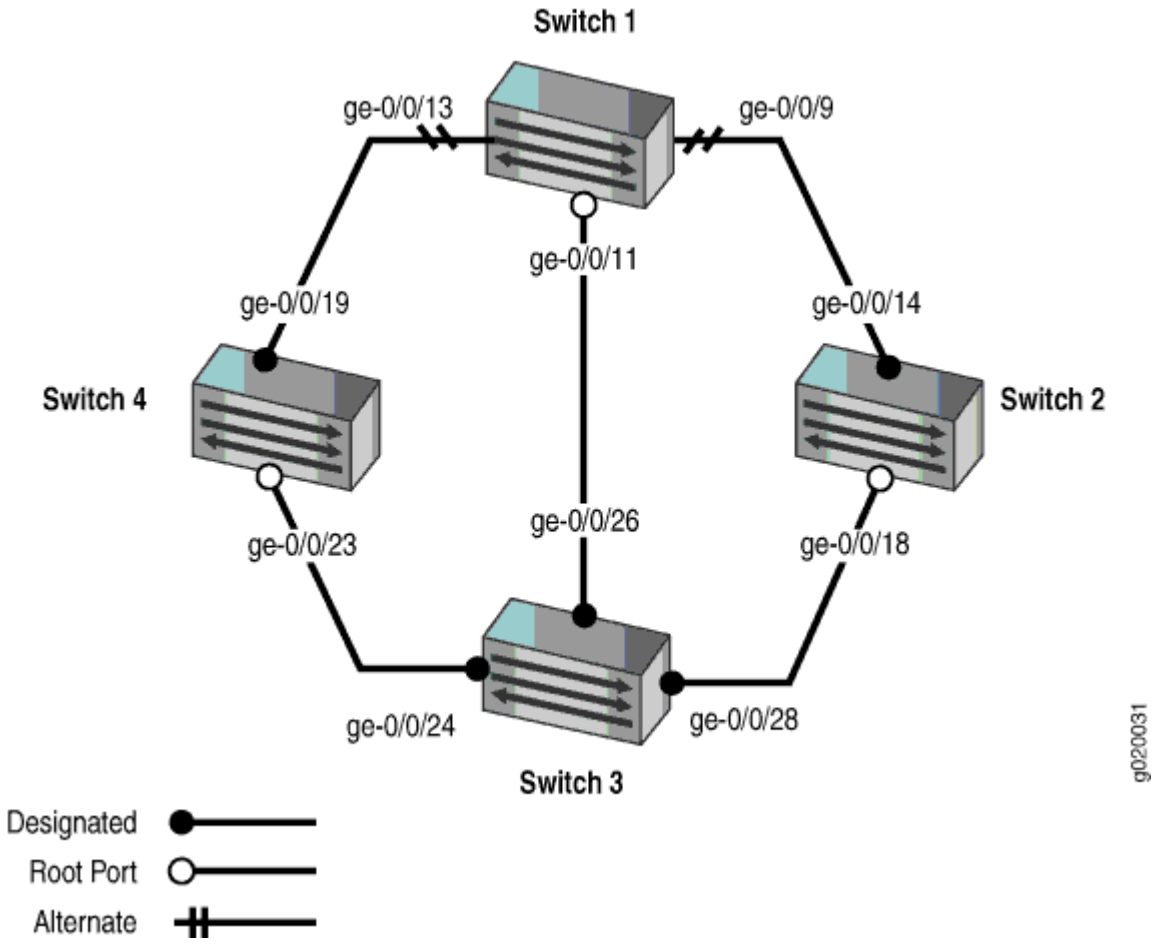


Table 3 on page 35 shows the components of the topology for this example.

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

Table 3: 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*.

Topology

Configuring RSTP and Nonstop Bridging on Switch 1

IN THIS SECTION

- Procedure | 36

Procedure

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

IN THIS SECTION

- Procedure | 41

Procedure

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 31 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

IN THIS SECTION

- Procedure | 46

Procedure

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

IN THIS SECTION

- Procedure | 51

Procedure

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

- Verifying RSTP Configuration on Switch 1 | **56**

- Verifying RSTP Configuration on Switch 2 | 57
- Verifying RSTP Configuration on Switch 3 | 57
- Verifying RSTP Configuration on Switch 4 | 58

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

- Requirements | 59
- Overview and Topology | 60
- Configuring RSTP and Nonstop Bridging on Switch 1 | 63
- Configuring RSTP and Nonstop Bridging on Switch 2 | 68
- Configuring RSTP and Nonstop Bridging on Switch 3 | 73
- Configuring RSTP and Nonstop Bridging on Switch 4 | 78
- Verification | 82

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

IN THIS SECTION

- Topology | 63

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 61 to create a loop-free topology with NSB applied to switches with dual Routing Engines.

Figure 2: Network Topology for RSTP

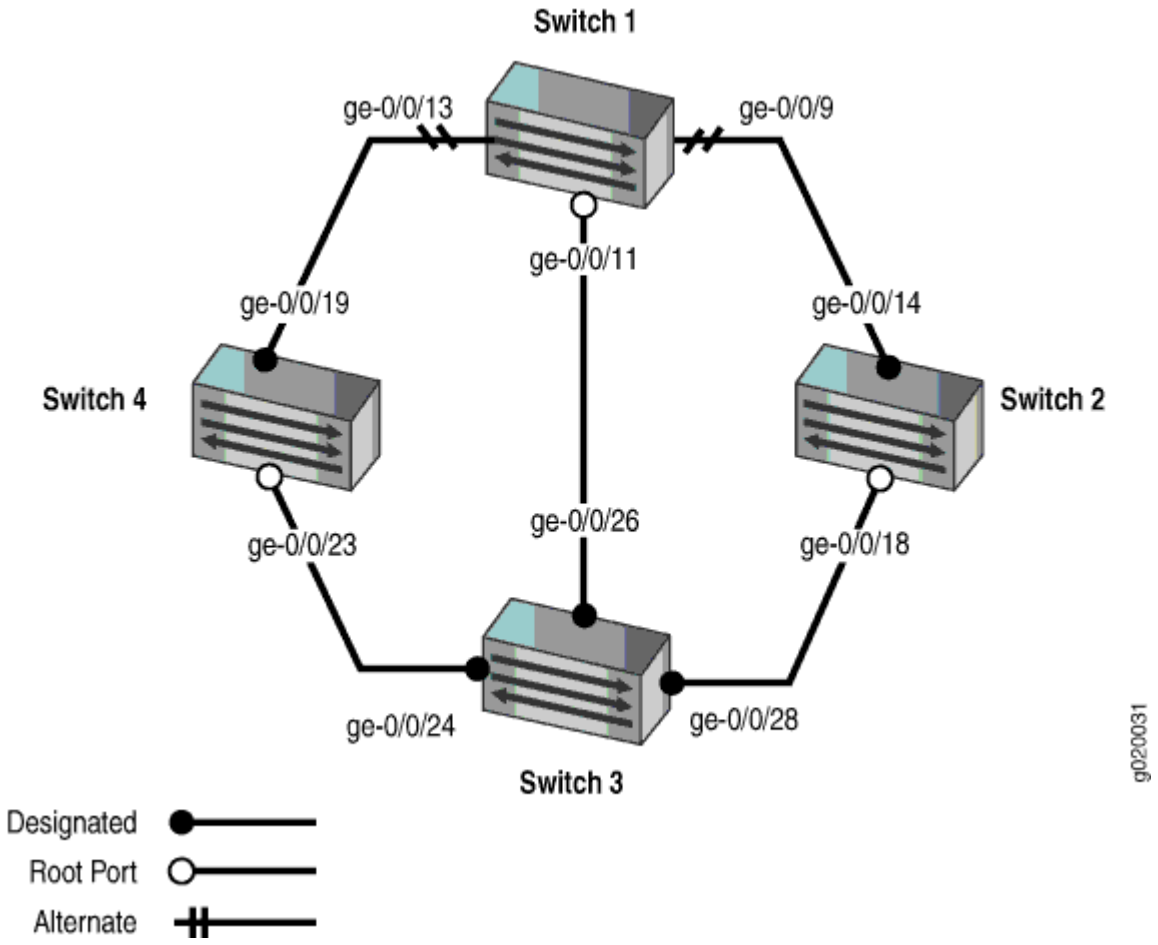


Table 4 on page 62 shows the components of the topology for this example.

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

Table 4: 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 EX Series Switches*.

Topology

Configuring RSTP and Nonstop Bridging on Switch 1

IN THIS SECTION

- Procedure | 63

Procedure

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

IN THIS SECTION

- Procedure | 68

Procedure

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

IN THIS SECTION

- Procedure | 73

Procedure

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

IN THIS SECTION

- Procedure | 78

Procedure

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

Verifying RSTP Configuration on Switch 1 | 83

- Verifying RSTP Configuration on Switch 2 | **84**
- Verifying RSTP Configuration on Switch 3 | **84**
- Verifying RSTP Configuration on Switch 4 | **85**

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:

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.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

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

IN THIS SECTION

- Understanding MSTP | 87
- Configuring MSTP | 91
- Configuring MSTP Instances on a Physical Interface | 95
- Example: Configuring Network Regions for VLANs with MSTP | 97
- Disabling MSTP | 129

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

- Benefits of MSTP | 88
- MSTP Maps Multiple VLANs | 88
- Configuring MSTP Regions | 89
- Selecting a Spanning Tree Protocol | 89

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 Series and ACX Series 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 5 on page 89 below.

Table 5: 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.

Table 5: 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, 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 | 26

Understanding VSTP

Configuring MSTP

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

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@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 232.

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 208.

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 that 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 | 95

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*.

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 208.

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;
            }
        }
    }
}
```

Example: Configuring Network Regions for VLANs with MSTP

IN THIS SECTION

- Requirements | 97
- Overview and Topology | 98
- Configuring MSTP on Switch 1 | 101
- Configuring MSTP on Switch 2 | 106
- Configuring MSTP on Switch 3 | 111
- Configuring MSTP on Switch 4 | 116
- Verification | 120

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

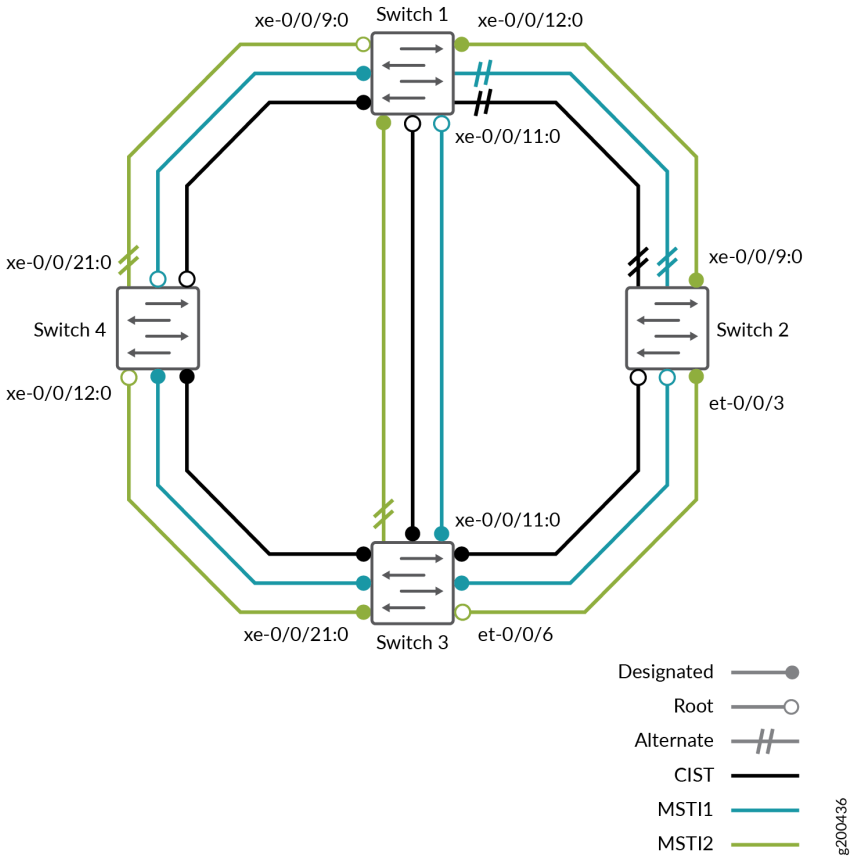
IN THIS SECTION

- Topology | 99

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.

Topology

Figure 3: Network Topology for MSTP



The interfaces shown in Figure 3 on page 99 will be configured for MSTP.

Table 6: 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

Table 6: Components of the Topology for Configuring MSTP on EX Series Switches *(Continued)*

Property	Settings
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 99 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

IN THIS SECTION

- Procedure | **101**

Procedure

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 91 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

IN THIS SECTION

- Procedure | 107

Procedure

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

IN THIS SECTION

- Procedure | 111

Procedure

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

IN THIS SECTION

- Procedure | 116

Procedure

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

- Verifying MSTP Configuration on Switch 1 | **121**
- Verifying MSTP Configuration on Switch 2 | **123**
- Verifying MSTP Configuration on Switch 3 | **125**
- Verifying MSTP Configuration on Switch 4 | **127**

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]**

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

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.

Configuring VSTP

IN THIS SECTION

- Understanding VSTP | **131**
- Global and Specific VSTP Configurations for Switches | **132**
- Example: Configuring VSTP on a Trunk Port with Tagged Traffic | **136**
- Reverting to RSTP or VSTP from Forced IEEE 802.1D STP | **153**

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

Understanding VSTP

IN THIS SECTION

- Benefits of VSTP | 131
- VSTP Restrictions | 131
- Recommended Uses of VSTP | 131

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
- VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a device.

VSTP Restrictions

VSTP has the following restrictions:

- Devices running Layer 2 next-generation (L2NG) software support 510 VLANs on VSTP.
- SRX Series Firewalls support only STP, RSTP, and MSTP; VSTP is not supported.
- In devices that does not support Enhanced Layer 2 Software (ELS), VSTP can support up to 253 VLANs.

Recommended Uses of VSTP

You can use Juniper Networks devices with VSTP, which maintains a separate spanning tree instance per VLAN. One Spanning Tree per VLAN allows fine grain load balancing but requires more BPDU CPU processing as the number of VLANs increases. Juniper Networks devices only inter-operate with PVST+ and Rapid-PVST+. For more information, see VSTP and RPVST+ convergence on native-vlan 1 for EX Switches .

TIP: 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.

SEE ALSO

vlan-group

Global and Specific VSTP Configurations for Switches

IN THIS SECTION

- Where Can I Configure VSTP? | **133**
- VSTP Commands to Configure All Interfaces | **134**
- VSTP Commands to Configure Specific Interfaces | **135**
- VSTP Commands to Disable Interfaces | **135**

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). The default factory configuration for devices that support ELS uses RSTP. This topic describes options for configuring VSTP on devices that support ELS.

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.
- If STP is needed on all the VLANs and the VLANs configured in the system are more than the maximum allowed VLANs for VSTP, then you must use RSTP instead of VSTP.

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

- Requirements | 137
- Overview | 137
- Configuration | 138
- Verification | 150

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

IN THIS SECTION

- Topology | **137**

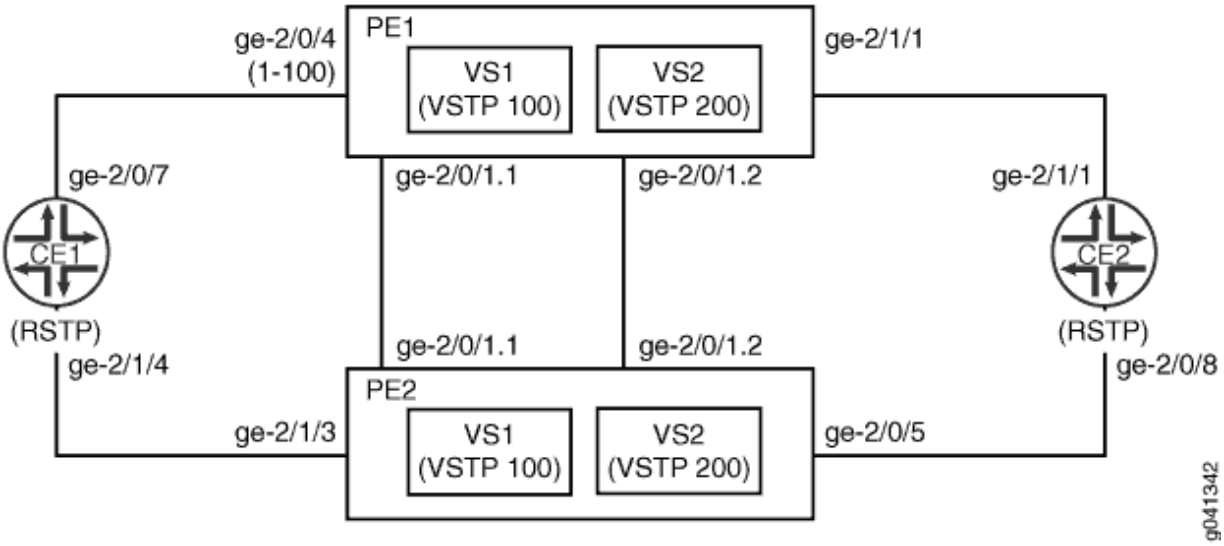
This example shows how to configure VSTP on a trunk port with tagged traffic.

Topology

Figure 4 on page 138 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

IN THIS SECTION

- CLI Quick Configuration | 138
- Configuring PE1, PE2, CE1, and CE2 | 140
- Results | 144

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

- Verifying That the Interfaces Are Operational | **150**
- Verifying the STP Bridge Parameters of the Routing Instances | **151**
- Displaying STP Statistics for the Configured Bridge | **152**

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

Reverting to RSTP or VSTP from Forced IEEE 802.1D STP

On devices that support ELS 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.

4

CHAPTER

BPDU Protection for Spanning-Tree Protocols

BPDU Protection for Spanning-Tree Protocols | 156

BPDU Protection for Spanning-Tree Protocols

IN THIS SECTION

- Understanding BPDU Protection for Spanning-Tree Instance Interfaces | **156**
- Understanding BPDU Protection for STP, RSTP, and MSTP | **158**
- Configuring BPDU Protection for Individual Spanning-Tree Instance Interfaces | **158**
- Understanding BPDUs Used for Exchanging Information Among Bridges | **159**
- Understanding BPDU Protection for EVPN-VXLAN | **160**
- Configuring Interface for BPDU Protection With Port Shutdown Mode | **160**
- Configuring Interface for BPDU Protection With BPDU Drop Mode | **163**
- Configuring BPDU Protection for Edge Interfaces | **166**
- Example: Blocking BPDUs on an Interface for 600 Seconds | **169**
- Example: Configuring BPDU Protection on Interfaces | **169**

Understanding BPDU Protection for Spanning-Tree Instance Interfaces

ACX Series routers, MX Series routers, PTX Series routers, EX Series switches, and QFX 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.

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.

BPDU-block is a feature that defends the STP topology from a misbehaving user application or device or a threat. You must enable BPDU guard on the interfaces that are not supposed to receive any BPDUs.

If an interface is configured to be edge port, it will transition directly to the Forwarding state. Such ports are connected to end devices and are not expected to receive BPDU. Therefore, to avoid loops, you must protect edge ports by enabling bpdu-block-on-edge.

On the routers and switches that support STP, 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 protected interface, the interface is disabled and stops forwarding frames. By default, all BPDUs are accepted and processed on all interfaces.

You can achieve BPDU protection in several ways. By default, if bpdu-block is enabled on the interface, on receiving BPDU, the interface will be disabled and all traffic forwarding will stop on the interface. However, if you do not want to disable the interface and do not want that interface to take part in the STP calculation, you can configure action drop. If you configure action drop, the interface remains up and running and traffic continues to flow; however, BPDUs are dropped.

The edge ports do not support action drop. BPDU-block-on-edge disables the interface if the edge ports receive BPDUs. You must clear the error to bring the interface back up.

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 under the `set protocols (mstp|rstp|vstp)` hierarchy. 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 protocols layer2-control` 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 | 208

Understanding VPLS Multihoming | 203

Understanding BPDU Protection for STP, RSTP, and MSTP

IN THIS SECTION

- Different Types of BPDUs | 158

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 Types 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. The root ports and designated ports forward traffic; the alternate and back up ports block the traffic.

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, *protected 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 router or 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 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 routers and 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)

Understanding BPDU Protection for EVPN-VXLAN

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.

Configuring Interface for BPDU Protection With Port Shutdown Mode

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.

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

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

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

3. Enable BPDU protection on the `et-0/0/0.0` interface:

```
[edit protocols]
user@switch# set layer2-control bpdu-block interface et-0/0/0.0
```

4. Commit the configuration:

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

5. Verify that BPDU protection is configured properly on the interface (`et-0/0/0.0`):

   - Run the `show ethernet-switching interfaces` operational mode command to see the state of STP configured on the interface:

```
user@switch> show ethernet-switching interface et-0/0/0
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down,
                         MMAS - Mac-move action shutdown,  AS - Autostate-exclude enabled,
                         SCTL - shutdown by Storm-control, SL - Secure Learning,
                         MI - MAC+IP limit hit)

Logical         Vlan                  TAG   MAC    MAC+IP STP         Logical
Tagging
interface       members                     limit  limit  state       interface flags
et-0/0/0.0                                  1007616 0                 DN
tagged
                default               1     1007616 0     Discarding
tagged
```

```
                vlan100               100   1007616 0     Discarding
tagged
```

In this output, note that the **et-0/0/0.0** interface is in blocked state because it has received BPDUs from the end device.

- Run the `show spanning-tree interfaces` operational mode command to ensure that the **et-0/0/0.0** interface is blocked:

```
user@switch> show spanning-tree interface et-0/0/0
Spanning tree interface parameters for instance 0

Interface                  Port ID    Designated         Designated         Port    State
Role
                                       port ID           bridge ID          Cost
et-0/0/0                    128:58       128:58  32768.605f7e0507de           50    BLK
DIS (Bpdu-Incon)
```

- Run the `show interfaces` **interface-name** operational mode command to verify that the interface is disabled:

```
user@switch> show interfaces et-0/0/0
Physical interface: et-0/0/0, Enabled, Physical link is Down
  Interface index: 1036, SNMP ifIndex: 521
  Link-level type: Ethernet, MTU: 1518, LAN-PHY mode, Speed: 400Gbps, BPDU Error:
Detected, Loop Detect PDU Error: None, Ethernet-Switching Error: None, MAC-REWRITE Error:
None, Loopback: Disabled, Source filtering: Disabled,
  Flow control: Disabled, Auto-negotiation: Disabled, Media type: Fiber
  Device flags   : Present Running Down
  Interface flags: Down SNMP-Traps Internal: 0x20
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 60:5f:7e:05:00:28, Hardware address: 60:5f:7e:05:00:28
  Last flapped   : 2023-01-19 11:46:36 IST (00:02:03 ago)
  Input rate     : 248 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None
  Active defects : None
  PCS statistics                      Seconds
    Bit errors                             0
    Errored blocks                         0
  PRBS Mode : Disabled
```

```
  Interface transmit statistics: Disabled
  Link Degrade :
    Link Monitoring                   :  Disable

  Logical interface et-0/0/0.0 (Index 1005) (SNMP ifIndex 533)
    Flags: Device-Down SNMP-Traps Encapsulation: Ethernet-Bridge DF
    Input packets : 36590
    Output packets: 0
    Protocol ethernet-switching, MTU: 1518
      Flags: Trunk-Mode
```

The physical link is down and BPDU error is detected.

Configuring Interface for BPDU 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, **et-0/0/0.0**) on the switch:

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

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

```
[edit]
user@switch set layer2-control bpdu-block interface et-0/0/0.0 drop
```

3. Commit the configuration:

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

4. Verify that the BPDU protection action-drop is configured on the interface:

   - Run the `show ethernet-switching interfaces` operational mode command to ensure that the the STP state of the interface is forwarding:

```
user@switch> show ethernet-switching interface et-0/0/0
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down,
                         MMAS - Mac-move action shutdown,  AS - Autostate-exclude enabled,
                         SCTL - shutdown by Storm-control, SL - Secure Learning,
                         MI - MAC+IP limit hit)

Logical         Vlan                  TAG   MAC    MAC+IP STP         Logical
Tagging
interface       members                     limit  limit  state       interface flags
et-0/0/0.0                                  1007616 0
tagged
                default               1     1007616 0     Forwarding
tagged
```

```
                vlan100                 100   1007616 0     Forwarding
tagged
```

In this output, note that the **et-0/0/0.0** interface is up even though it has received incompatible BPDU packets because the **drop** feature is configured for this interface.

- Run the `show interfaces` **interface-name** operational mode command to ensure that the **et-0/0/0.0** interface is displayed in the output and that the **State** of the interface is **Up**:

```
user@switch> show interfaces et-0/0/0
Physical interface: et-0/0/0, Enabled, Physical link is Up
  Interface index: 1036, SNMP ifIndex: 521
  Link-level type: Ethernet, MTU: 1518, LAN-PHY mode, Speed: 400Gbps, BPDU Error: None,
Loop Detect PDU Error: None, Ethernet-Switching Error: None, MAC-REWRITE Error: None,
Loopback: Disabled, Source filtering: Disabled,
  Flow control: Disabled, Auto-negotiation: Disabled, Media type: Fiber
  Device flags   : Present Running Down
  Interface flags: Down SNMP-Traps Internal: 0x20
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 60:5f:7e:05:00:28, Hardware address: 60:5f:7e:05:00:28
  Last flapped   : 2023-01-18 17:44:33 IST (00:00:01 ago)
  Input rate     : 744 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None
  Active defects : None
  PCS statistics                      Seconds
    Bit errors                             0
    Errored blocks                         0
  PRBS Mode : Disabled
  Interface transmit statistics: Disabled
  Link Degrade :
    Link Monitoring                   :  Disable

  Logical interface et-0/0/0.0 (Index 1005) (SNMP ifIndex 533)
    Flags: Device-Down SNMP-Traps Encapsulation: Ethernet-Bridge DF
    Input packets : 83
    Output packets: 0
    Protocol ethernet-switching, MTU: 1518
      Flags: Trunk-Mode
```

The physical link is up and there is no BPDU error.

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 avoid loops. If BPDU protection is enabled on an edge interface, the interface shuts down on encountering ae BPDU thereby preventing any traffic from passing through the interface. You can re-enable the interface by issuing the `clear error bpdu interface` **interface-name** operational mode command. The `clear error bpdu interface` **interface-name** 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.

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

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

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

3. Configure the `et-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 et-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 (`et-0/0/0.0`):

   - Run the `show ethernet-switching interfaces` operational mode command to see the state of STP configured on the interface:

```
user@switch> show ethernet-switching interface et-0/0/0
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down,
                         MMAS - Mac-move action shutdown,  AS - Autostate-exclude enabled,
                         SCTL - shutdown by Storm-control, SL - Secure Learning,
                         MI - MAC+IP limit hit, LP - Loop Protect Down)
Logical Interface flags (DL - disable learning, AD - packet action drop,
                         LH - MAC limit hit, DN - interface down,
                         MMAS - Mac-move action shutdown,  AS - Autostate-exclude enabled,
                         SCTL - shutdown by Storm-control, SL - Secure Learning,
                         MI - MAC+IP limit hit, LP - Loop Protect Down)

Logical         Vlan                  TAG   MAC    MAC+IP STP         Logical
Tagging
interface       members                     limit  limit  state       interface flags
et-0/0/0.0                                  294912 0                  DN
untagged
                default               1     294912 0      Discarding
untagged
```

     In this output, you note that the **et-0/0/0.0** interface is in blocked state because it has received BPDUs from the end device.

   - Run the `show spanning-tree interfaces` operational mode command to ensure that the **et-0/0/0.0** interface is blocked:

```
user@switch> show spanning-tree interface et-0/0/0
Spanning tree interface parameters for instance 0

Interface                 Port ID    Designated         Designated         Port    State
Role
```

```
                                      port ID           bridge ID          Cost
et-0/0/0                   128:58       128:58  32768.605f7e0507de           50    BLK
DIS (Bpdu-Incon)
```

- Run the `show interfaces` **interface-name** operational mode command to verify that the interface is disabled:

```
user@switch> show interfaces et-0/0/0
Physical interface: et-0/0/0, Enabled, Physical link is Down
  Interface index: 1036, SNMP ifIndex: 521
  Link-level type: Ethernet, MTU: 1518, LAN-PHY mode, Speed: 400Gbps, BPDU Error:
Detected, Loop Detect PDU Error: None, Ethernet-Switching Error: None, MAC-REWRITE Error:
None, Loopback: Disabled, Source filtering: Disabled,
  Flow control: Disabled, Auto-negotiation: Disabled, Media type: Fiber
  Device flags   : Present Running Down
  Interface flags: Down SNMP-Traps Internal: 0x20
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 60:5f:7e:05:00:28, Hardware address: 60:5f:7e:05:00:28
  Last flapped   : 2023-01-19 11:46:36 IST (00:02:03 ago)
  Input rate     : 248 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : None
  Active defects : None
  PCS statistics                      Seconds
    Bit errors                             0
    Errored blocks                         0
  PRBS Mode : Disabled
  Interface transmit statistics: Disabled
  Link Degrade :
    Link Monitoring                   :  Disable

  Logical interface et-0/0/0.0 (Index 1005) (SNMP ifIndex 533)
    Flags: Device-Down SNMP-Traps Encapsulation: Ethernet-Bridge DF
    Input packets : 36590
    Output packets: 0
    Protocol ethernet-switching, MTU: 1518
      Flags: Trunk-Mode
```

The physical link is down and BPDU error is detected.

Example: Blocking BPDUs on an Interface for 600 Seconds

The following example, when used with a full bridge configuration with aggregated Ethernet, blocks BPDUs on 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 | 208

Checking the Status of Spanning-Tree Instance Interfaces | 232

Example: Configuring BPDU Protection on Interfaces

IN THIS SECTION

- Requirements | 170
- Overview and Topology | 170
- Configuration | 173

NOTE: This example uses Junos OS for EX Series switches without support for the Enhanced Layer 2 Software (ELS) configuration style. For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

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

IN THIS SECTION

- Topology | **172**

This example explains how to configure BPDU protection on an interface.

Figure 5 on page 172 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, the `shutdown` statement is enabled by default, and 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 there is no spanning-tree protocol configured 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.

Topology

Figure 5: BPDU Protection Topology

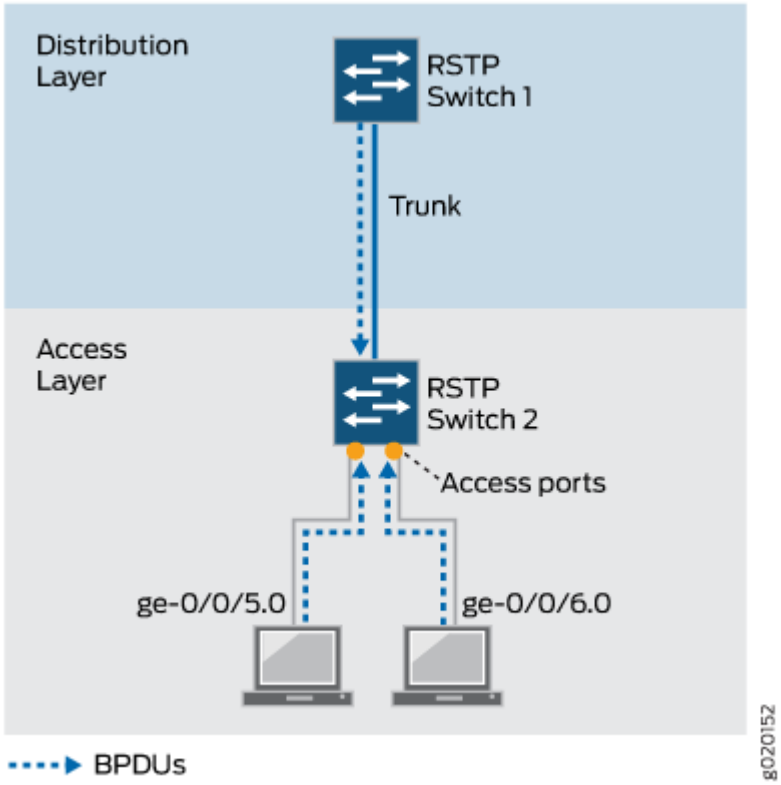


Table 7 on page 172 shows the components that will be configured for BPDU protection.

Table 7: 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

IN THIS SECTION

- Procedure | 173
- Procedure | 174

To configure BPDU protection on the interfaces:

Procedure

CLI Quick Configuration

This is the first scenario that explains configuration for the default BPDU block (action: `shutdown`). To quickly configure BPDU protection on Switch 2, copy the following commands and paste them into the switch terminal window:

```
[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 the `shutdown` statement:

1. Configure the BPDU block (action: `shutdown`) on the downstream interface **ge-0/0/5** on Switch 2:

```
 [edit protocols]
user@switch# set layer2-control bpdu-block interface ge-0/0/5
```

2. Configure the BPDU block (action: `shutdown`) on the downstream interface **ge-0/0/6** on Switch 2:

```
 [edit protocols]
user@switch# set layer2-control bpdu-block interface ge-0/0/6
```

Results

Check the results of the configuration:

```
user@switch> show protocols layer2-control
bpdu-block {
    interface ge-0/0/5;
    interface ge-0/0/6;
}
```

Procedure

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 layer2-control bpdu-block interface ge-0/0/5 drop
user@switch# set protocols layer2-control bpdu-block interface ge-0/0/6 drop
```

NOTE: If xSTP is enabled on the interface, you must disable it before configuring BPDU drop action: block. You can disable RSTP globally by 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. Configure the BPDU `drop` statement on the downstream interface **ge-0/0/5** on Switch 2:

```
 [edit protocols layer2-control]
user@switch# set bpdu-block interface ge-0/0/50 drop
```

2. Configure the BPDU `drop` statement on the downstream interface **ge-0/0/6** on Switch 2:

```
 [edit protocols layer2-control]
user@switch# set bpdu-block interface ge-0/0/6 drop
```

Results

Check the results of the configuration:

```
user@switch> show configuration protocols layer2-control
bpdu-block {
    interface ge-0/0/5;
    interface ge-0/0/6;
}
```

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 | 177
- Eliminating Bridge Loops in Ethernet LANs with Spanning Tree Protocol | 179
- Example: Enabling Loop Protection for Spanning-Tree Protocols | 187
- Configuring Loop Protection for a Spanning-Tree Instance Interface | 187
- Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on non-ELS EX Series Switches | 189
- Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches With ELS | 195

Understanding Loop Protection for Spanning-Tree Instance Interfaces

IN THIS SECTION

- How Does Loop Protection Work? | 178
- Benefits of Loop Protection on STP Protocols | 178
- What Action Causes a Loop? | 178
- What Can Loop Protection Do When BPDUs Don't Arrive? | 178
- When Should I Use Loop Protection? | 179
- What Happens if I Do Not Use Loop Protection? | 179

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

Understanding Bridge Loops | 180

How STP Helps Eliminate Loops | **183**

Types of Spanning-Tree Protocols Supported | **186**

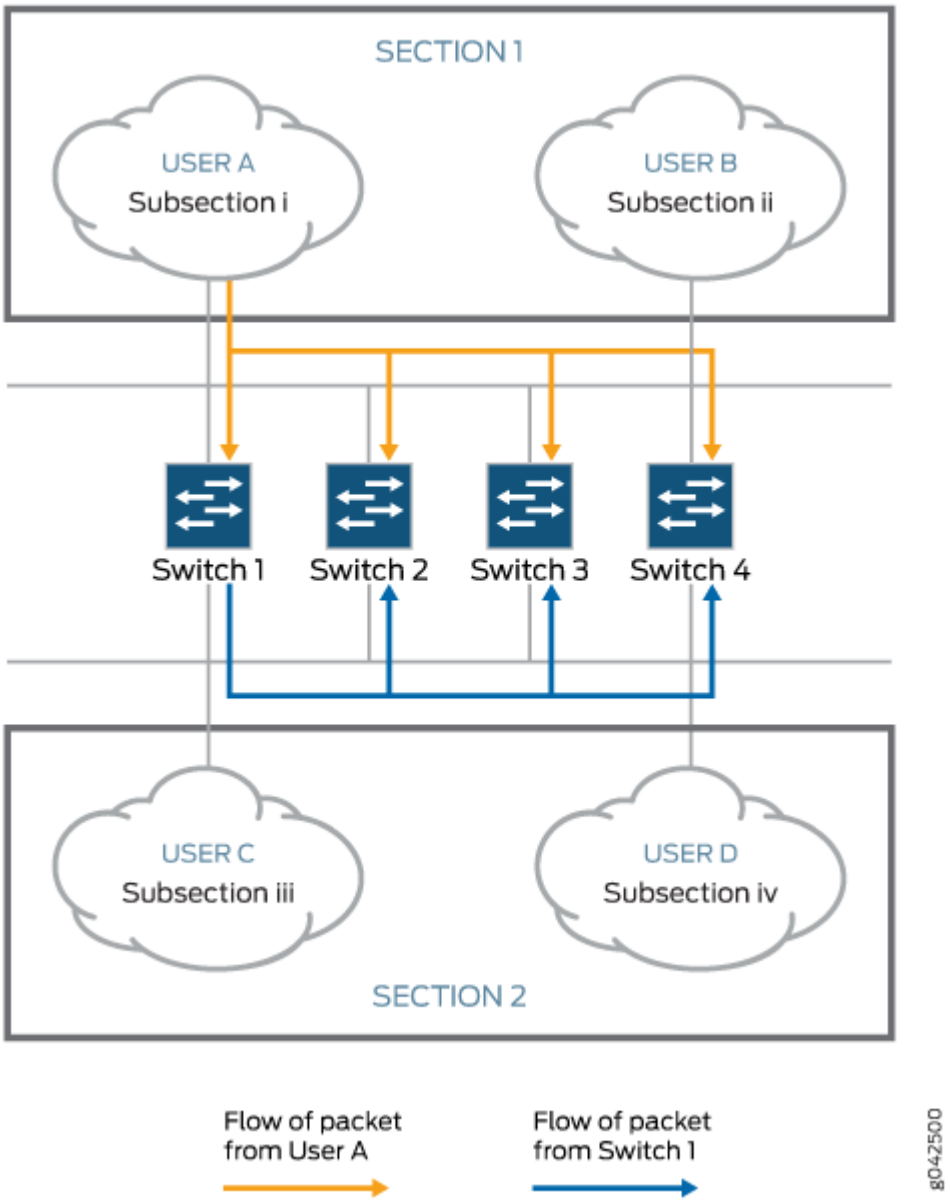
The Spanning Tree Protocol (STP) is a network protocol that is used to eliminate bridge loops in Ethernet LANs. STP prevents network loops and associated network outage by blocking redundant links or paths. The redundant paths can be used to keep the network operational if the primary link fails.

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 6 on page 181). 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 6: 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 8: 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 9: 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 6 on page 181, 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 10: 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.

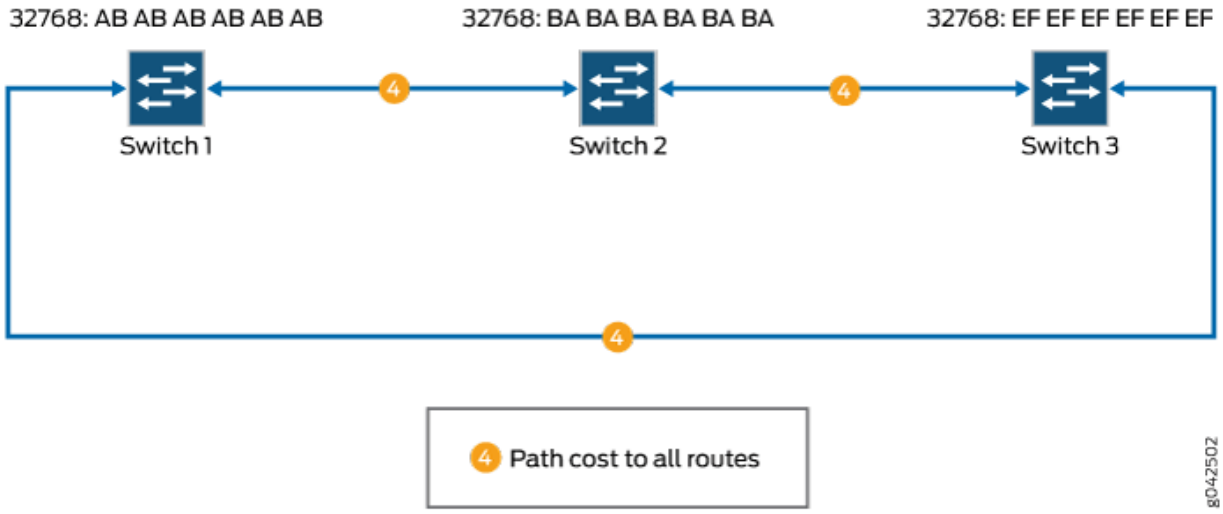
How STP Helps Eliminate Loops

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 7 on page 184). 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 7: Simple Network with Redundant Links

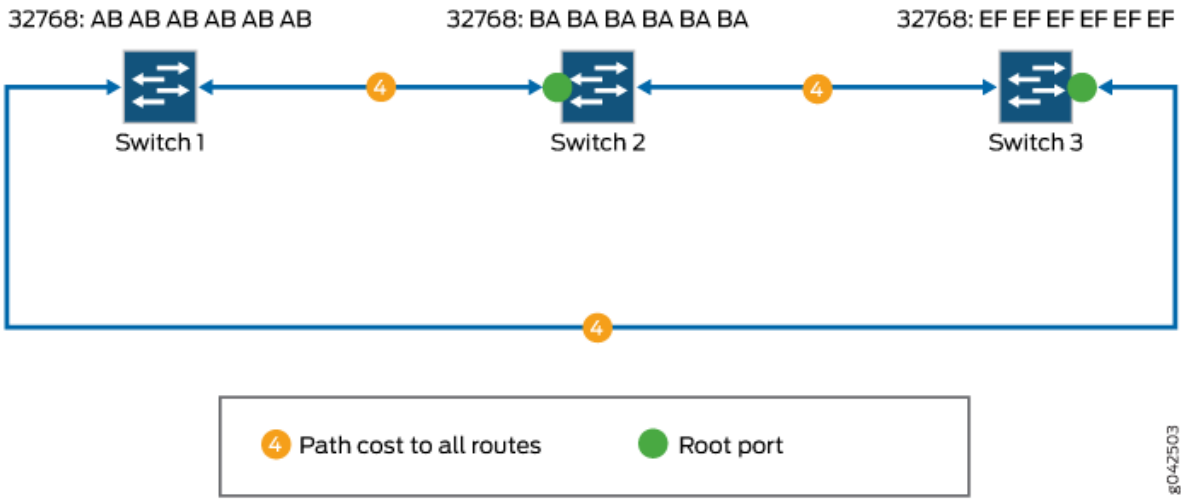


To eliminate network loops, STP performs the following steps in this sample network:

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.

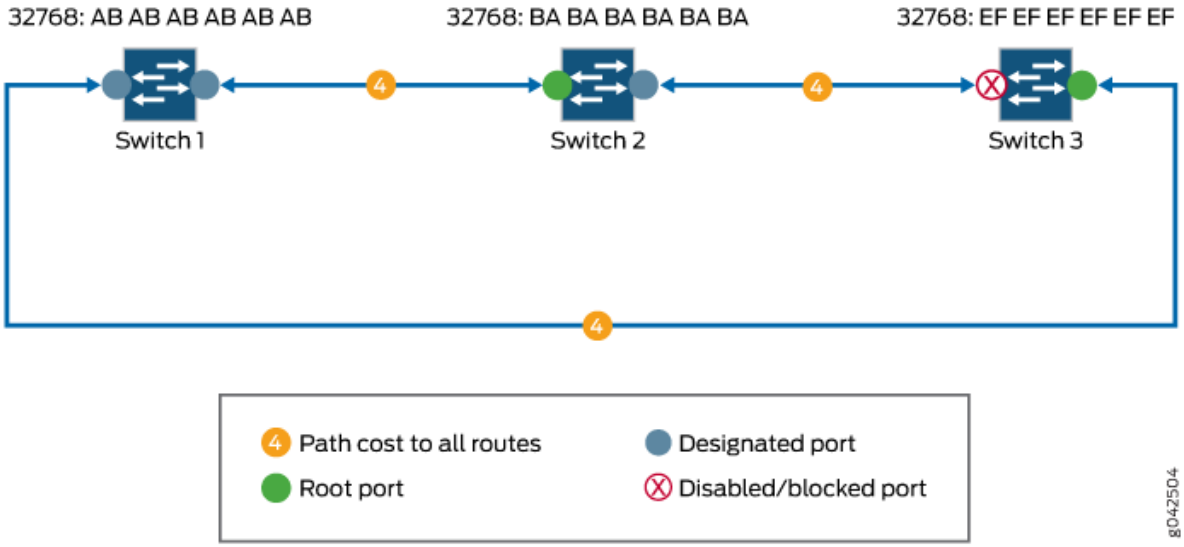
2. *Elects the root ports.* Typically, root ports use the least-cost paths from one switch to the other. In this example, assume that all paths have similar costs. Therefore, the root port for Switch 2 is the port that receives packets through the direct path from Switch 1 (cost 4), because the other path is through Switch 3 (cost 4 + 4) as shown in Figure 8 on page 185. Similarly, for Switch 3, the root port is the one that uses the direct path from Switch 1.

Figure 8: 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 9 on page 185, the designated ports are marked.

Figure 9: 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

- Requirements | 189
- Overview and Topology | 190
- Configuration | 192
- Verification | 193

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

IN THIS SECTION

- Topology | 191

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 10 on page 191. 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.

Topology

Figure 10: Network Topology for Loop Protection

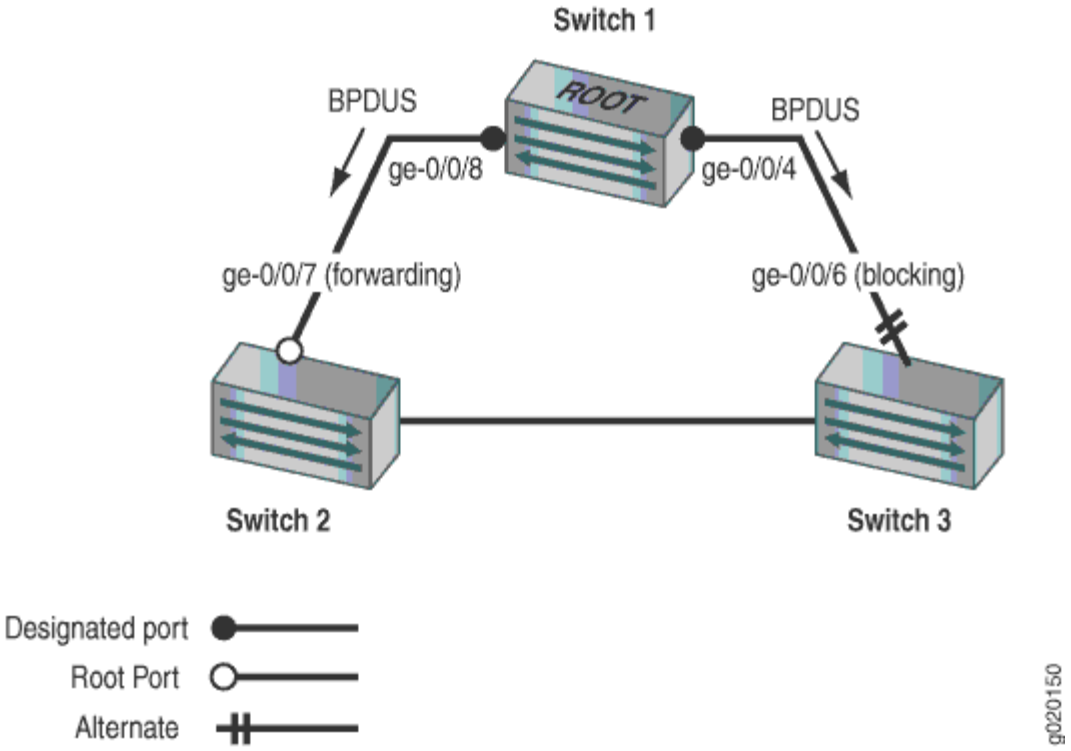


Table 11 on page 191 shows the components that will be configured for loop protection.

Table 11: 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

IN THIS SECTION

- Procedure | 192

To configure loop protection on an interface:

Procedure

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

- Displaying the Interface State Before Loop Protection Is Triggered | **193**
- Verifying That Loop Protection Is Working on an Interface | **194**

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

- Requirements | **196**
- Overview and Topology | **196**
- Configuration | **198**
- Verification | **199**

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 177. 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

IN THIS SECTION

- Topology | **197**

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 11 on page 197. 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.

Topology

Figure 11: Network Topology for Loop Protection

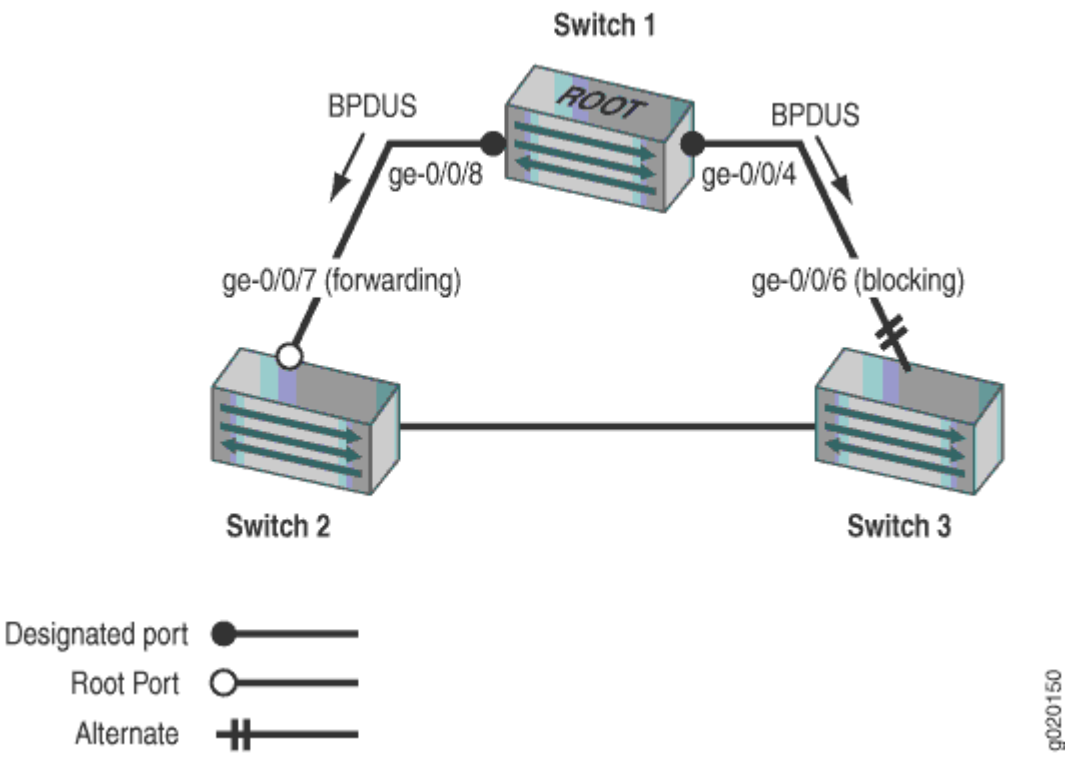


Table 12 on page 197 shows the components that will be configured for loop protection.

Table 12: 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**.

Table 12: Components of the Topology for Configuring Loop Protection on EX Series Switches *(Continued)*

Property	Settings
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

IN THIS SECTION

- Procedure | 198

To configure loop protection on an interface:

Procedure

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

- Displaying the Interface State Before Loop Protection Is Triggered | **199**
- Verifying That Loop Protection Is Working on an Interface | **200**

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 Devices with RSTP | 32

CHAPTER 6

Root Protection for VPLS Multihome Environments

Root Protection for VPLS Multihome Environments

IN THIS SECTION

- Understanding VPLS Multihoming | 203
- Understanding Bridge Priority for Election of Root Bridge and Designated Bridge | 208
- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network | 208
- Example: Configuring VPLS Root Topology Change Actions | 210
- Enabling Root Protection for a Spanning-Tree Instance Interface | 210
- Configuring VPLS Root Protection Topology Change Actions to Control Individual VLAN Spanning-Tree Behavior | 211
- Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches | 213
- Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on EX Series Switches With ELS | 220

Understanding VPLS Multihoming

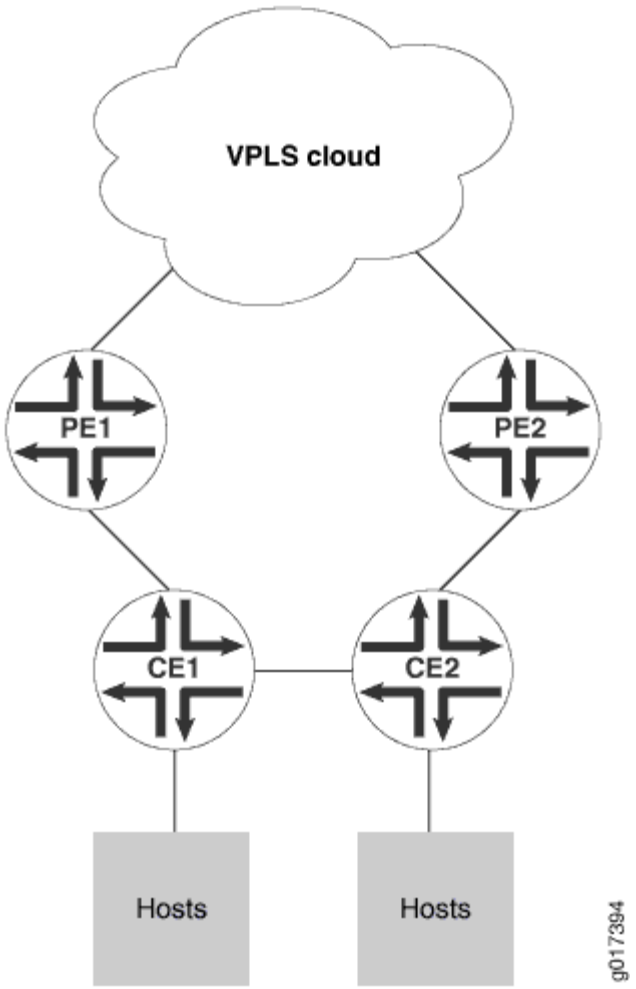
IN THIS SECTION

- Benefits of Multihoming | 204
- How Does Multihoming Work? | 205
- VPLS Multihoming Hold Time Before Switching to Primary Priority | 205
- VPLS Multihoming Bridge Flush of MAC Cache on Topology Change | 206
- VPLS Multihoming System Identifiers for Bridges in the Ring | 207
- VPLS Multihoming Priority of the Backup Bridge | 207

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 12 on page 204 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 12: 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 12 on page 204, 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

- Benefits of Spanning Tree Protocol Root Protection | **209**
- How Root Protection Works | **209**
- Where Should I Enable Root Protection? | **209**

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

- Requirements | 213
- Overview and Topology | 213
- Configuration | 216
- Verification | 217

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

IN THIS SECTION

- Topology | 216

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 13 on page 215. 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 13: Network Topology for Root Protection

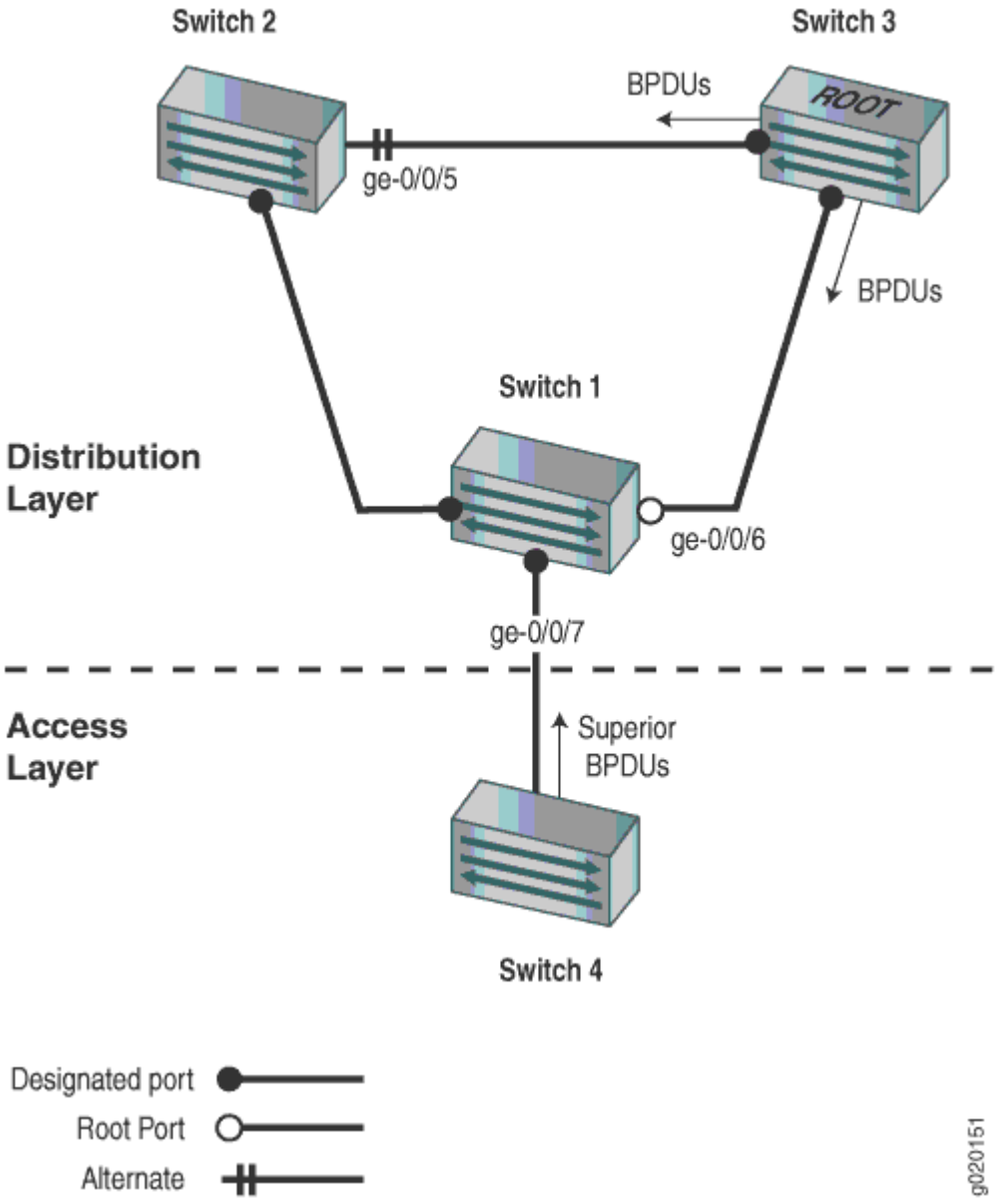


Table 13 on page 215 shows the components that will be configured for root protection.

Table 13: 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**.

Table 13: Components of the Topology for Configuring Root Protection on EX Series Switches *(Continued)*

Property	Settings
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.

Topology

Configuration

IN THIS SECTION

- Procedure | 217

To configure root protection on an interface:

Procedure

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

- Displaying the Interface State Before Root Protection Is Triggered | **218**
- Verifying That Root Protection Is Working on the Interface | **219**

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

- Requirements | 220
- Overview and Topology | 221
- Configuration | 223
- Verification | 224

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

IN THIS SECTION

- Topology | 223

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 14 on page 222. 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 14: Network Topology for Root Protection

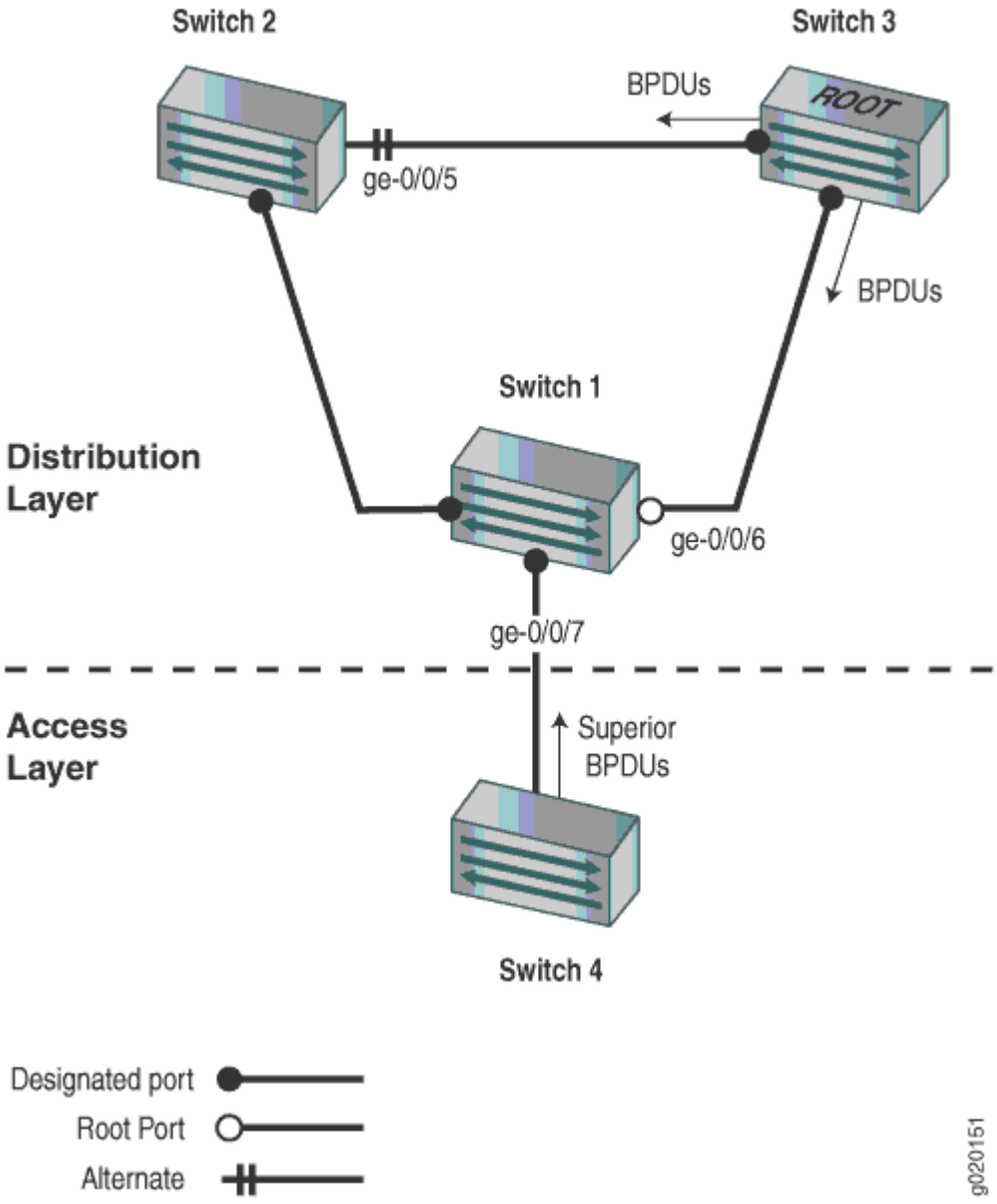


Table 14 on page 222 shows the components that will be configured for root protection.

Table 14: 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`.

Table 14: Components of the Topology for Configuring Root Protection on EX Series Switches *(Continued)*

Property	Settings
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.

Topology

Configuration

IN THIS SECTION

- Procedure | 224

To configure root protection on an interface:

Procedure

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

- Displaying the Interface State Before Root Protection Is Triggered | 225
- Verifying That Root Protection Is Working on the Interface | 226

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.

CHAPTER 7

Monitoring and Troubleshooting

Monitoring and Troubleshooting Spanning Tree Protocols | 229

Monitoring and Troubleshooting Spanning Tree Protocols

IN THIS SECTION

- Monitoring Spanning Tree Protocols on Switches | 229
- Checking the Status of Spanning-Tree Instance Interfaces | 232
- Understanding Spanning-Tree Protocol Trace Options | 233
- Configuring Tracing Spanning-Tree Operations | 233
- Example: Tracing Spanning-Tree Protocol Operations | 236
- Unblocking a Switch Interface That Receives BPDUs in Error (CLI Procedure) | 236
- Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error (CLI Procedure) | 237
- Clearing the Blocked Status of a Spanning-Tree Instance Interface | 238
- Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface | 238
- Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface | 239
- Clearing a MAC Rewrite Error on an Interface with Layer 2 Protocol Tunneling | 239
- Understanding Forward Delay Before Ports Transition to Forwarding State | 240

Monitoring Spanning Tree Protocols on Switches

IN THIS SECTION

- Purpose | 230
- Action | 230
- Meaning | 230

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 15 on page 230 summarizes the spanning-tree protocol parameters.

Table 15: Summary of Spanning Tree Protocols Output Fields

Field	Values
Bridge Parameters	
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.

Table 15: Summary of Spanning Tree Protocols Output Fields *(Continued)*

Field	Values
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.
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.

Table 15: Summary of Spanning Tree Protocols Output Fields *(Continued)*

Field	Values
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 for Routing Devices.

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 237. 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 237 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 and Operational Commands

Junos CLI Reference Overview | 242

Junos CLI Reference Overview

We've consolidated all Junos CLI commands and configuration statements in one place. Learn about the syntax and options that make up the statements and commands and understand the contexts in which you'll use these CLI elements in your network configurations and operations.

- Junos CLI Reference

Click the links to access Junos OS and Junos OS Evolved configuration statement and command summary topics.

- Configuration Statements
- Operational Commands