



Junos[®] OS

Spanning-Tree Protocols Feature Guide



Modified: 2018-03-07

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. and/or its affiliates in the United States and other countries. All other trademarks may be 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.

Junos® OS Spanning-Tree Protocols Feature Guide
Copyright © 2018 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://www.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 the Documentation	xiii
	Documentation and Release Notes	xiii
	Supported Platforms	xiii
	Using the Examples in This Manual	xiv
	Merging a Full Example	xiv
	Merging a Snippet	xv
	Documentation Conventions	xv
	Documentation Feedback	xvii
	Requesting Technical Support	xviii
	Self-Help Online Tools and Resources	xviii
	Opening a Case with JTAC	xviii
Chapter 1	Understanding Spanning-Tree Protocols	21
	Understanding RSTP	21
	Spanning Tree Protocols Help Prevent Broadcast Storms	21
	RSTP is an Enhancement of the Original STP	22
	Port Roles Determine Participation in the Spanning Tree	22
	Port States Determine How a Port Processes a Frame	23
	Edge Ports Connect to Devices That Cannot Be Part of a Spanning Tree	23
	BPDUs Maintain the Spanning-Tree	23
	When an RSTP Root Bridge Fails	24
	Devices Must Relearn MAC Addresses After a Link Failure	24
	Selecting a Spanning Tree Protocol	24
	Understanding STP	26
	Selecting a Spanning-Tree Protocol	28
	Understanding VSTP	29
	Selecting a Spanning-Tree Protocol	30
	Understanding Spanning-Tree Protocol Trace Options	31
	Understanding Provider Bridge Participation in RSTP or MSTP Instances	31
Chapter 2	Configuring Spanning-Tree Protocols	33
	Understanding Spanning-Tree Instance Interface	33
	Understanding Spanning-Tree Instance Interface Priority	34
	Understanding Spanning-Tree Instance Interface Cost	34
	Understanding Spanning-Tree Instance Interface Point-to-Point Link Mode	35
	Understanding BDPDU Protection for Spanning-Tree Instance Interfaces	35
	Understanding Forward Delay Before Ports Transition to Forwarding State	36
	Configuring Spanning Tree Protocols on EX Series Switches (J-Web Procedure)	36
	Configuring a Virtual Switch Routing Instance on MX Series Routers	41

	Configuring a Spanning-Tree Instance Interface as an Edge Port for Faster Convergence	42
Chapter 3	Configuring STP	45
	Understanding System Identifier for Bridges in STP or RSTP Instances	45
	Configuring STP on EX Series Switches (CLI Procedure)	45
Chapter 4	Configuring MSTP	47
	Understanding MSTP	48
	MSTP Maps Multiple VLANs	48
	Configuring MSTP Regions	49
	Selecting a Spanning Tree Protocol	49
	Configuring MSTP on Switches	51
	Configuring Multiple Spanning Tree Protocol	54
	Configuring MSTP Instances on a Physical Interface	58
	Disabling MSTP	59
Chapter 5	Configuring RSTP	61
	Understanding System Identifier for Bridges in STP or RSTP Instances	61
	Configuring Rapid Spanning Tree Protocol	62
	Configuring RSTP on EX Series Switches (CLI Procedure)	65
	Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP	66
	Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches	84
	Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP	103
	Reverting to RSTP or VSTP from Forced IEEE 802.1D STP	103
	Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure)	104
Chapter 6	Configuring VSTP	105
	Configuring VLAN SpanningTree Protocol	106
	Configuring VLAN Spanning Tree Protocol on Switches	111
	Configuring VSTP on EX Series Switches (CLI Procedure)	113
	Understanding VSTP on a Trunk Port with Tagged Traffic Overview	115
	Example: Configuring VSTP on a Trunk Port with Tagged Traffic	115
	Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP	127
	Reverting to RSTP or VSTP from Forced IEEE 802.1D STP	127
	Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP	128
	Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure)	129
Chapter 7	Configuring BPDU Protection for Spanning-Tree Protocols	131
	Understanding BPDU Protection for Spanning-Tree Instance Interfaces	132
	Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches	133
	Different Kinds of BPDUs	133
	Protecting Switches from Incompatible BPDUs	133
	Understanding BPDU Protection for Individual Spanning-Tree Instance Interfaces	134
	Understanding BPDUs Used for Exchanging Information Among Bridges	135
	Understanding Maximum Age for Awaiting Arrival of Hello BPDUs	136
	Understanding Hello Time for Root Bridge to Transmit Hello BPDUs	136

	Understanding BPDU Protection on All Edge Ports of the Bridge	136
	Configuring BPDU Protection for Spanning-Tree Instance Interfaces	137
	Configuring BPDU Protection on Switch Spanning Tree Interfaces	139
	Configuring BPDU Protection on an EX Series Interface (CLI Procedure)	140
	Configuring BPDU protection For Edge Interfaces	140
	Configuring BPDU Protection for Interfaces (Port Shutdown Mode)	141
	Configuring BPDU Protection for Interfaces (BPDU Drop Mode)	143
	Configuring BPDU Protection on All Edge Ports	145
	Unblocking a Switch Interface That Receives BPDUs in Error (CLI Procedure) . .	146
	Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error (CLI Procedure)	147
	Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations	147
	Example: Configuring BPDU Protection on Switch Edge Interfaces to Prevent STP Miscalculations	152
	Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches	157
	Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches	161
	Example: Blocking BPDUs on Aggregated Ethernet Interface for 600 Seconds	167
	Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches	167
Chapter 8	Configuring Loop Protection for Spanning-Tree Protocols	175
	Understanding Loop Protection for Spanning-Tree Instance Interfaces	175
	Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches	176
	Understanding Spanning Tree Protocol Used for Eliminating Bridge Loops in Ethernet LANs	177
	Understanding Bridge Loops	178
	How STP Helps Eliminate Loops	179
	Types of Spanning-Tree Protocols Supported	181
	Example: Enabling Loop Protection for Spanning-Tree Protocols	183
	Configuring Loop Protection for a Spanning-Tree Instance Interface	183
	Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on non-ELS EX Series Switches	184
	Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches . .	189
Chapter 9	Configuring Network Regions for VLANs	195
	Example: Configuring Network Regions for VLANs with MSTP on Switches . . .	195
	Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches	217
Chapter 10	Configuring Root Protection in a VPLS Multihoming Environment	239
	Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure	240
	Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology	241

	Understanding Bridge Priority for Election of Root Bridge and Designated Bridge	242
	Understanding VPLS Multihoming: Priority of the Backup Bridge	243
	Understanding VPLS Multihoming: Hold Time Before Switching to Primary Priority	243
	Understanding VPLS Multihoming: System Identifier for Bridges in the Ring	244
	Understanding VPLS Multihoming: Bridge Flush of MAC Cache on Topology Change	245
	Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches	246
	Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network	247
	Example: Configuring VPLS Root Topology Change Actions	247
	Enabling Root Protection for a Spanning-Tree Instance Interface	248
	Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior	249
	Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior	250
	Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches	251
	Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on EX Series Switches	256
Chapter 11	Configuring Layer 2 Protocol Tunneling	263
	Understanding Layer 2 Protocol Tunneling Through a Network	263
	Understanding Layer 2 Protocol Tunneling Configuration Guidelines	265
	Configuring Layer 2 Protocol Tunneling	266
Chapter 12	Monitoring Layer 2 Spanning-Tree Protocol	269
	Monitoring Spanning Tree Protocols on Switches	269
	Checking the Status of Spanning-Tree Instance Interfaces	272
	Clearing the Blocked Status of a Spanning-Tree Instance Interface	272
	Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface	273
	Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface	273
	Configuring Tracing Spanning-Tree Operations	274
	Example: Tracing Spanning-Tree Protocol Operations	276
Chapter 13	Configuration Statements for Spanning-Tree Protocols	277
	access-trunk	278
	arp-on-stp	279
	backup-bridge-priority	280
	block (Spanning Trees)	281
	bpdu-destination-mac-address (Spanning Tree)	282
	bpdu-block	283
	bpdu-block-on-edge	284
	bpdu-timeout-action	286
	bridge-priority	288
	configuration-name	290

cost	291
disable	293
disable-timeout	295
drop (BPDU Block)	296
edge	297
enable-all-ifl	298
extended-system-id	299
force-version (IEEE 802.1D STP)	300
forward-delay	301
hello-time	303
interface (BPDU Blocking)	305
interface (Spanning Tree)	307
layer2-control	309
log (Spanning Trees)	310
mac-rewrite	311
max-age	313
max-hops	315
mode	316
msti	318
mstp	320
no-root-port	324
priority (Protocols STP)	326
priority-hold-time	327
protocol	328
protocols (STP Type)	330
revision-level	331
rstp	332
shutdown (BPDU Block)	335
stp	336
system-id	338
traceoptions (Spanning Tree)	339
vlan (MSTP)	343
vlan (VSTP)	345
vlan-group	347
vpls-flush-on-topology-change	348
vstp	349
Chapter 14	
Operational Mode Commands for Spanning-Tree Configuration	355
clear bpdu-error	356
clear error bpdu interface	357
clear error mac-rewrite	358
clear spanning-tree protocol-migration	359
clear spanning-tree statistics	360
clear spanning-tree statistics bridge	362
clear spanning-tree stp-buffer	363
show bridge mac-table	364
show mac-rewrite interface	370
show spanning-tree bridge	372
show spanning-tree interface	377

show spanning-tree mstp configuration	386
show spanning-tree statistics	389
show spanning-tree statistics bridge	391
show spanning-tree statistics interface	392
show spanning-tree statistics message-queues	393
show spanning-tree stp-buffer see-all	394

List of Figures

Chapter 5	Configuring RSTP	61
	Figure 1: Network Topology for RSTP	67
	Figure 2: Network Topology for RSTP	86
Chapter 6	Configuring VSTP	105
	Figure 3: Topology for VSTP Configured on a Trunk Port with Tagged Traffic . . .	116
Chapter 7	Configuring BPDU Protection for Spanning-Tree Protocols	131
	Figure 4: BPDU Protection Topology	149
	Figure 5: BPDU Protection Topology	153
	Figure 6: BPDU Protection Topology	158
	Figure 7: BPDU Protection Topology	163
	Figure 8: BPDU Protection Topology	169
Chapter 8	Configuring Loop Protection for Spanning-Tree Protocols	175
	Figure 9: Formation of Bridge Loops	178
	Figure 10: Simple Network with Redundant Links	180
	Figure 11: Electing Root Ports	181
	Figure 12: Selecting Designated Ports and Blocking Redundant Paths	181
	Figure 13: Network Topology for Loop Protection	186
	Figure 14: Network Topology for Loop Protection	191
Chapter 9	Configuring Network Regions for VLANs	195
	Figure 15: Network Topology for MSTP	197
	Figure 16: Network Topology for MSTP	218
Chapter 10	Configuring Root Protection in a VPLS Multihoming Environment	239
	Figure 17: VPLS Multihoming Configuration	241
	Figure 18: Network Topology for Root Protection	253
	Figure 19: Network Topology for Root Protection	258

List of Tables

	About the Documentation	xiii
	Table 1: Notice Icons	xvi
	Table 2: Text and Syntax Conventions	xvi
Chapter 1	Understanding Spanning-Tree Protocols	21
	Table 3: Selecting a Spanning Tree Protocol	25
	Table 4: Selecting a Spanning-Tree Protocol	28
	Table 5: Selecting a Spanning-Tree Protocol	30
Chapter 2	Configuring Spanning-Tree Protocols	33
	Table 6: Spanning-Tree Protocol Configuration Parameters	37
Chapter 4	Configuring MSTP	47
	Table 7: Selecting a Spanning Tree Protocol	49
Chapter 5	Configuring RSTP	61
	Table 8: Components of the Topology for Configuring RSTP	67
	Table 9: Components of the Topology for Configuring RSTP	86
Chapter 7	Configuring BPDU Protection for Spanning-Tree Protocols	131
	Table 10: Components of the Topology for Configuring BPDU Protection on MX Series Routers	149
	Table 11: Components of the Topology for Configuring BPDU Protection on EX Series Switches	154
	Table 12: Components of the Topology for Configuring BPDU Protection on EX Series Switches	158
	Table 13: Components of the Topology for Configuring BPDU Protection on EX Series Switches	163
	Table 14: Components of the Topology for Configuring BPDU Protection on EX Series Switches	170
Chapter 8	Configuring Loop Protection for Spanning-Tree Protocols	175
	Table 15: Components of the Topology for Configuring Loop Protection on EX Series Switches	186
	Table 16: Components of the Topology for Configuring Loop Protection on EX Series Switches	191
Chapter 9	Configuring Network Regions for VLANs	195
	Table 17: Components of the Topology for Configuring MSTP on EX Series Switches	197
	Table 18: Components of the Topology for Configuring MSTP on EX Series Switches	218
Chapter 10	Configuring Root Protection in a VPLS Multihoming Environment	239

	Table 19: Components of the Topology for Configuring Root Protection on EX Series Switches	253
	Table 20: Components of the Topology for Configuring Root Protection on EX Series Switches	258
Chapter 11	Configuring Layer 2 Protocol Tunneling	263
	Table 21: MAC Rewrite and VPLS Configurations	264
	Table 22: DPCs Supported for Layer 2 Protocol Tunneling	264
Chapter 12	Monitoring Layer 2 Spanning-Tree Protocol	269
	Table 23: Summary of Spanning Tree Protocols Output Fields	270
Chapter 14	Operational Mode Commands for Spanning-Tree Configuration	355
	Table 24: show bridge mac-table Output Fields	365
	Table 25: show mac-rewrite interface Output Fields	370
	Table 26: show spanning-tree bridge Output Fields	373
	Table 27: show spanning-tree Interface Output Fields	378
	Table 28: show spanning-tree mstp configuration Output Fields	387
	Table 29: show spanning-tree statistics Output Fields	389
	Table 30: show spanning-tree statistics bridge Output Fields	391
	Table 31: show spanning-tree statistics interface Output Fields	392
	Table 32: show spanning-tree statistics message-queues Output Fields	393
	Table 33: show spanning-tree stp-buffer see-all Output Fields	394

About the Documentation

- [Documentation and Release Notes on page xiii](#)
- [Supported Platforms on page xiii](#)
- [Using the Examples in This Manual on page xiv](#)
- [Documentation Conventions on page xv](#)
- [Documentation Feedback on page xvii](#)
- [Requesting Technical Support on page xviii](#)

Documentation and Release Notes

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

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

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

Supported Platforms

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

- [MX Series](#)
- [EX Series](#)
- [QFX Series](#)
- [SRX Series](#)
- [T Series](#)
- [M Series](#)
- [ACX Series](#)
- [NFX Series](#)
- [TI600](#)

- [T640](#)
- [SRX3400](#)
- [M Series](#)
- [SRX210](#)

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

```
[edit]
```

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

For more information about the **load** command, see [CLI Explorer](#).

Documentation Conventions

[Table 1](#) on page [xvi](#) defines notice icons used in this guide.

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

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

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

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

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <https://www.juniper.net/documentation/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/documentation/feedback/>.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

CHAPTER 1

Understanding Spanning-Tree Protocols

- [Understanding RSTP on page 21](#)
- [Understanding STP on page 26](#)
- [Understanding VSTP on page 29](#)
- [Understanding Spanning-Tree Protocol Trace Options on page 31](#)
- [Understanding Provider Bridge Participation in RSTP or MSTP Instances on page 31](#)

Understanding RSTP

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. Rapid Spanning Tree Protocol (RSTP) is the default spanning-tree protocol for preventing loops on Ethernet networks.

This topic describes:

- [Spanning Tree Protocols Help Prevent Broadcast Storms on page 21](#)
- [RSTP is an Enhancement of the Original STP on page 22](#)
- [Port Roles Determine Participation in the Spanning Tree on page 22](#)
- [Port States Determine How a Port Processes a Frame on page 23](#)
- [Edge Ports Connect to Devices That Cannot Be Part of a Spanning Tree on page 23](#)
- [BPDUs Maintain the Spanning-Tree on page 23](#)
- [When an RSTP Root Bridge Fails on page 24](#)
- [Devices Must Relearn MAC Addresses After a Link Failure on page 24](#)
- [Selecting a Spanning Tree Protocol on page 24](#)

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*.

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). Rapid Spanning Tree Protocol (RSTP), originally defined in IEEE 802.1w and later merged into IEEE 802.1D, facilitates faster spanning-tree convergence after a topology change. This topic explains the spanning-tree default RSTP.



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**.

RSTP is an Enhancement of the Original STP

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 configuration on EX Series switches. In addition, note that EX Series switches configured to use STP actually run RSTP force version 0, which is compatible with STP.

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

RSTP 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 an RSTP 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 an RSTP 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 build 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.

Selecting a Spanning Tree Protocol

The default factory configuration for EX Series switches is RSTP, a faster version of the original STP. To determine which spanning-tree protocol is best for your situation, see [Table 3 on page 25](#) below.

Table 3: Selecting a Spanning Tree Protocol

Protocol	Advantages	Disadvantages
RSTP	<ul style="list-style-type: none"> Rapid Spanning Tree Protocol is the default 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 	<ul style="list-style-type: none"> RSTP does not work with 802.1D 1998 bridges. RSTP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning tree. This limits the number of forwarding paths for data traffic.
STP	<ul style="list-style-type: none"> Spanning Tree Protocol works with 802.1D 1998 bridges. RSTP is backward compatible with STP; therefore, switches do not all have to run STP. 	<ul style="list-style-type: none"> 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.
MSTP	<ul style="list-style-type: none"> Multiple Spanning Tree Protocol works with most VLANs. RSTP and STP are recognized as distinct spanning-tree regions by MSTP. 	<ul style="list-style-type: none"> Some protocols require compatibility that is not provided by MSTP. In this case, use VSTP. MSTP supports a limited number of ports. MSTP uses more CPU than RSTP and does not converge as fast as RSTP.
VSTP	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. As a workaround, reduce the number of VSTP instances to fewer than 190.

- Related Documentation**
- [Understanding STP on page 26](#)
 - [Understanding MSTP on page 48](#)
 - [Understanding VSTP on page 29](#)
 - [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
 - [Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66](#)
 - [Configuring RSTP on EX Series Switches \(CLI Procedure\) on page 65](#)

Understanding STP

Ethernet networks are susceptible to broadcast storms if loops are introduced. However, an Ethernet network should always 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 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.

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). Configure STP when you need to support older 802.1D 1998 bridges.



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

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

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.



NOTE: 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.



NOTE: EX Series switches configured to use STP actually run RSTP force version 0, which is compatible with STP. For an explanation of RSTP, see [“Understanding RSTP” on page 21](#). 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](#).

This topic describes:

- [Selecting a Spanning-Tree Protocol on page 28](#)

Selecting a Spanning-Tree Protocol

The default factory configuration for devices is RSTP, a faster version of STP. To determine which spanning-tree protocol is best for your situation, see [Table 4 on page 28](#) below.

Table 4: Selecting a Spanning-Tree Protocol

Protocol	Advantages	Disadvantages
RSTP	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • RSTP does not work with 802.1D 1998 bridges. • RSTP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic.
STP	<ul style="list-style-type: none"> • Spanning Tree Protocol works with 802.1D 1998 bridges. • RSTP is backward compatible with STP; therefore, switches do not all have to run STP. 	<ul style="list-style-type: none"> • 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. • Edge ports are not supported when the original IEEE 802.1D STP is configured. <p>NOTE: If you specify edge at the [edit protocols stp] hierarchy level, the software ignores the option.</p>
MSTP	<ul style="list-style-type: none"> • Multiple Spanning Tree Protocol works with most VLANs. • RSTP and STP are recognized as distinct spanning-tree regions by MSTP. 	<ul style="list-style-type: none"> • Some protocols require compatibility that is not provided by MSTP. In this case, use VSTP. • MSTP supports a limited number of ports. • MSTP uses more CPU than RSTP and does not converge as fast as RSTP.
VSTP	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • With VSTP, there can be only one 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. As a workaround, reduce the number of VSTP instances to fewer than 190.

Related Documentation

- [Configuring STP on EX Series Switches \(CLI Procedure\) on page 45](#)
- [Understanding RSTP on page 21](#)
- [Understanding MSTP on page 48](#)

- [Understanding VSTP on page 29](#)
- [Understanding Layer 2 Protocol Tunneling on EX Series Switches](#)

Understanding VSTP

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 is RSTP. If you use VLANs, however, we recommend that you enable MSTP unless your network requires the device compatibility provided by VSTP. Switches configured to run VSTP automatically assign each VLAN to one spanning-tree instance that runs RSTP. While this approach is useful to optimize network usage in small networks with a limited number of VLANs, a VSTP configuration in a network with several hundred VLANs can overload switch CPUs. MSTP ensures that your network is not slowed down by the increased network traffic caused by hundreds of VLANs, each with its own spanning-tree instance.

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.

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



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



NOTE: When you configure VSTP with the `set protocol vstp vlan all` command, VLAN ID 1 is not set; it is excluded so that the configuration is compatible with Cisco PVST+. If you want VLAN ID 1 to be included in the VSTP configuration on your switch, you must set it separately with the `set protocol vstp vlan 1` command.



NOTE: The `vlan all` option is supported on all devices.



NOTE: 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.

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 30](#).

Table 5: Selecting a Spanning-Tree Protocol

Protocol	Advantages	Disadvantages
RSTP	<ul style="list-style-type: none"> 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 so switches do not all have to run RSTP. RSTP supports more ports than MSTP or VSTP. 	<ul style="list-style-type: none"> RSTP does not work with 802.1D 1998 bridges. RSTP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning tree. This limits the number of forwarding paths for data traffic.
STP	<ul style="list-style-type: none"> Spanning Tree Protocol works with 802.1D 1998 bridges. RSTP is backward compatible with STP so switches do not all have to run STP. 	<ul style="list-style-type: none"> 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.
MSTP	<ul style="list-style-type: none"> Multiple Spanning Tree Protocol works with most VLANs. RSTP and STP are recognized as distinct Spanning Tree regions by MSTP. 	<ul style="list-style-type: none"> Some protocols require compatibility that is not provided by MSTP. In this case, use VSTP. MSTP supports a limited number of ports. MSTP uses more CPU than RSTP and does not converge as fast as RSTP.
VSTP	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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.

Related Documentation

- [Understanding STP on page 26](#)
- [Understanding RSTP on page 21](#)
- [Understanding MSTP on page 48](#)
- [Configuring VLAN Spanning-Tree Protocol](#)
- [Configuring VLAN Spanning Tree Protocol on Switches on page 111](#)

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*.

Related Documentation

- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [Configuring VLAN SpanningTree Protocol on page 106](#)
- [Example: Tracing Spanning-Tree Protocol Operations on page 276](#)
- [traceoptions \(Spanning Tree\) on page 339](#)

Understanding Provider Bridge Participation in RSTP or MSTP Instances

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

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

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

Related Documentation

- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [bpdu-destination-mac-address on page 282](#)

CHAPTER 2

Configuring Spanning-Tree Protocols

- [Understanding Spanning-Tree Instance Interface on page 33](#)
- [Understanding Spanning-Tree Instance Interface Priority on page 34](#)
- [Understanding Spanning-Tree Instance Interface Cost on page 34](#)
- [Understanding Spanning-Tree Instance Interface Point-to-Point Link Mode on page 35](#)
- [Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35](#)
- [Understanding Forward Delay Before Ports Transition to Forwarding State on page 36](#)
- [Configuring Spanning Tree Protocols on EX Series Switches \(J-Web Procedure\) on page 36](#)
- [Configuring a Virtual Switch Routing Instance on MX Series Routers on page 41](#)
- [Configuring a Spanning-Tree Instance Interface as an Edge Port for Faster Convergence on page 42](#)

Understanding Spanning-Tree Instance Interface

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

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

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

Related Documentation

- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [Configuring VLAN SpanningTree Protocol on page 106](#)
- [cost on page 291](#)
- [edge on page 297](#)
- [interface \(Spanning Tree\) on page 307](#)
- [mode on page 316](#)

- [priority on page 326](#)

Understanding Spanning-Tree Instance Interface Priority

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

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

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

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

Related Documentation

- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [Configuring VLAN SpanningTree Protocol on page 106](#)
- [interface \(Spanning Tree\) on page 307](#)
- [priority on page 326](#)

Understanding Spanning-Tree Instance Interface Cost

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

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

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

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

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

- Related Documentation**
- [Configuring Rapid Spanning Tree Protocol on page 62](#)
 - [Configuring Multiple Spanning Tree Protocol on page 54](#)
 - [Configuring VLAN SpanningTree Protocol on page 106](#)
 - [cost on page 291](#)
 - [interface \(Spanning Tree\) on page 307](#)

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

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

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

- Related Documentation**
- [Configuring Rapid Spanning Tree Protocol on page 62](#)
 - [Configuring Multiple Spanning Tree Protocol on page 54](#)
 - [Configuring VLAN SpanningTree Protocol on page 106](#)
 - [mode on page 316](#)
 - [interface \(Spanning Tree\) on page 307](#)

Understanding BPDU Protection for Spanning-Tree Instance Interfaces

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

The Spanning Tree Protocol (STP) family is designed to break possible loops in a Layer 2 bridged network. Loop prevention avoids damaging broadcast storms that can potentially render the network useless. STP processes on bridges exchange BPDUs to determine the LAN topology, decide the root bridge, stop forwarding on some ports, and so on. However, a misbehaving user application or device can interfere with the operation of the STP protocols and cause network problems.

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

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

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

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

**Related
Documentation**

- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)
- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240](#)
- [Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 137](#)
- [Configuring BPDU Protection on All Edge Ports on page 145](#)

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.

**Related
Documentation**

- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [Configuring VLAN SpanningTree Protocol on page 106](#)
- [forward-delay on page 301](#)

Configuring Spanning Tree Protocols on EX Series Switches (J-Web Procedure)



NOTE: This topic applies only to the J-Web Application package.

EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP). You can configure STP, RSTP, and MSTP by using the J-Web interface. You can configure bridge protocol data unit (BPDU) protection on interfaces to prevent them from receiving BPDUs that could result in STP misconfigurations, which could lead to network outages.



NOTE: In EX4300 switches, you can configure STP only by enabling RSTP and forcing it to act as STP. You need to select the Force STP check box from the RSTP configuration page.

To configure STP, MSTP, or RSTP for an EX Series switch by using the J-Web interface:

1. Select **Configure > Switching > Spanning Tree**.

The Spanning Tree Configuration page displays the spanning-tree protocol configuration parameters and a list of interfaces configured for each spanning-tree protocol configuration.



NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See [Using the Commit Options to Commit Configuration Changes](#) for details about all commit options.

2. Click one of the following options:

- **Add**—Creates a spanning-tree protocol configuration.
 - a. Select a protocol name.
 - b. Enter information as described in [Table 6 on page 37](#).
 - c. Click **OK** to apply changes to the configuration or click **Cancel** to cancel without saving changes.
- **Edit**—Modifies a selected spanning-tree protocol configuration.
 - a. Enter information as described in [Table 6 on page 37](#).
 - b. Click **OK** to apply changes to the configuration or click **Cancel** to cancel without saving changes.
- **Delete**—Deletes a selected spanning-tree protocol configuration.

Table 6: Spanning-Tree Protocol Configuration Parameters

Field	Function	Your Action
General		
Protocol Name	Specifies the spanning-tree protocol type: STP, MSTP, or RSTP.	None.

Table 6: Spanning-Tree Protocol Configuration Parameters (*continued*)

Field	Function	Your Action
Disable	Disables spanning-tree protocols on the interface.	To enable this option, select the check box.
BPDU Protect	Specifies BPDU protection on all edge interfaces on the switch.	To enable this option, select the check box.
Bridge Priority	Specifies the bridge priority. The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.	Select a value from the list.
Forward Delay	Specifies the number of seconds an interface waits before changing from spanning-tree learning and listening states to the forwarding state.	Type a value.
Hello Time	Specifies the time interval in seconds at which the root bridge transmits configuration BPDUs.	Type a value.
Max Age	Specifies the maximum-aging time in seconds for all MST instances. The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.	Type a value.
Max Hops	(MSTP only) Specifies the number of hops in a region before the BPDU is discarded.	Type a value.
Configuration Name	(MSTP only) Specifies the MSTP region name carried in the MSTP BPDUs.	Type a name.
Revision Level	(MSTP only) Specifies the revision number of the MSTP configuration.	Type a value.
Force STP Version	Enables or disables STP.	To enable this option, select the check box.
<p>NOTE: This option is supported only on EX4300 switches.</p>		
Ports		

Table 6: Spanning-Tree Protocol Configuration Parameters (*continued*)

Field	Function	Your Action
Interface Name	Specifies an interface for the spanning-tree protocol.	<ol style="list-style-type: none"> Click the Ports tab. Choose one of the following options: <ul style="list-style-type: none"> Click Add and select an interface from the list. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. Select an interface in the Port/State table and click Edit. To delete an interface from the configuration, select it in the Port/State table and click Remove.
Cost	Specifies the link cost to determine which bridge is the designated bridge and which interface is the designated interface.	Type a value.
Priority	Specifies the interface priority to determine which interface is elected as the root port.	Select a value from the list.
Disable Port	Disables the spanning-tree protocol on the interface.	To enable the option, select the check box.
NOTE: This option is not supported on EX4300 switches.		
Edge	Configures the interface as an edge interface. Edge interfaces immediately transition to a forwarding state.	To enable the option, select the check box.
No Root Port	Specifies an interface as a spanning-tree designated port. If the bridge receives superior STP BPDUs on a root-protected interface, that interface transitions to a root-prevented STP state (inconsistency state) and the interface is blocked. This blocking prevents a bridge that should not be the root bridge from being elected the root bridge. When the bridge stops receiving superior STP BPDUs on the root-protected interface, interface traffic is no longer blocked.	To enable the option, select the check box.
Interface Mode	Specifies the link mode.	<ol style="list-style-type: none"> To enable the option, select the check box. Select one of the following: <ul style="list-style-type: none"> Point to Point—For a full-duplex link, the default link mode is point-to-point. Shared—For a half-duplex link, the default link mode is shared.

Table 6: Spanning-Tree Protocol Configuration Parameters (*continued*)

Field	Function	Your Action
BPDU Timeout Action	Specifies the BPDU timeout action for the interface.	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Log • Block <p>NOTE: For EX4300 switches, you can select one of the following options:</p> <ul style="list-style-type: none"> • Alarm • Block
MSTI (MSTP only)		
MSTI Name	Specifies a name (an MSTI ID) for the MST instance.	<ol style="list-style-type: none"> 1. Click the MSTI tab. 2. Choose one of the following options: <ul style="list-style-type: none"> • Click Add. • Select an MSTI ID and click Edit. • To delete an MSTI from the configuration, select the MSTI ID and click Remove. <p>NOTE: For EX4300 switches, the MSTI ID can be 1 through 64.</p>
Bridge Priority	Specifies the bridge priority. The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.	Select a value from the list.
VLAN ID	Specifies the VLAN for the MST instance.	<p>In the VLAN box, choose one of the following options:</p> <ul style="list-style-type: none"> • Click Add, select a VLAN from the list, and click OK. • To remove a VLAN association, select the VLAN ID, click Remove, and click OK.

Table 6: Spanning-Tree Protocol Configuration Parameters (*continued*)

Field	Function	Your Action
Interfaces	Specifies an interface for the MST instance.	<ol style="list-style-type: none"> 1. In the Interfaces box, click Add and select an interface from the list, or select an interface from the list and click Edit. 2. Specify the link cost to determine which bridge is the designated bridge and which interface is the designated interface. 3. Specify the interface priority to determine which interface is elected as the root port. 4. If you want to disable the interface, select the check box. 5. Click OK. <p>To delete an interface configuration, select the interface, click Remove, and click OK.</p>

Related Documentation

- [Monitoring Spanning Tree Protocols on Switches on page 269](#)
- [Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error \(CLI Procedure\) on page 147](#)
- [Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157](#)
- [Example: Configuring BPDU Protection on Switch Edge Interfaces to Prevent STP Miscalculations on page 152](#)
- [Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195](#)
- [Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66](#)

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* .

**Related
Documentation**

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

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

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

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

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

- Do not configure a spanning-tree instance interface as an edge port if it is connected to any Layer 2 bridge. An instance interface connected to Layer 2 bridges but configured as an edge port can cause physical loops.
- If the spanning-tree protocol is configured to run the original IEEE 802.1D spanning-tree version, the edge-port option (if configured) is ignored.

- If edge ports are configured at both the VSTP global and VLAN levels, the configuration at the VLAN level overrides the global configuration.

**Related
Documentation**

- [Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on page 147](#)
- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [Configuring VLAN SpanningTree Protocol on page 106](#)
- [edge on page 297](#)
- [interface \(Spanning Tree\) on page 307](#)
- [Configuring RSTP on EX Series Switches \(CLI Procedure\) on page 65](#)
- [Configuring VLAN Spanning Tree Protocol on Switches on page 111](#)
- [Configuring MSTP on Switches on page 51](#)

CHAPTER 3

Configuring STP

- [Understanding System Identifier for Bridges in STP or RSTP Instances on page 45](#)
- [Configuring STP on EX Series Switches \(CLI Procedure\) on page 45](#)

Understanding System Identifier for Bridges in STP or RSTP Instances

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

Related Documentation

- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [extended-system-id on page 299](#)

Configuring STP on EX Series Switches (CLI Procedure)

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

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

To configure STP:

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

- To delete RSTP on the entire switch:

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

- To disable RSTP on a specific interface:

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

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

- To enable STP on all interfaces:

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

- To enable STP on a specific interface:

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

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

- To enable ARP on STP on all interfaces:

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

- To enable ARP on STP on a specific interface:

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

Related Documentation

- [Understanding STP on page 26](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)

CHAPTER 4

Configuring MSTP

- [Understanding MSTP on page 48](#)
- [Configuring MSTP on Switches on page 51](#)
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [Configuring MSTP Instances on a Physical Interface on page 58](#)
- [Disabling MSTP on page 59](#)

Understanding MSTP

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:

- [MSTP Maps Multiple VLANs on page 48](#)
- [Configuring MSTP Regions on page 49](#)
- [Selecting a Spanning Tree Protocol on page 49](#)

MSTP Maps Multiple VLANs

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

MSTP creates a common and internal spanning tree (CIST) to interconnect and manage all MSTP regions and even individual devices that run RSTP or STP, which are recognized as distinct spanning-tree regions by MSTP. The CIST views each MSTP region as a virtual bridge, regardless of the actual number of devices participating in the MSTP region, and enables multiple spanning-tree instances (MSTIs) to link to other regions. The CIST is a single topology that connects all switches (STP, RSTP, and MSTP devices) through an

active topology, ensuring connectivity between LANs and devices within a bridged network. This functionality provided by MSTP enables you to better utilize network resources while remaining backward-compatible with older network devices.

Configuring MSTP Regions

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

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

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

Selecting a Spanning Tree Protocol

The default factory configuration is RSTP, a faster version of STP. To determine which spanning-tree protocol is best for your situation, see [Table 7 on page 49](#) below.

Table 7: Selecting a Spanning Tree Protocol

Protocol	Advantages	Disadvantages
RSTP	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • RSTP does not work with 802.1D 1998 bridges. • RSTP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic.

Table 7: Selecting a Spanning Tree Protocol (*continued*)

Protocol	Advantages	Disadvantages
STP	<ul style="list-style-type: none"> Spanning Tree Protocol works with 802.1D 1998 bridges. RSTP is backward compatible with STP; therefore, switches do not all have to run STP. 	<ul style="list-style-type: none"> 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 <code>force-version</code>. However, the CLI does not include <code>[edit protocols stp]</code>.
MSTP	<ul style="list-style-type: none"> Multiple Spanning Tree Protocol works with most VLANs. RSTP and STP are recognized as distinct spanning-tree regions by MSTP. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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.

- Related Documentation**
- [Understanding RSTP on page 21](#)
 - [Understanding VSTP on page 29](#)
 - [Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195](#)
 - [Configuring MSTP on Switches on page 51](#)

Configuring MSTP on Switches

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

To configure the Multiple Spanning Tree Protocol:

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

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

- 2.

Configure the interfaces that participate in the MSTP instance.

- Configure a specific 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
```

- Enable MSTP on all the interfaces:



NOTE: You *cannot* disable MSTP on all the interfaces.

- a. Enable MSTP on all interfaces:

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

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 272](#).

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 242](#).

4. Configure hello BPDU timers.

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

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

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

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

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

```
[edit ... protocols mstp]
user@switch# set forward-delay seconds
```

6. Configure MSTP-specific options.

a. Configure the MSTP region configuration name:

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

b. Configure the MSTP revision level:

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

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

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

Related Documentation

- [Configuring MSTP Instances on a Physical Interface on page 58](#)

Configuring Multiple Spanning Tree Protocol

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

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

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

To configure the Multiple Spanning Tree Protocol:

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

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

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

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

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

a. Enable configuration of the interface:

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

b. Configure the interface priority:

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

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

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

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

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

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

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

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

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

You can also enable BPDU root protection for all spanning-tree protocol instances on the interface. BPDU root protect ensures the port is the spanning-tree designated port. If the port receives superior BPDU packets, root protect moves this port to a root-prevented spanning-tree state. For configuration details, see [“Checking the Status of Spanning-Tree Instance Interfaces” on page 272](#).

4. Configure the bridge priority:

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

For more information, see [“Understanding Bridge Priority for Election of Root Bridge and Designated Bridge” on page 242](#).

5. Configure hello BPDU timers.

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

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

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

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

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

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

7. Configure MSTP-specific options.

- a. Configure the MSTP region configuration name:

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

- b. Configure the MSTP revision level:

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

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

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

8. Verify the MSTP configuration:

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



```
        max-hops hops; # MST maximum hops.  
    }  
}
```

- Related Documentation**
- [Configuring MSTP Instances on a Physical Interface on page 58](#)
 - [Disabling MSTP on page 59](#)

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 MSTP” on page 54.

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 242.](#)

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

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

5. Verify the MST interface configuration.

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

- Related Documentation**
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
 - [Disabling MSTP on page 59](#)

Disabling MSTP

To disable the entire MSTP instance:

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

- `[edit protocols mstp]`
- `[edit routing-instances routing-instance-name protocols mstp]`

**Related
Documentation**

- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [Configuring MSTP Instances on a Physical Interface on page 58](#)

CHAPTER 5

Configuring RSTP

- [Understanding System Identifier for Bridges in STP or RSTP Instances on page 61](#)
- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [Configuring RSTP on EX Series Switches \(CLI Procedure\) on page 65](#)
- [Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66](#)
- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
- [Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 103](#)
- [Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 103](#)
- [Forcing RSTP or VSTP to Run as IEEE 802.1D STP \(CLI Procedure\) on page 104](#)

Understanding System Identifier for Bridges in STP or RSTP Instances

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

Related Documentation

- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [extended-system-id on page 299](#)

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 bpd-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 272](#).

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 242](#).

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.
      bpd-destination-mac-address provider-bridge-group; # Optional
      extended-system-id identifier; # Optional.
      interface interface-name {
        priority interface-priority;
        cost interface-link-cost; # Optional.
        mode (p2p | shared);
        edge; # Optional.
      }
      bridge-priority bridge-priority;
      max-age seconds;
      hello-time seconds;
      forward-delay seconds; # Optional.
    }
  }
}
```

Related Documentation

- [Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 103](#)
- [Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 103](#)
- [Understanding Provider Bridge Participation in RSTP or MSTP Instances on page 31](#)
- [Understanding System Identifier for Bridges in STP or RSTP Instances on page 45](#)

Configuring RSTP on EX Series Switches (CLI Procedure)

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

To enable RSTP:

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

- To disable MSTP:

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

2. Configure RSTP

- To enable RSTP on a specific interface:

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

- To disable RSTP on a specific interface:

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

- To enable RSTP on a range of interfaces:

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

- To enable RSTP on all interfaces:

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

Related Documentation

- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)
- [Understanding RSTP on page 21](#)

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



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 84. 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 on page 66](#)
- [Overview and Topology on page 66](#)
- [Configuring RSTP and Nonstop Bridging on Switch 1 on page 68](#)
- [Configuring RSTP and Nonstop Bridging on Switch 2 on page 72](#)
- [Configuring RSTP and Nonstop Bridging on Switch 3 on page 75](#)
- [Configuring RSTP and Nonstop Bridging on Switch 4 on page 79](#)
- [Verification on page 82](#)

Requirements

This example uses the following software and hardware components:

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

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

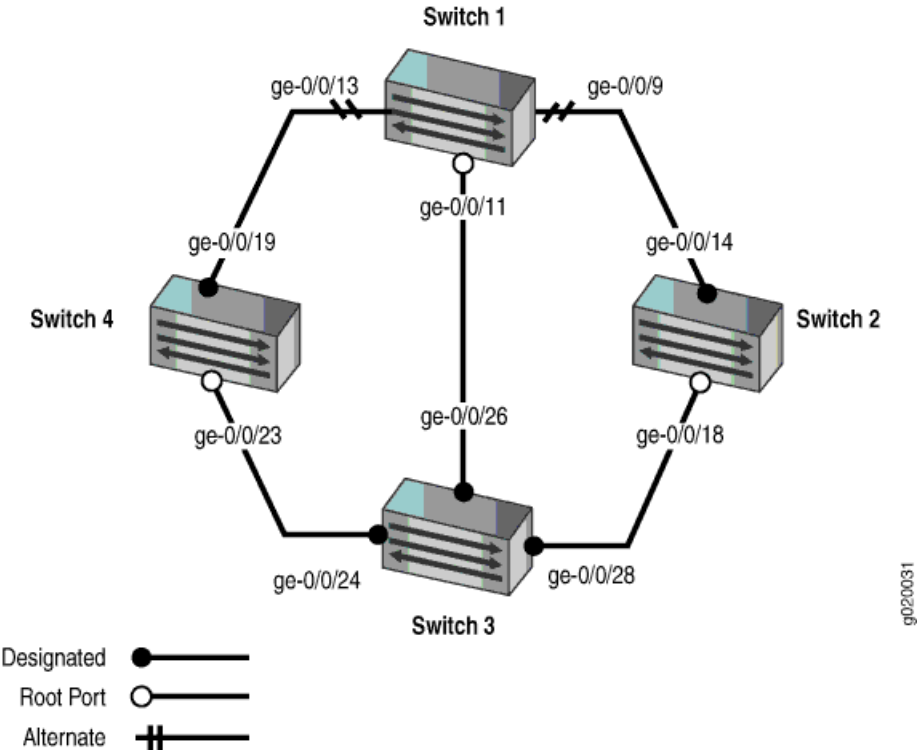
- Installed and connected the four switches. See the hardware documentation for your switch.
- Performed the initial software configuration on all switches. See *Connecting and Configuring an EX Series Switch (CLI Procedure)* or *Connecting and Configuring an EX Series Switch (J-Web Procedure)*.

Overview and Topology

RSTP works by identifying certain links as point to point links and blocking other possible paths. When one of the point-to-point links fails, a designated alternate link transitions to the forwarding state and take over. Configuring nonstop bridging (NSB) on a switch

with redundant Routing Engines keeps RSTP synchronized on both Routing Engines. This way, RSTP remains active immediately after a switchover because it is already synchronized to the backup Routing Engine. RSTP does not have to reconverge after a Routing Engine switchover when NSB is enabled because the neighbor devices do not detect an RSTP change on the switch. In this example, four EX Series switches are connected in the topology displayed in [Figure 1 on page 67](#) to create a loop-free topology with NSB applied to switches with dual Routing Engines.

Figure 1: Network Topology for RSTP



[Table 8 on page 67](#) shows the components of the topology for this example.



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

Table 8: Components of the Topology for Configuring RSTP

Property	Settings
Switch 1	The following interfaces on Switch 1 are connected in this way: <ul style="list-style-type: none">• 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

Table 8: Components of the Topology for Configuring RSTP (*continued*)

Property	Settings
Switch 2	<p>The following interfaces on Switch 2 are connected in this way:</p> <ul style="list-style-type: none"> • ge-0/0/14 is connected to Switch 1 • ge-0/0/18 is connected to Switch 3
Switch 3	<p>The following interfaces on Switch 3 are connected in this way:</p> <ul style="list-style-type: none"> • 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	<p>The following interfaces on Switch 4 are connected in this way:</p> <ul style="list-style-type: none"> • ge-0/0/19 is connected to Switch 1 • ge-0/0/23 is connected to Switch 3
VLAN names and tag IDs	<p>voice-vlan, tag 10 employee-vlan, tag 20 guest-vlan, tag 30 camera-vlan, tag 40</p>

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

An RSTP topology contains ports that have specific roles:

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



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

Configuring RSTP and Nonstop Bridging on Switch 1

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

```
[edit]
set vlans voice-vlan description "Voice VLAN"
```

```

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

```

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

```

set chassis redundancy graceful switchover
set system commit synchronize
set protocols layer2-control nonstop-bridging

```

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

```
}
system {
    commit synchronize;
}
chassis {
    redundancy {
        graceful-switchover;
    }
}
```

Configuring RSTP and Nonstop Bridging on Switch 2

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

```
[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/14 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/18 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/14 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/18 unit 0 family ethernet-switching interface-mode trunk
set protocols rstp bridge-priority 32k
set protocols rstp interface ge-0/0/14 cost 1000
set protocols rstp interface ge-0/0/14 mode point-to-point
set protocols rstp interface ge-0/0/18 cost 1000
set protocols rstp interface ge-0/0/18 mode point-to-point
```



NOTE: Starting with Junos OS Release 15.1 for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can configure spanning tree parameters globally on all spanning tree interfaces. See [“Configuring RSTP on EX Series Switches \(CLI Procedure\)” on page 65](#) 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;
    }
  }
}
```

```

vlangs {
  voice-vlan {
    vlan-id 10;
  }
  employee-vlan {
    vlan-id 20;
  }
  guest-vlan {
    vlan-id 30;
  }
  camera-vlan {
    vlan-id 40;
  }
}
system {
  commit synchronize;
}
chassis {
  redundancy {
    graceful-switchover;
  }
}

```

Configuring RSTP and Nonstop Bridging on Switch 3

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

```

[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/26 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/28 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/26 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/28 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/24 unit 0 family ethernet-switching interface-mode trunk
set protocols rstp bridge-priority 8k
set protocols rstp interface ge-0/0/26 cost 1000
set protocols rstp interface ge-0/0/26 mode point-to-point
set protocols rstp interface ge-0/0/28 cost 1000
set protocols rstp interface ge-0/0/28 mode point-to-point
set protocols rstp interface ge-0/0/24 cost 1000
set protocols rstp interface ge-0/0/24 mode point-to-point

```

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

```

set chassis redundancy graceful switchover
set system commit synchronize

```

set protocols layer2-control nonstop-bridging**Step-by-Step
Procedure**

To configure RSTP and nonstop bridging on Switch 3:

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

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

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

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

3. Configure the port mode for the interfaces:

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

4. Configure RSTP on the switch:

```
[edit protocols]
user@switch3# rstp bridge-priority 8k
user@switch3# rstp interface ge-0/0/26 cost 1000
user@switch3# rstp interface ge-0/0/26 mode point-to-point
user@switch3# rstp interface ge-0/0/28 cost 1000
user@switch3# rstp interface ge-0/0/28 mode point-to-point
user@switch3# rstp interface ge-0/0/24 cost 1000
user@switch3# rstp interface ge-0/0/24 mode point-to-point
```

**Step-by-Step
Procedure**

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

1. Enable graceful Routing Engine switchover (GRES):

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

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

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

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

3. Enable nonstop bridging:

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



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

Results Check the results of the configuration:

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

```
    }
  }
}
}
}
protocols {
  layer2-control {
    nonstop-bridging;
  }
  rstp {
    bridge-priority 8k;
    interface ge-0/0/26 {
      cost 1000;
      mode point-to-point;
    }
    interface ge-0/0/28 {
      cost 1000;
      mode point-to-point;
    }
    interface ge-0/0/24 {
      cost 1000;
      mode point-to-point;
    }
    bridge-priority 8k;
  }
}
}
vlands {
  voice-vlan {
    vlan-id 10;
  }
  employee-vlan {
    vlan-id 20;
  }
  guest-vlan {
    vlan-id 30;
  }
  camera-vlan {
    vlan-id 40;
  }
}
system {
  commit synchronize;
}
chassis {
  redundancy {
    graceful-switchover;
  }
}
```

Configuring RSTP and Nonstop Bridging on Switch 4

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

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

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

```
set chassis redundancy graceful switchover
set system commit synchronize
set protocols layer2-control nonstop-bridging
```

Step-by-Step Procedure To configure RSTP and nonstop bridging on Switch 4:

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

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

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

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

3. Configure the port mode for the interfaces:

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

4. Configure RSTP on the switch:

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

**Step-by-Step
Procedure**

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

1. Enable graceful Routing Engine switchover (GRES):

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

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

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

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

3. Enable nonstop bridging:

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



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

Results Check the results of the configuration:

```
user@switch4> show configuration
interfaces {
  ge-0/0/23 {
    unit 0 {
      family ethernet-switching {
```



```
        interface-mode trunk;
        vlan {
            members [10 20 30 40];
        }
    }
}
ge-0/0/19 {
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members [10 20 30 40];
            }
        }
    }
}
}
protocols {
    layer2-control {
        nonstop-bridging;
    }
    rstp {
        bridge-priority 16k;
        interface ge-0/0/23 {
            cost 1000;
            mode point-to-point;
        }
        interface ge-0/0/19 {
            cost 1000;
            mode point-to-point;
        }
    }
}
}
vlangs {
    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

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

- [Verifying RSTP Configuration on Switch 1 on page 82](#)
- [Verifying RSTP Configuration on Switch 2 on page 82](#)
- [Verifying RSTP Configuration on Switch 3 on page 83](#)
- [Verifying RSTP Configuration on Switch 4 on page 83](#)

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 port ID	Designated bridge ID	Port Cost	State	Role
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 Refer to the topology in [Figure 1 on page 67](#). 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 port ID	Designated bridge ID	Port Cost	State	Role
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 Refer to the topology in [Figure 1 on page 67](#). 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 port ID	Designated bridge ID	Port Cost	State	Role
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 Refer to the topology in [Figure 1 on page 67](#). 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 port ID	Designated bridge ID	Port Cost	State	Role
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	DESC

Meaning Refer to the topology in [Figure 1 on page 67](#). The operational mode command **show spanning-tree interface** shows that interface **ge-0/0/23** is the root interface and forwarding.

Release History Table

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

- Related Documentation**
- [Configuring RSTP on EX Series Switches \(CLI Procedure\) on page 65](#)
 - [Understanding RSTP on page 21](#)

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

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 on page 85](#)
- [Overview and Topology on page 85](#)
- [Configuring RSTP and Nonstop Bridging on Switch 1 on page 87](#)
- [Configuring RSTP and Nonstop Bridging on Switch 2 on page 91](#)
- [Configuring RSTP and Nonstop Bridging on Switch 3 on page 94](#)
- [Configuring RSTP and Nonstop Bridging on Switch 4 on page 97](#)
- [Verification on page 100](#)

Requirements

This example uses the following hardware and software components:

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

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

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

Overview and Topology

RSTP works by identifying certain links as point to point links and blocking other possible paths. When one of the point-to-point links fails, a designated alternate link transitions to the forwarding state and take over. Configuring nonstop bridging (NSB) on a switch with redundant Routing Engines keeps RSTP synchronized on both Routing Engines. This way, RSTP remains active immediately after a switchover because it is already synchronized to the backup Routing Engine. RSTP does not have to reconverge after a Routing Engine switchover when NSB is enabled because the neighbor devices do not detect an RSTP change on the switch. In this example, four EX Series switches are connected in the topology displayed in [Figure 1 on page 67](#) to create a loop-free topology with NSB applied to switches with dual Routing Engines.

Figure 2: Network Topology for RSTP

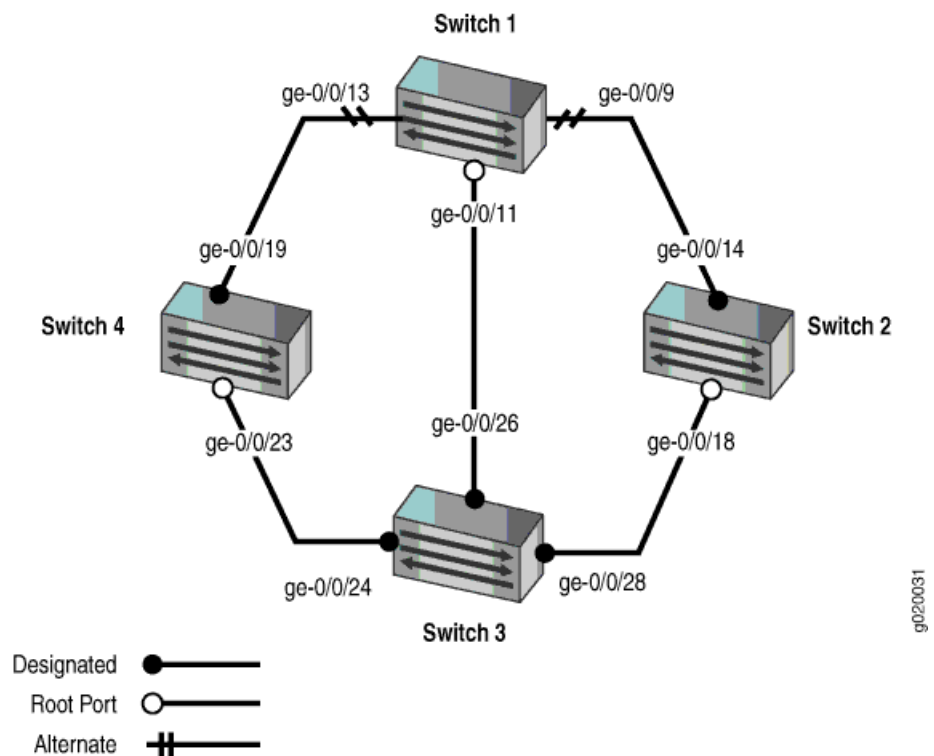


Table 8 on page 67 shows the components of the topology for this example.



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

Table 9: Components of the Topology for Configuring RSTP

Property	Settings
Switch 1	<p>The following interfaces on Switch 1 are connected in this way:</p> <ul style="list-style-type: none"> • 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	<p>The following interfaces on Switch 2 are connected in this way:</p> <ul style="list-style-type: none"> • ge-0/0/14 is connected to Switch 1 • ge-0/0/18 is connected to Switch 3
Switch 3	<p>The following interfaces on Switch 3 are connected in this way:</p> <ul style="list-style-type: none"> • 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

Table 9: Components of the Topology for Configuring RSTP (*continued*)

Property	Settings
Switch 4	<p>The following interfaces on Switch 4 are connected in this way:</p> <ul style="list-style-type: none"> • <code>ge-0/0/19</code> is connected to Switch 1 • <code>ge-0/0/23</code> is connected to Switch 3
VLAN names and tag IDs	<p>voice-vlan, tag 10 employee-vlan, tag 20 guest-vlan, tag 30 camera-vlan, tag 40</p>

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

An RSTP topology contains ports that have specific roles:

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



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

Configuring RSTP and Nonstop Bridging on Switch 1

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

```
[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/9 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/13 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;
        }
    }
}
}
vlangs {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
system {
    commit synchronize;
}
chassis {
    redundancy {
        graceful-switchover;
    }
}
```

```

ethernet-switching-options {
    nonstop-bridging;
}

```

Configuring RSTP and Nonstop Bridging on Switch 2

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

```

[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/14 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/18 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/14 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/18 unit 0 family ethernet-switching port-mode trunk
set protocols rstp bridge-priority 32k
set protocols rstp interface ge-0/0/14.0 cost 1000
set protocols rstp interface ge-0/0/14.0 mode point-to-point
set protocols rstp interface ge-0/0/18.0 cost 1000
set protocols rstp interface ge-0/0/18.0 mode point-to-point

```

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

```

set chassis redundancy graceful switchover
set system commit synchronize
set ethernet-switching-options nonstop-bridging

```

Step-by-Step Procedure To configure RSTP and nonstop bridging on Switch 2:

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

```

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

```

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

```

[edit interfaces]

```

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

3. Configure the port mode for the interfaces:

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

4. Configure RSTP on the switch:

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

Step-by-Step Procedure

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

1. Enable graceful Routing Engine switchover (GRES):

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

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

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

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

3. Enable nonstop bridging:

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



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

Results Check the results of the configuration:

```
user@switch2> show configuration
```

```
interfaces {
  ge-0/0/14 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members [10 20 30 40];
        }
      }
    }
  }
  ge-0/0/18 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members [10 20 30 40];
        }
      }
    }
  }
}
protocols {
  rstp {
    bridge-priority 32k;
    interface ge-0/0/14.0 {
      cost 1000;
      mode point-to-point;
    }
    interface ge-0/0/18.0 {
      cost 1000;
      mode point-to-point;
    }
  }
}
vlans {
  voice-vlan {
    vlan-id 10;
  }
  employee-vlan {
    vlan-id 20;
  }
  guest-vlan {
    vlan-id 30;
  }
  camera-vlan {
    vlan-id 40;
  }
}
system {
  commit synchronize;
}
chassis {
  redundancy {
    graceful-switchover;
  }
}
```

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

Configuring RSTP and Nonstop Bridging on Switch 3

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

```
[edit]  
set vlans voice-vlan description "Voice VLAN"  
set vlans voice-vlan vlan-id 10  
set vlans employee-vlan description "Employee VLAN"  
set vlans employee-vlan vlan-id 20  
set vlans guest-vlan description "Guest VLAN"  
set vlans guest-vlan vlan-id 30  
set vlans camera-vlan description "Camera VLAN"  
set vlans camera-vlan vlan-id 40  
set interfaces ge-0/0/26 unit 0 family ethernet-switching vlan members [10 20 30 40]  
set interfaces ge-0/0/28 unit 0 family ethernet-switching vlan members [10 20 30 40]  
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members [10 20 30 40]  
set interfaces ge-0/0/26 unit 0 family ethernet-switching port-mode trunk  
set interfaces ge-0/0/28 unit 0 family ethernet-switching port-mode trunk  
set interfaces ge-0/0/24 unit 0 family ethernet-switching port-mode trunk  
set protocols rstp bridge-priority 8k  
set protocols rstp interface ge-0/0/26.0 cost 1000  
set protocols rstp interface ge-0/0/26.0 mode point-to-point  
set protocols rstp interface ge-0/0/28.0 cost 1000  
set protocols rstp interface ge-0/0/28.0 mode point-to-point  
set protocols rstp interface ge-0/0/24.0 cost 1000  
set protocols rstp interface ge-0/0/24.0 mode point-to-point
```

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

```
set chassis redundancy graceful switchover  
set system commit synchronize  
set ethernet-switching-options nonstop-bridging
```

Step-by-Step Procedure To configure RSTP and nonstop bridging on Switch 3:

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

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

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

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

3. Configure the port mode for the interfaces:

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

4. Configure RSTP on the switch:

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

Step-by-Step Procedure

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

1. Enable graceful Routing Engine switchover (GRES):

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

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

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

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

3. Enable nonstop bridging:

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



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

Results Check the results of the configuration:

```
user@switch3> show configuration
interfaces {
  ge-0/0/26 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members [10 20 30 40];
        }
      }
    }
  }
  ge-0/0/28 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members [10 20 30 40];
        }
      }
    }
  }
  ge-0/0/24 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members [10 20 30 40];
        }
      }
    }
  }
}
protocols {
  rstp {
    bridge-priority 8k;
    interface ge-0/0/26.0 {
      cost 1000;
      mode point-to-point;
    }
    interface ge-0/0/28.0 {
      cost 1000;
      mode point-to-point;
    }
  }
}
```



```

        interface ge-0/0/24.0 {
            cost 1000;
            mode point-to-point;
        }
    }
    bridge-priority 8k;
}
}
vpls {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
system {
    commit synchronize;
}
chassis {
    redundancy {
        graceful-switchover;
    }
}
ethernet-switching-options {
    nonstop-bridging;
}

```

Configuring RSTP and Nonstop Bridging on Switch 4

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

```

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

```

```
set protocols rstp interface ge-0/0/19.0 cost 1000
set protocols rstp interface ge-0/0/19.0 mode point-to-point
```

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

```
set chassis redundancy graceful switchover
set system commit synchronize
set ethernet-switching-options nonstop-bridging
```

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 4:

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

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

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

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

3. Configure the port mode for the interfaces:

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

4. Configure RSTP on the switch:

```
[edit protocols]
user@switch4# rstp bridge-priority 16k
user@switch4# rstp interface all cost 1000
user@switch4# rstp interface ge-0/0/23.0 cost 1000
user@switch4# rstp interface ge-0/0/23.0 mode point-to-point
user@switch4# rstp interface ge-0/0/19.0 cost 1000
user@switch4# rstp interface ge-0/0/19.0 mode point-to-point
```

Step-by-Step Procedure

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

1. Enable graceful Routing Engine switchover (GRES):

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

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

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

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

3. Enable nonstop bridging:

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



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

Results Check the results of the configuration:

```
user@switch4> show configuration
interfaces {
  ge-0/0/23 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members [10 20 30 40];
        }
      }
    }
  }
  ge-0/0/19 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members [10 20 30 40];
        }
      }
    }
  }
}
protocols {
  rstp {
    bridge-priority 16k;
    interface ge-0/0/23.0 {
```

```
        cost 1000;
        mode point-to-point;
    }
    interface ge-0/0/19.0 {
        cost 1000;
        mode point-to-point;
    }
}
}
vllans {
    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

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

- [Verifying RSTP Configuration on Switch 1 on page 100](#)
- [Verifying RSTP Configuration on Switch 2 on page 101](#)
- [Verifying RSTP Configuration on Switch 3 on page 101](#)
- [Verifying RSTP Configuration on Switch 4 on page 102](#)

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 port ID	Designated bridge ID	Port Cost	State	Role
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 Refer to the topology in [Figure 1 on page 67](#). 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 port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/14.0	128:527	128:527	32768.0019e2503d20	1000	FWD	DESC
ge-0/0/18.0	128:529	128:529	8192.0019e25051e0	1000	FWD	ROOT

Meaning Refer to the topology in [Figure 1 on page 67](#). 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 port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/26.0	128:539	128:539	8192.0019e25051e0	1000	FWD	DESC
ge-0/0/28.0	128:541	128:541	8192.0019e25051e0	1000	FWD	DESC
ge-0/0/24.0	128:537	128:537	8192.0019e25051e0	1000	FWD	DESC

Meaning Refer to the topology in [Figure 1 on page 67](#). 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 port ID	Designated bridge ID	Port Cost	State	Role
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	DESC

Meaning Refer to the topology in [Figure 1 on page 67](#). The operational mode command **show spanning-tree interface** shows that interface **ge-0/0/23.0** is the root interface and forwarding.

Related Documentation

- [Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217](#)
- [Understanding RSTP on page 21](#)

Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP

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

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

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

Related Documentation

- [Configuring RSTP on EX Series Switches \(CLI Procedure\) on page 65](#)
- [Configuring VLAN Spanning Tree Protocol on Switches on page 111](#)
- [Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 103](#)
- [force-version on page 300](#)

Reverting to RSTP or VSTP from Forced IEEE 802.1D STP

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

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

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

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

Include this statement at the following hierarchy levels:

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

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

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

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

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

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

**Related
Documentation**

- [Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 103](#)
- [Configuring RSTP on EX Series Switches \(CLI Procedure\) on page 65](#)
- [Configuring VLAN Spanning Tree Protocol on Switches on page 111](#)

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



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

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

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

1. Enable IEEE 802.1D STP:

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



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

**Related
Documentation**

- [Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 103](#)
- [Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 103](#)

CHAPTER 6

Configuring VSTP

- [Configuring VLAN SpanningTree Protocol on page 106](#)
- [Configuring VLAN Spanning Tree Protocol on Switches on page 111](#)
- [Configuring VSTP on EX Series Switches \(CLI Procedure\) on page 113](#)
- [Understanding VSTP on a Trunk Port with Tagged Traffic Overview on page 115](#)
- [Example: Configuring VSTP on a Trunk Port with Tagged Traffic on page 115](#)
- [Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 127](#)
- [Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 127](#)
- [Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 128](#)
- [Forcing RSTP or VSTP to Run as IEEE 802.1D STP \(CLI Procedure\) on page 129](#)

Configuring VLAN SpanningTree Protocol

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



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

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

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

To configure the VLAN Spanning Tree Protocol:

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

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

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

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



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

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

a. Enable configuration of the interface:

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

b. Configure the interface priority:

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

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

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

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

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

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

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

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

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

You can also enable BPDU root protection for all spanning-tree protocol instances on the interface. BPDU root protect ensures the port is the spanning-tree designated port. If the port receives superior BPDU packets, root protect moves this port to a root-prevented spanning-tree state. For configuration details, see [“Checking the Status of Spanning-Tree Instance Interfaces” on page 272](#).

4. Enable configuration of a VLAN instance:

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

5. Configure the bridge priority:

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

For more information, see [“Understanding Bridge Priority for Election of Root Bridge and Designated Bridge” on page 242](#).

6. Configure hello BPDUs.

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

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

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

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

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

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

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

a. Enable configuration of the interface:

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

b. Configure the interface priority:

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

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

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

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

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

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

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

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

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

You can also enable BPDU root protection for all spanning-tree protocol instances on the interface. BPDU root protect ensures the port is the spanning-tree designated port. If the port receives superior BPDU packets, root protect moves this port to a root-prevented spanning-tree state. For configuration details, see [“Checking the Status of Spanning-Tree Instance Interfaces” on page 272](#).

9. Verify the VSTP configuration:

```
[edit]
... { # Optional logical system and/or routing instance
  protocols (STP Type) {
    vstp {
      force-version stp; # Optional.
      interface interface-name {
        priority interface-priority;
        cost interface-link-cost; # Optional.
        mode (p2p | shared);
        edge; # Optional.
      }
    }
  }
}
```

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

**Related
Documentation**

- [Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 103](#)
- [Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 103](#)
- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240](#)
- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 241](#)

Configuring VLAN Spanning Tree Protocol on Switches

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



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



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



NOTE: When you configure VSTP with the `set protocol vstp vlan all` command, VLAN ID 1 is not set; it is excluded so that the configuration is compatible with Cisco PVST+. If you want VLAN ID 1 to be included in the VSTP configuration on your switch, you must set it separately with the `set protocol vstp vlan 1` command.

You can enable or disable VSTP as follows:

- Enabling VSTP as the version of spanning-tree protocol to be configured:
 - Enable VSTP on an individual interface:

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

- Enable VSTP on all interfaces on the switch:

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

- Enable VSTP on a specific interface within a specific VLAN:

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

- Enable VSTP on all the interfaces within a specific VLAN:

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

- Enable VSTP on all the interfaces within all the VLANs on the switch:

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

- Enable VSTP on all the VLANs on the switch:

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

- Enable VSTP for a specific interface within a specified VLAN group:

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

- Enable VSTP for all the interfaces within a specified VLAN group:

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

You can disable VSTP as follows:



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

- Disable VSTP on an individual interface:

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

- Disable VSTP on a specific interface within a specific VLAN:

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

- Disable a specific VSTP interface on all the VLANs on the switch:

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

- Disable a specific VSTP interface within a specific VLAN group:

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

Related Documentation

- [Understanding VSTP on page 29](#)

Configuring VSTP on EX Series Switches (CLI Procedure)

The default spanning-tree protocol for EX Series switches is Rapid Spanning Tree Protocol (RSTP). VLAN Spanning Tree Protocol (VSTP) is an alternate protocol that allows EX Series switches to run one or more Spanning Tree Protocol (STP) or RSTP instances for each VLAN on which VSTP is enabled. For networks with multiple VLANs, VSTP improves intelligent tree spanning by defining best paths within the VLANs instead of within the entire network.



NOTE: 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.

You can configure VSTP for 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 a specific interface:

- 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.

To configure VSTP:

- For all interfaces on any of the following levels:
 - For all interfaces on the switch:

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

- For all interfaces within all VLANs:

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

- For all interfaces within a specified VLAN:

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

- For all 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
```

- On a specific interface within any of the following scopes:

- For a specific interface on the switch:

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

- For 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.

- For a specific interface within a specified VLAN:

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

- For a specific interface 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 interface-name
```

Related Documentation

- [Understanding VSTP on page 29](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)

Understanding VSTP on a Trunk Port with Tagged Traffic Overview

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

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

- Related Documentation**
- [access-trunk on page 278](#)
 - [Example: Configuring VSTP on a Trunk Port with Tagged Traffic on page 115](#)

Example: Configuring VSTP on a Trunk Port with Tagged Traffic

This example shows how to configure the VSTP to send and receive standard untagged Rapid Spanning Tree Protocol (RSTP) bridge protocol data units (BPDUs) on access trunks that interoperate with tagged VSTP BPDUs sent over the double-tagged trunk ports.

- [Requirements on page 115](#)
- [Overview on page 115](#)
- [Configuration on page 116](#)
- [Verification on page 124](#)

Requirements

This example uses the following hardware and software components:

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

Overview

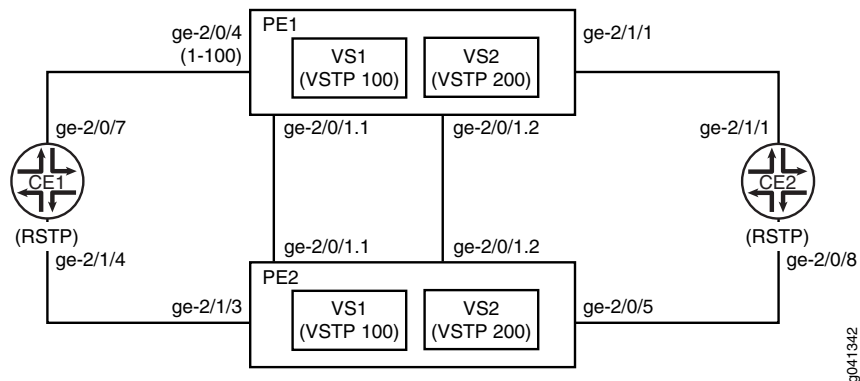
This example shows how to configure VSTP on a trunk port with tagged traffic.

Topology

[Figure 3 on page 116](#) 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 3: Topology for VSTP Configured on a Trunk Port with Tagged Traffic



Configuration

CLI Quick Configuration

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

Device PE1

```
set interfaces ge-2/0/1 flexible-vlan-tagging
set interfaces ge-2/0/1 encapsulation flexible-ethernet-services
set interfaces ge-2/0/1 unit 1 vlan-id 100
set interfaces ge-2/0/1 unit 1 family bridge interface-mode trunk
set interfaces ge-2/0/1 unit 1 family bridge inner-vlan-id-list 1-100
set interfaces ge-2/0/1 unit 2 vlan-id 200
set interfaces ge-2/0/1 unit 2 family bridge interface-mode trunk
set interfaces ge-2/0/1 unit 2 family bridge inner-vlan-id-list 1-100
set interfaces ge-2/0/4 encapsulation ethernet-vpls
set interfaces ge-2/0/4 unit 0 description to_CE1
set interfaces ge-2/0/4 unit 0 family bridge interface-mode trunk
set interfaces ge-2/0/4 unit 0 family bridge vlan-id-list 1-100
set interfaces ge-2/1/1 unit 0 description to_CE2
set interfaces ge-2/1/1 unit 0 family bridge interface-mode trunk
set interfaces ge-2/1/1 unit 0 family bridge vlan-id-list 1-100
set routing-instances vs1 instance-type virtual-switch
set routing-instances vs1 interface ge-2/0/1
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	<pre> 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 </pre>
Device CE1	<pre> 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 </pre>
Device CE2	<pre> 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 </pre>

Configuring PE1, PE2, CE1, and CE2

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

To configure Device PE1:

1. Configure the network interfaces.

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

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

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

2. Configure the routing instances.

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

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

Step-by-Step Procedure To configure Device PE2:

1. Configure the interfaces.

```
[edit interfaces]
user@PE2# set ge-2/0/1 flexible-vlan-tagging
```

```

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

```

```

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

```

```

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

```

2. Configure the routing instances.

```

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

```

```

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

```

Step-by-Step Procedure

To configure CE1:

1. Configure the interfaces.

```

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

```

```

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

```

2. Configure the protocols.

```

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

```

3. Configure the bridge domain.

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

Step-by-Step Procedure

To configure CE2:

1. Configure the interfaces.

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

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

2. Configure the protocols.

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

3. Configure the bridge domain.

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

Results

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

```
Device PE1 user@PE1# show interfaces
ge-2/0/1 {
  flexible-vlan-tagging;
  encapsulation flexible-ethernet-services;
  unit 1 {
    vlan-id 100;
    family bridge {
      interface-mode trunk;
      inner-vlan-id-list 1-100;
    }
  }
  unit 2 {
    vlan-id 200;
    family bridge {
      interface-mode trunk;
      inner-vlan-id-list 1-100;
    }
  }
}
```



```

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

user@PE1# show routing-instances
vs1 {
  instance-type virtual-switch;
  interface ge-2/0/1.1;
  interface ge-2/0/4.0;
  protocols {
    vstp {
      vlan 100 {
        interface ge-2/0/1;
        interface ge-2/0/4 {
          access-trunk;
        }
      }
    }
  }
  bridge-domains {
    bd {
      vlan-id-list 1-100;
    }
  }
}
vs2 {
  instance-type virtual-switch;
  interface ge-2/0/1.2;
  interface ge-2/0/1.0;
  protocols {
    vstp {
      vlan 200 {
        interface ge-2/0/1;
        interface ge-2/1/1 {
          access-trunk;
        }
      }
    }
  }
}

```

```
    }  
  }  
  bridge-domains {  
    bd {  
      vlan-id-list 1-100;  
    }  
  }  
}
```

Device PE2

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

```
user@PE2# show routing-instances  
vs1 {  
  instance-type virtual-switch;  
  interface ge-2/0/1.1;  
  interface ge-2/1/3.0;  
  protocols {  
    vstp {  
      vlan 100 {
```

```

        interface ge-2/0/1;
        interface ge-2/1/3 {
            access-trunk;
        }
    }
}
bridge-domains {
    bd {
        vlan-id-list 1-100;
    }
}
}
vs2 {
    instance-type virtual-switch;
    interface ge-2/0/1.2;
    interface ge-2/0/5.0;
    protocols {
        vstp {
            vlan 200 {
                interface ge-2/0/1;
                interface ge-2/0/5 {
                    access-trunk;
                }
            }
        }
    }
    bridge-domains {
        bd {
            vlan-id-list 1-100;
        }
    }
}
}

```

```

Device CE1 user@CE1# show interfaces
ge-2/0/7 {
    unit 0 {
        description to_PE1;
        family bridge {
            interface-mode trunk;
            vlan-id-list 1-100;
        }
    }
}
ge-2/1/4 {
    unit 0 {
        description to_PE2;
        family bridge {
            interface-mode trunk;
            vlan-id-list 1-100;
        }
    }
}

user@CE1# show protocols

```

```
rstp {
  interface ge-2/0/7;
  interface ge-2/1/4;
}

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

Device CE2

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

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

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

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

Verification

Confirm that the configuration is working properly.

- [Verifying That the Interfaces Are Operational on page 124](#)
- [Verifying the STP Bridge Parameters of the Routing Instances on page 125](#)
- [Displaying STP Statistics for the Configured Bridge on page 125](#)

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

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

Verifying the STP Bridge Parameters of the Routing Instances

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

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

```
user@PE1> show spanning-tree bridge routing-instance vs1
```

STP bridge parameters

```
Routing instance name      : vs1
Enabled protocol          : RSTP
```

STP bridge parameters for VLAN 100

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

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

Displaying STP Statistics for the Configured Bridge

Purpose Display spanning-tree statistics for the configured bridge.

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

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

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

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

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

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

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

Related Documentation

- [access-trunk on page 278](#)
- [Understanding VSTP on a Trunk Port with Tagged Traffic Overview on page 115](#)

Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP

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

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

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

Related Documentation

- [Configuring RSTP on EX Series Switches \(CLI Procedure\) on page 65](#)
- [Configuring VLAN Spanning Tree Protocol on Switches on page 111](#)
- [Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 103](#)
- [force-version on page 300](#)

Reverting to RSTP or VSTP from Forced IEEE 802.1D STP

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

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

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

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

Include this statement at the following hierarchy levels:

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

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

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

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

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

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

**Related
Documentation**

- [Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 103](#)
- [Configuring RSTP on EX Series Switches \(CLI Procedure\) on page 65](#)
- [Configuring VLAN Spanning Tree Protocol on Switches on page 111](#)

Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP

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

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

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

**Related
Documentation**

- [Configuring RSTP on EX Series Switches \(CLI Procedure\) on page 65](#)
- [Configuring VLAN Spanning Tree Protocol on Switches on page 111](#)
- [Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 103](#)
- [force-version on page 300](#)

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



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

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

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

1. Enable IEEE 802.1D STP:

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



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

Related Documentation

- [Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 103](#)
- [Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 103](#)

CHAPTER 7

Configuring BPDU Protection for Spanning-Tree Protocols

- [Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 132](#)
- [Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133](#)
- [Understanding BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 134](#)
- [Understanding BPDUs Used for Exchanging Information Among Bridges on page 135](#)
- [Understanding Maximum Age for Awaiting Arrival of Hello BPDUs on page 136](#)
- [Understanding Hello Time for Root Bridge to Transmit Hello BPDUs on page 136](#)
- [Understanding BPDU Protection on All Edge Ports of the Bridge on page 136](#)
- [Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 137](#)
- [Configuring BPDU Protection on Switch Spanning Tree Interfaces on page 139](#)
- [Configuring BPDU Protection on an EX Series Interface \(CLI Procedure\) on page 140](#)
- [Configuring BPDU Protection on All Edge Ports on page 145](#)
- [Unblocking a Switch Interface That Receives BPDUs in Error \(CLI Procedure\) on page 146](#)
- [Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error \(CLI Procedure\) on page 147](#)
- [Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on page 147](#)
- [Example: Configuring BPDU Protection on Switch Edge Interfaces to Prevent STP Miscalculations on page 152](#)
- [Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157](#)
- [Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 161](#)
- [Example: Blocking BPDUs on Aggregated Ethernet Interface for 600 Seconds on page 167](#)
- [Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167](#)

Understanding BPDU Protection for Spanning-Tree Instance Interfaces

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

The Spanning Tree Protocol (STP) family is designed to break possible loops in a Layer 2 bridged network. Loop prevention avoids damaging broadcast storms that can potentially render the network useless. STP processes on bridges exchange BPDUs to determine the LAN topology, decide the root bridge, stop forwarding on some ports, and so on. However, a misbehaving user application or device can interfere with the operation of the STP protocols and cause network problems.

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

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

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

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

Related Documentation

- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)
- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240](#)
- [Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 137](#)
- [Configuring BPDU Protection on All Edge Ports on page 145](#)

Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches

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

- [Different Kinds of BPDUs on page 133](#)
- [Protecting Switches from Incompatible BPDUs on page 133](#)

Different Kinds of BPDUs

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

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

Protecting Switches from Incompatible BPDUs

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

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

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

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

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

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

**Related
Documentation**

- [Configuring BPDU Protection on Switch Spanning Tree Interfaces on page 139](#)

Understanding BPDU Protection for Individual Spanning-Tree Instance Interfaces

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

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



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

**Related
Documentation**

- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)
- [Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35](#)

- [Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 137](#)

Understanding BPDUs Used for Exchanging Information Among Bridges

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

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



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

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

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

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



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

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

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

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

**Related
Documentation**

- [Understanding Loop Protection for Spanning-Tree Instance Interfaces on page 175](#)
- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)
- [Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35](#)

Understanding Maximum Age for Awaiting Arrival of Hello BPDUs

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

**Related
Documentation**

- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [Configuring VLAN SpanningTree Protocol on page 106](#)
- [max-age on page 313](#)

Understanding Hello Time for Root Bridge to Transmit Hello BPDUs

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

**Related
Documentation**

- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [Configuring VLAN SpanningTree Protocol on page 106](#)
- [hello-time on page 303](#)

Understanding BPDU Protection on All Edge Ports of the Bridge

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

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



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

Related Documentation

- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)
- [Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35](#)
- [Configuring BPDU Protection on All Edge Ports on page 145](#)

Configuring BPDU Protection for Spanning-Tree Instance Interfaces

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

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

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

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

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

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

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

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

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

```
[edit]
interfaces {
  ge-fpc/pic/port { # VLAN encapsulation on a Gigabit Ethernet.
    encapsulation (ethernet-bridge | ethernet-vpls | extended-vlan-bridge |
      extended-vlan-vpls | vlan-bridge | vlan-vpls);
  }
  xe-fpc/pic/port { # VLAN encapsulation on 10-Gigabit Ethernet.
    encapsulation (ethernet-bridge | ethernet-vpls | extended-vlan-bridge |
      extended-vlan-vpls | vlan-bridge | vlan-vpls);
  }
  ae-X { # VLAN encapsulation
    encapsulation (ethernet-vpls | vlan-vpls); # on aggregated Ethernet.
    ...
  }
  ae-X { # Extended VLAN encapsulation
```

```
    vlan-tagging; # on aggregated Ethernet.
    encapsulation extended-vlan-vpls;
    unit logical-unit-number {
        vlan-id number;
        .....
    }
    .....
}
}
protocols
  layer2-control {
    bpdu-block
      interface interface-name;
      disable-timeout seconds;
  }
}
```

**Related
Documentation**

- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)
- [Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35](#)
- [Understanding BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 134](#)

Configuring BPDU Protection on Switch Spanning Tree Interfaces



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

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

To configure BPDU protection for spanning-tree instance interfaces:

- On a specific spanning-tree interface:
 1. To enable BPDU protection on a specified spanning-tree interface:

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

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

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

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

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

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

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

Related Documentation

- [Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35](#)
- [Understanding BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 134](#)
- [clear error bpu interface on page 357](#)

Configuring BPDU Protection on an EX Series Interface (CLI Procedure)

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

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

This topic describes:

- [Configuring BPDU protection For Edge Interfaces on page 140](#)
- [Configuring BPDU Protection for Interfaces \(Port Shutdown Mode\) on page 141](#)
- [Configuring BPDU Protection for Interfaces \(BPDU Drop Mode\) on page 143](#)

Configuring BPDU protection For Edge Interfaces

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

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



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

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



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

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

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

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

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

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

4. Commit the configuration:

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

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

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

```
user@switch> show ethernet-switching interfaces
Interface  State  VLAN members  Tag  Tagging  Blocking
ge-0/0/0.0 down  default      untagged  Disabled by bpdv-control
me0.0      up     mgmt         untagged  unblocked
```

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

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

Configuring BPDU Protection for Interfaces (Port Shutdown Mode)

In a spanning-tree network, you might need to configure BPDU protection on interfaces that are not explicitly configured as edge interfaces. In such cases, use the **set ethernet-switching-options bpdv-block** configuration command for BPDU protection. When you use this command, you can configure for the interface to either shutdown, or to only drop the BPDU packets and retain its state as up, on receiving incompatible BPDU packets. For the procedure to configure an interface to drop BPDU packets and to retain

its status as up, see “[Configuring BPDU Protection for Interfaces \(BPDU Drop Mode\)](#)” on [page 143](#). For configuring an interface to only drop incompatible BPDU packets and to retain the interface state as up, no spanning-tree protocol must be configured on the interface and also on the switch.

This section discusses the procedure to shutdown an interface when it receives incompatible BPDU packets. To configure an interface to shutdown upon receipt of incompatible BPDUs, a spanning-tree protocol may or may not be configured on the interface or switch.

To configure BPDU shutdown protection on interfaces:



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

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

```
user@switch> show ethernet-switching interfaces
Interface  State  VLAN members  Tag  Tagging  Blocking
ge-0/0/0.0  up    default                untagged unblocked
```

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

2. (Optional) Configure any spanning-tree protocol on the switch if not configured already. The Rapid Spanning Tree Protocol (RSTP) is configured in this procedure.

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



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

3. Enable RSTP on a specific interface—for example, **ge-0/0/0.0**:

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

4. (Optional) Ensure that the spanning-tree protocol is configured on the **ge-0/0/0.0** interface:

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

Interface	Port ID	Designated	Designated	Port	State	Role
-----------	---------	------------	------------	------	-------	------

		port ID	bridge ID	Cost		
ge-0/0/0.0	128:513	16:513	8192.841888af0681	20000	FWD	ROOT

In this output, the **ge-0/0/0.0** interface is displayed because a spanning-tree protocol is configured on this interface.

5. Enable the BPDU protection on the interface (**ge-0/0/0.0**) so that the interface shuts down on receiving incompatible BPDU packets:

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

6. Commit the configuration change:

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

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

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

```
user@switch> show ethernet-switching interfaces
Interface  State  VLAN members  Tag  Tagging  Blocking
ge-0/0/0.0  down  default      Tag  untagged  Disabled by
                                         bpdu-control
```

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

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

Configuring BPDU Protection for Interfaces (BPDU Drop Mode)

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

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



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

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

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

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

Or,

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

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

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



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

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

```
user@switch> show ethernet-switching interfaces
Interface  State  VLAN members      Tag  Tagging  Blocking
ge-0/0/0.0  up    default           Tag  untagged unblocked
```

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

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

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

4. Commit the configuration:

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

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

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

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


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

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

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

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

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/0.0	128:513	16:513	8192.841888af0681	20000	DIS	DIS

Related Documentation

- [Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133](#)
- [Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157](#)
- [Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167](#)

Configuring BPDU Protection on All Edge Ports

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

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

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

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

2. Verify BPDU protection for edge ports:

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

- Related Documentation**
- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)
 - [Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35](#)
 - [Understanding BPDU Protection on All Edge Ports of the Bridge on page 136](#)

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.

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.

- Related Documentation**
- [Example: Configuring BPDU Protection on Switch Edge Interfaces to Prevent STP Miscalculations on page 152](#)
 - [Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 161](#)
 - [Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133](#)

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 bpdur-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 bpdur-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.

Related Documentation

- [Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133](#)
- [Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157](#)
- [Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167](#)

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

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

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

- [Requirements on page 148](#)
- [Overview on page 148](#)
- [Configuration on page 149](#)
- [Verification on page 150](#)

Requirements

This example uses the following hardware and software components:

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

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

- RSTP enabled on the routers.

Overview

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

[Figure 4 on page 149](#) shows the topology for this example. In this example, Router 1 and Router 2 are configured for RSTP and create a loop-free topology. The interfaces on Router 2 are edge access ports which frequently receive outside BPDUs generated by PC applications.

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

Topology

Figure 4: BPDU Protection Topology

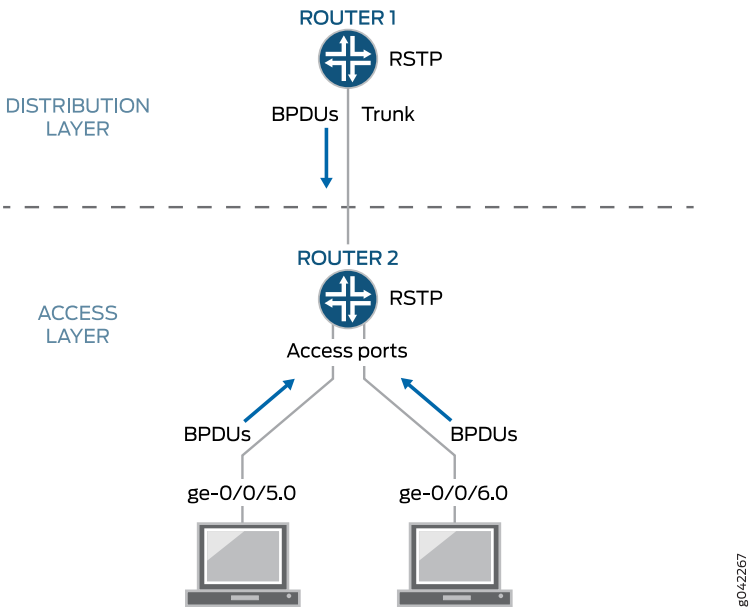


Table 10 on page 149 describes the components that are configured for BPDU protection.

Table 10: Components of the Topology for Configuring BPDU Protection on MX Series Routers

Property	Settings
Router 1 (Distribution Layer)	Router 1 is connected to Router 2 on a trunk interface.
Router 2 (Access Layer)	Router 2 has these access ports that require BPDU protection: <ul style="list-style-type: none">ge-0/0/5.0ge-0/0/6.0

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

Configuration

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

Router 2 `set protocols rstp interface ge-0/0/5.0 edge`
`set protocols rstp interface ge-0/0/6.0 edge`
`set protocols rstp bpdu-block-on-edge`

Configuring Router 2

Step-by-Step Procedure

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

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

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

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

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

Results

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

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

Verification

Verify that the configuration is working properly.

- [Displaying the Interface State Before BPDU Protection Is Triggered on page 150](#)
- [Verifying That BPDU Protection Is Working Correctly on page 151](#)

Displaying the Interface State Before BPDU Protection Is Triggered

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

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

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

Spanning tree interface parameters for instance 0

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

[output truncated]

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

Verifying That BPDU Protection Is Working Correctly

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

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

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

Spanning tree interface parameters for instance 0

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

[output truncated]

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

Disabling the BPDU protection configuration on an interface does not automatically re-enable the interface. However, if the **disable-timeout** statement has been included in the BPDU configuration, the interface does return to service after the timer expires. Otherwise, you must use the operational mode command **clear error bpdv interface *interface-name*** to unblock and re-enable the interface.

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

- Related Documentation**
- [Configuring a Spanning-Tree Instance Interface as an Edge Port for Faster Convergence on page 42](#)

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

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

This example configures BPDU protection on an EX Series switch that uses RSTP. The upstream configuration is done on the edge interfaces, where outside BPDUs are often received from other devices:

- [Requirements on page 152](#)
- [Overview and Topology on page 153](#)
- [Configuration on page 154](#)
- [Verification on page 155](#)

Requirements

This example uses the following software and hardware components:

- Two EX Series switches in an RSTP topology
- Junos OS Release 13.2X50-D10 or later or later for EX Series or QFX Series switches

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

- RSTP enabled on the switches.



NOTE: By default, RSTP is enabled on all EX Series switches.

Overview and Topology

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

Figure 5 on page 153 shows the topology for this example. In this example, Switch 1 and Switch 2 are configured for RSTP and create a loop-free topology. The interfaces on Switch 2 are edge access ports—edge access ports frequently receive outside BPDUs generated by PC applications.

This example configures interface **ge-0/0/5** and interface **ge-0/0/6** as edge ports on Switch 2, and then configures BPDU protection on those ports. With BPDU protection enabled, these interfaces shut down when they encounter an outside BPDU sent by the PCs connected to Switch 2.

Figure 5: BPDU Protection Topology

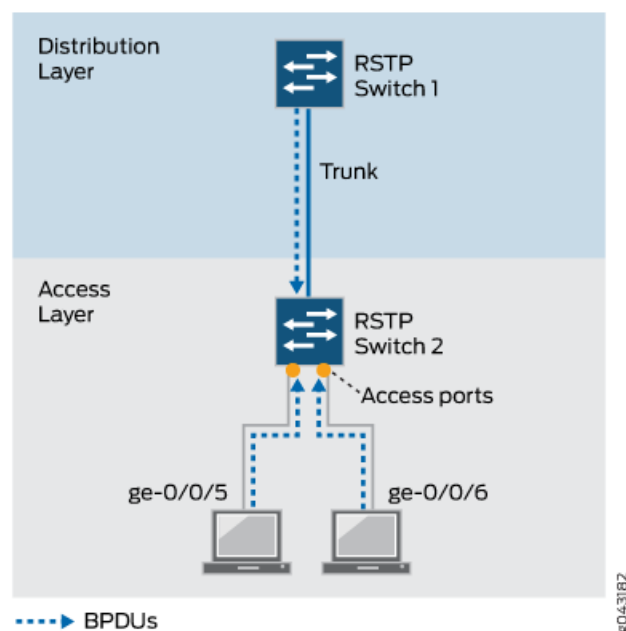


Table 11 on page 154 shows the components that will be configured for BPDU protection.

Table 11: Components of the Topology for Configuring BPDU Protection on EX Series Switches

Property	Settings
Switch 1 (Distribution Layer)	Switch 1 is connected to Switch 2 on a trunk interface.
Switch 2 (Access Layer)	Switch 2 has these access ports that require BPDU protection: <ul style="list-style-type: none"> • <code>ge-0/0/5</code> • <code>ge-0/0/6</code>

This configuration example uses RSTP topology. You also can configure BPDU protection for MSTP topologies at the `[edit protocols mstp]` hierarchy level.

Configuration

To configure BPDU protection on two access interfaces:

CLI Quick Configuration

Quickly configure RSTP on the two Switch 2 interfaces, and then configure BPDU protection on all edge ports on Switch 2 by copying the following commands and pasting them into the switch terminal window:



NOTE: This example configures BPDU protection on specific interfaces. Starting with Junos OS Release 15.1 for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can also configure BPDU protection globally on all spanning tree interfaces. See [“Configuring BPDU Protection on Switch Spanning Tree Interfaces” on page 139](#) for additional information.

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

Step-by-Step Procedure

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

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

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

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

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

Results Check the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- [Displaying the Interface State Before BPDU Protection Is Triggered on page 155](#)
- [Verifying That BPDU Protection Is Working Correctly on page 155](#)

Displaying the Interface State Before BPDU Protection Is Triggered

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

Action Use the operational mode command:

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

Spanning tree interface parameters for instance 0

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/0	128:513	128:513	32768.0019e2503f00	20000	BLK	DIS
ge-0/0/1	128:514	128:514	32768.0019e2503f00	20000	BLK	DIS
ge-0/0/2	128:515	128:515	32768.0019e2503f00	20000	BLK	DIS
ge-0/0/3	128:516	128:516	32768.0019e2503f00	20000	FWD	DESG
ge-0/0/4	128:517	128:517	32768.0019e2503f00	20000	FWD	DESG
ge-0/0/5	128:518	128:518	32768.0019e2503f00	20000	FWD	DESG
ge-0/0/6	128:519	128:519	32768.0019e2503f00	20000	FWD	DESG

[output truncated]

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

Verifying That BPDU Protection Is Working Correctly

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

Action Use the operational mode command:

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

Spanning tree interface parameters for instance 0

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/0	128:513	128:513	32768.0019e2503f00	20000	BLK	DIS
ge-0/0/1	128:514	128:514	32768.0019e2503f00	20000	BLK	DIS
ge-0/0/2	128:515	128:515	32768.0019e2503f00	20000	BLK	DIS
ge-0/0/3	128:516	128:516	32768.0019e2503f00	20000	FWD	DESG
ge-0/0/4	128:517	128:517	32768.0019e2503f00	20000	FWD	DESG
ge-0/0/5	128:518	128:518	32768.0019e2503f00	20000	BLK	DIS
(Bpdu-Incon)						
ge-0/0/6	128:519	128:519	32768.0019e2503f00	20000	BLK	DIS
(Bpdu-Incon)						
ge-0/0/7	128:520	128:1	16384.00aabbcc0348	20000	FWD	ROOT
ge-0/0/8	128:521	128:521	32768.0019e2503f00	20000	FWD	DESG

[output truncated]

Meaning When BPDUs are sent from the PCs to interface **ge-0/0/5** and interface **ge-0/0/6** on Switch 2, the output from the operational mode command **show spanning-tree interface** shows that the interfaces have transitioned to a BPDU inconsistent state. The BPDU inconsistent state causes the interfaces to shut down.

Disabling the BPDU protection configuration on an interface does not automatically reenables the interface. However, if the **disable-timeout** statement has been included in the BPDU configuration, the interface does return to service after the timer expires. Otherwise, you must use the operational mode command **clear error bpdu** to unblock and reenables the interface.

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

Release History Table

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

Related Documentation

- [Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133](#)
- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
- [Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167](#)

- [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 184](#)
- [Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches on page 251](#)

Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches

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

This example configures BPDU protection on an EX Series switch that uses RSTP. The upstream configuration is done on the edge interfaces, where outside BPDUs are often received from other devices:

- [Requirements on page 157](#)
- [Overview and Topology on page 157](#)
- [Configuration on page 159](#)
- [Verification on page 159](#)

Requirements

This example uses the following hardware and software components:

- Two EX Series switches in an RSTP topology
- Junos OS Release 9.1 or later for EX Series switches

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

- RSTP enabled on the switches.



NOTE: By default, RSTP is enabled on all EX Series switches.

Overview and Topology

The switches, being in an RSTP topology, support a loop-free network through the exchange of BPDUs. Receipt of outside BPDUs in an STP, RSTP, or MSTP topology, however, can lead to network outages by triggering an STP misconfiguration. To prevent such outages, enable BPDU protection on STP interfaces that could receive outside

BPDUs. If an outside BPDU is received on a BPDU-protected interface, the interface shuts down to prevent the outside BPDU from accessing the STP interface.

Figure 5 on page 153 shows the topology for this example. In this example, Switch 1 and Switch 2 are configured for RSTP and create a loop-free topology. The interfaces on Switch 2 are edge access ports—edge access ports frequently receive outside BPDUs generated by PC applications.

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

Figure 6: BPDU Protection Topology

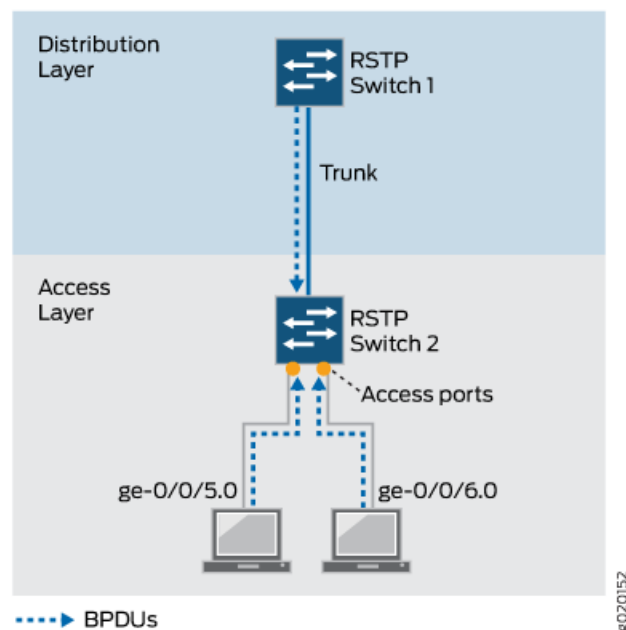


Table 11 on page 154 shows the components that will be configured for BPDU protection.

Table 12: Components of the Topology for Configuring BPDU Protection on EX Series Switches

Property	Settings
Switch 1 (Distribution Layer)	Switch 1 is connected to Switch 2 on a trunk interface.
Switch 2 (Access Layer)	Switch 2 has these access ports that require BPDU protection: <ul style="list-style-type: none"> • ge-0/0/5.0 • ge-0/0/6.0

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

Configuration

To configure BPDU protection on two access interfaces:

CLI Quick Configuration Quickly configure RSTP on the two Switch 2 interfaces, and then configure BPDU protection on all edge ports on Switch 2 by copying the following commands and pasting them into the switch terminal window:

```
[edit]
set protocols rstp interface ge-0/0/5.0 edge
set protocols rstp interface ge-0/0/6.0 edge
set protocols rstp bpd-block-on-edge
```

Step-by-Step Procedure To configure RSTP on the two Switch 2 interfaces, and then configure BPDU protection:

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

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

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

```
[edit protocols rstp]
user@switch# set bpd-block-on-edge
```

Results Check the results of the configuration:

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

Verification

To confirm that the configuration is working properly:

- [Displaying the Interface State Before BPDU Protection Is Triggered on page 159](#)
- [Verifying That BPDU Protection Is Working Correctly on page 160](#)

Displaying the Interface State Before BPDU Protection Is Triggered

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

Action Use the operational mode command:

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

Spanning tree interface parameters for instance 0

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

[output truncated]

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

Verifying That BPDU Protection Is Working Correctly

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

Action Use the operational mode command:

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

Spanning tree interface parameters for instance 0

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

[output truncated]

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

Disabling the BPDU protection configuration on an interface does not automatically re-enable the interface. However, if the `disable-timeout` statement has been included in the BPDU configuration, the interface does return to service after the timer expires. Otherwise, you must use the operational mode command `clear bpdu-error` to unblock and re-enable the interface.

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

Related Documentation

- [Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133](#)
- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
- [Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167](#)
- [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 184](#)
- [Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches on page 251](#)

Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches



NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see [“Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches” on page 167](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

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

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

- [Requirements on page 162](#)
- [Overview and Topology on page 162](#)
- [Configuration on page 163](#)
- [Verification on page 164](#)

Requirements

This example uses the following software and hardware components:

- One EX Series switch in an RSTP topology
- One EX Series switch that is not in any spanning-tree topology
- Junos OS Release 13.2X50-D10 or later or later for EX Series switches

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

- Ensured that RSTP is operating on Switch 1.
- Disabled RSTP on Switch 2



NOTE: By default, RSTP is enabled on all EX Series switches.

Overview and Topology

EX Series switches provide Layer 2 loop prevention through Rapid Spanning Tree protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). All spanning-tree protocols use a special type of frame called a BPDU to communicate. Other devices also use BPDUs—PC bridging applications, for example, generate their own BPDUs. These different BPDUs are not compatible. When BPDUs generated by spanning-tree protocols are transmitted to a device that uses another type of BPDU, they can cause problems on the device. Similarly, if switches within a spanning-tree topology receive BPDUs from other devices, network outages can occur because of the miscalculations caused by the outside BPDUs. Therefore, you must configure BPDU protection on interfaces in a spanning-tree topology to avoid network outages.

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

[Figure 5 on page 153](#) shows the topology for this example. Switch 1 and Switch 2 are connected through a trunk interface. Switch 1 is configured for RSTP and Switch 2 does not have a spanning-tree protocol configured on it.

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



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

Figure 7: BPDU Protection Topology

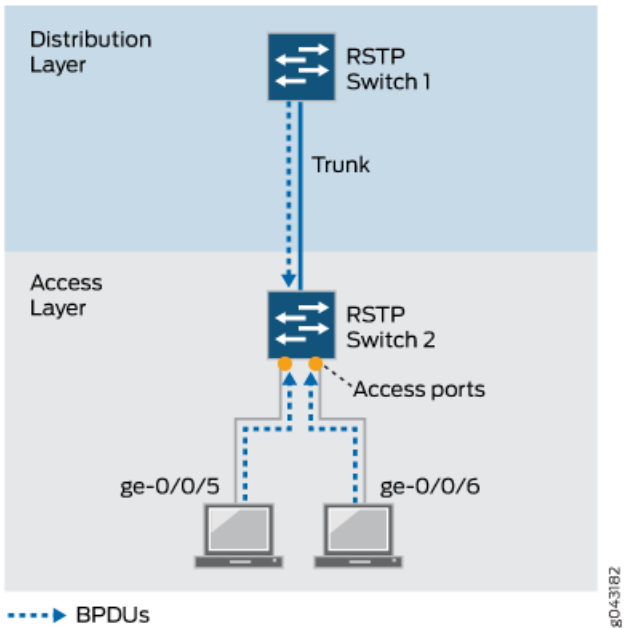


Table 13 on page 163 shows the components that will be configured for BPDU protection.

Table 13: Components of the Topology for Configuring BPDU Protection on EX Series Switches

Property	Settings
Switch 1 (Distribution Layer)	Switch 1 is connected to Switch 2 through a trunk interface. Switch 1 is configured for RSTP.
Switch 2 (Access Layer)	Switch 2 has two downstream access ports connected to laptops: <ul style="list-style-type: none">• ge-0/0/5• ge-0/0/6

Configuration

To configure BPDU protection on the interfaces:

CLI Quick Configuration This configuration causes the interface to automatically shutdown if it receives BPDUs. To quickly configure BPDU protection on Switch 2, copy the following commands and paste them into the switch terminal window:



NOTE: This example configures BPDU protection on specific interfaces. However, starting with Junos OS Release 15.1 for EX Series and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can configure BPDU protection globally on all spanning tree interfaces. See [“Configuring BPDU Protection on Switch Spanning Tree Interfaces” on page 139](#) for additional information.

```
[edit]
user@switch# set protocols layer2-control bpdv-block interface ge-0/0/5
[edit]
user@switch# set protocols layer2-control bpdv-block interface ge-0/0/6
```

Step-by-Step Procedure To configure BPDU protection for automatic shutdown.

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


```
[edit protocol layer 2]
user@switch# set bpdv-block interface ge-0/0/5
```
2. To shutdown the BPDU interface on the downstream interface **ge-0/0/6** on Switch 2:


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

Results Check the results of the configuration:

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

Verification

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

- [Displaying the Interface State Before BPDU Protection Is Triggered on page 165](#)
- [Verifying That BPDU Shutdown Protection Is Working Correctly on page 165](#)

Displaying the Interface State Before BPDU Protection Is Triggered

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

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

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

```
Physical interface: ge-0/0/5, Enabled, Physical link is Down
  Interface index: 659, SNMP ifIndex: 639, Generation: 161
  Link-level type: Ethernet, MTU: 1514, MRU: 0, Link-mode: Auto, Speed: Auto,
  BPDU Error: Detected, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled,

  Remote fault: Online, Media type: Copper,
  IEEE 802.3az Energy Efficient Ethernet: Disabled
  Device flags   : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues    : 12 supported, 12 maximum usable queues
  Hold-times    : Up 0 ms, Down 0 ms
```

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

Verifying That BPDU Shutdown Protection Is Working Correctly

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

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

```
user@switch> show interfaces extensive ge-0/0/5
Physical interface: ge-0/0/5, Enabled, Physical link is Down
  Interface index: 659, SNMP ifIndex: 639, Generation: 161
  Link-level type: Ethernet, MTU: 1514, MRU: 0, Link-mode: Auto, Speed: Auto,
  BPDU Error: Detected, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Disabled, Auto-negotiation: Enabled,

  Remote fault: Online, Media type: Copper,
  IEEE 802.3az Energy Efficient Ethernet: Disabled
  Device flags   : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues    : 12 supported, 12 maximum usable queues
  Hold-times    : Up 0 ms, Down 0 ms
```

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

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

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

**Related
Documentation**

- [Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133](#)
- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
- [Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157](#)
- [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 184](#)
- [Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches on page 251](#)

Example: Blocking BPDUs on Aggregated Ethernet Interface for 600 Seconds

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

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

Related Documentation

- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)
- [Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35](#)
- [Understanding BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 134](#)
- [Understanding BPDU Protection on All Edge Ports of the Bridge on page 136](#)
- [Checking the Status of Spanning-Tree Instance Interfaces on page 272](#)
- [Clearing the Blocked Status of a Spanning-Tree Instance Interface on page 272](#)

Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches

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



NOTE: The BPDU drop feature can be specified only on interfaces on which no spanning-tree protocol is configured.

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

- [Requirements on page 168](#)
- [Overview and Topology on page 168](#)

- [Configuration on page 170](#)
- [Verification on page 172](#)

Requirements

This example uses the following hardware and software components:

- One EX Series switch in an RSTP topology
- One EX Series switch that is not in any spanning-tree topology
- Junos OS Release 9.1 or later for EX Series switches

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

- Ensured that RSTP is operating on Switch 1.
- Disabled or enabled RSTP on Switch 2 (depending on the configuration that you plan to implement.)

If you want to enable the BPDU shutdown feature, then it is optional to disable spanning-tree protocols on the interface.



NOTE: By default, RSTP is enabled on all EX Series switches.

Overview and Topology

EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). All spanning-tree protocols use a special type of frame called a BPDU to communicate. Other devices also use BPDUs—PC bridging applications, for example, generate their own BPDUs. These different BPDUs are not compatible. When BPDUs generated by spanning-tree protocols are transmitted to a device that uses another type of BPDU, they can cause problems on the device. Similarly, if switches within a spanning-tree topology receive BPDUs from other devices, network outages can occur because of the miscalculations caused by the outside BPDUs. Therefore, you must configure BPDU protection on interfaces in a spanning-tree topology to avoid network outages.

This example explains how to block outside BPDUs from reaching a switch interface connected to devices that are not part of the STP topology. This example addresses two scenarios. In the first scenario, an interface is shutdown when it encounters an outside BPDU. In the second scenario, an interface drops only BPDU packets while retaining the status of the interface as up and allowing all other traffic to pass through the interface.

[Figure 5 on page 153](#) shows the topology for this example. Switch 1 and Switch 2 are connected through a trunk interface. Switch 1 is configured for RSTP while Switch 2 has a spanning-tree protocol configured on it for the first scenario, and does not have a spanning-tree protocol configured on it for the second scenario.

In the first scenario, this example configures downstream BPDU protection on Switch 2 interfaces **ge-0/0/5.0** and **ge-0/0/6.0** when the default spanning-tree protocol (RSTP) is not disabled on these interfaces. When BPDU protection is enabled with the **shutdown** statement, the switch interfaces will shut down if BPDUs generated by the laptops attempt to access Switch 2.

In the second scenario, this example configures downstream BPDU protection on Switch 2 interfaces **ge-0/0/5.0** and **ge-0/0/6.0** when the default spanning-tree protocol (RSTP) is disabled on these interfaces. When BPDU protection is enabled with the **drop** statement, the switch interfaces drop only the BPDUs while allowing remaining traffic to pass through and retaining their status as up if BPDUs generated by the laptops attempt to access Switch 2.



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

Figure 8: BPDU Protection Topology

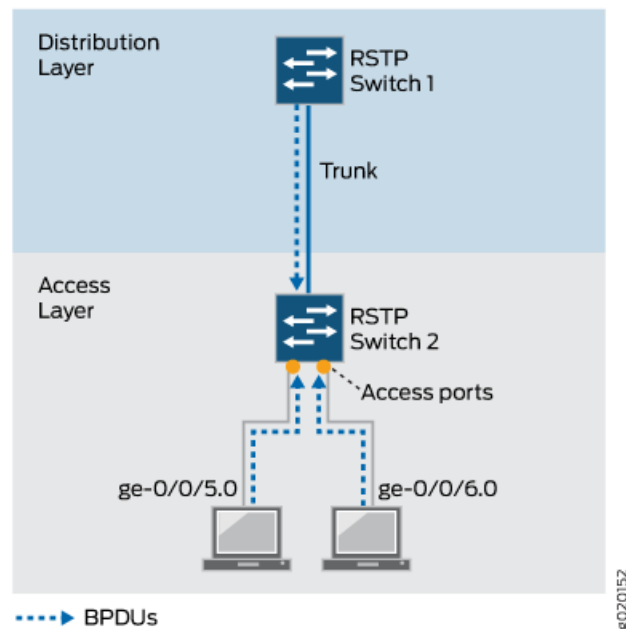


Table 13 on page 163 shows the components that will be configured for BPDU protection.

Table 14: 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: <ul style="list-style-type: none"> • <code>ge-0/0/5.0</code> • <code>ge-0/0/6.0</code>

Configuration

To configure BPDU protection on the interfaces:

CLI Quick Configuration

This is the first scenario that explains configuration for the **shutdown** statement. To quickly configure BPDU protection on Switch 2 for the **shutdown** statement, copy the following commands and paste them into the switch terminal window:

```
[edit]
user@switch# set ethernet-switching-options bpdu-block interface ge-0/0/5.0 shutdown
[edit]
user@switch# set ethernet-switching-options bpdu-block interface ge-0/0/6.0 shutdown
```

Step-by-Step Procedure

To configure BPDU protection for the **shutdown** statement:

1. Configure the BPDU **shutdown** statement on the downstream interface **ge-0/0/5.0** on Switch 2:

```
[edit ethernet-switching-options]
user@switch# set bpdu-block interface ge-0/0/5.0 shutdown
```

2. Configure the BPDU **shutdown** statement on the downstream interface **ge-0/0/6.0** on Switch 2:

```
[edit ethernet-switching-options]
user@switch# set bpdu-block interface ge-0/0/6.0 shutdown
```

Results Check the results of the configuration:

```
user@switch> show ethernet-switching-options
bpdu-block {
  interface ge-0/0/5.0 {
    shutdown;
  }
  interface ge-0/0/6.0 {
    shutdown;
  }
}
```

CLI Quick Configuration This is the second scenario that explains configuration for the **drop** statement. To quickly configure BPDU protection on Switch 2 for the **drop** statement, copy the following commands and paste them into the switch terminal window:

```
[edit]
user@switch# set protocols rstp interface ge-0/0/5.0 disable
user@switch# set protocols rstp interface ge-0/0/6.0 disable
user@switch# set ethernet-switching-options bpdu-block interface ge-0/0/5.0 drop
user@switch# set ethernet-switching-options bpdu-block interface ge-0/0/6.0 drop
```



NOTE: You can also disable RSTP globally using the `delete protocols rstp`, the `set protocols rstp disable`, or the `set protocols rstp interface all disable` command.

Step-by-Step Procedure To configure BPDU protection for the **drop** statement:

1. Disable RSTP on both the interfaces **ge-0/0/5.0** and **ge-0/0/6.0** interfaces:

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

2. Configure the BPDU **drop** statement on the downstream interface **ge-0/0/5.0** on Switch 2:

```
[edit ethernet-switching-options]
user@switch# set bpdu-block interface ge-0/0/5.0 drop
```

3. Configure the BPDU **drop** statement on the downstream interface **ge-0/0/6.0** on Switch 2:

```
[edit ethernet-switching-options]
user@switch# set bpdu-block interface ge-0/0/6.0 drop
```

Results Check the results of the configuration:

```
user@switch> show protocols rstp
interface ge-0/0/5.0 {
  disable;
}
interface ge-0/0/6.0 {
  disable;
}
user@switch> show ethernet-switching-options
bpdu-block {
  interface ge-0/0/5.0 {
    drop;
  }
  interface ge-0/0/6.0 {
    drop;
  }
}
```

```
    }
}
```

Verification

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

- [Displaying the Interface State Before BPDU Protection Is Triggered on page 172](#)
- [Verifying That BPDU Shutdown Protection Is Working Correctly on page 172](#)
- [Verifying That BPDU Drop Protection Is Working Correctly on page 173](#)

Displaying the Interface State Before BPDU Protection Is Triggered

Purpose Before any BPDUs can be received on Switch 2 on either interface **ge-0/0/5.0** or interface **ge-0/0/6.0**, confirm the state of those interfaces.

Action Use the operational mode command **show ethernet-switching interfaces**:

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

Interface	State	VLAN members	Tag	Tagging	Blocking
ge-0/0/5.0	up	default		untagged	unblocked
ge-0/0/6.0	up	default		untagged	unblocked

Meaning The output from the operational mode command **show ethernet-switching interfaces** shows that **ge-0/0/5.0** and interface **ge-0/0/6.0** are **up** and **unblocked**.

Verifying That BPDU Shutdown Protection Is Working Correctly

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

Action Issue **show ethernet-switching interfaces** to see what happened when the BPDUs reached the two interfaces configured for BPDU protection on Switch 2:

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

Interface	State	VLAN members	Tag	Tagging	Blocking
ge-0/0/5.0	down	default		untagged	Disabled by bpdu-control
ge-0/0/6.0	down	default		untagged	Disabled by bpdu-control

Meaning When the BPDUs sent from laptops reached interfaces **ge-0/0/5.0** and **ge-0/0/6.0** on Switch 2, the interfaces transitioned to a BPDU inconsistent state, shutting down the two interfaces to prevent BPDUs from reaching the laptops.

You need to re-enable the blocked interfaces. There are two ways to do this. If you included the statement **disable-timeout** in the BPDU configuration, the interface returns

to service after the timer expires. Otherwise, use the operational mode command `clear bpdur-error` to unblock and re-enable `ge-0/0/5.0` and `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.

If BPDUs reach the downstream interfaces on Switch 2 again, BPDU protection is triggered again and the interfaces shut down. In such cases, you must find and repair the misconfiguration that is sending BPDUs to interfaces `ge-0/0/5.0` and `ge-0/0/6.0`.

Verifying That BPDU Drop Protection Is Working Correctly

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

Action Issue `show ethernet-switching interfaces` to see what happened when the BPDUs reached the two interfaces configured for BPDU protection on Switch 2:

```
user@switch> show ethernet-switching interfaces
Interface  State  VLAN members  Tag  Tagging  Blocking
ge-0/0/5.0  up    default          Tag  untagged  unblocked-xSTP bpdur
                                     filter enabled
ge-0/0/6.0  up    default          Tag  untagged  unblocked-xSTP bpdur
                                     filter enabled
```

Meaning When the BPDUs sent from laptops reached interfaces `ge-0/0/5.0` and `ge-0/0/6.0` on Switch 2, the interfaces dropped those BPDUs to prevent them from reaching Switch 2, and the state of both the interfaces is `up`.

- Related Documentation**
- [Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133](#)
 - [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
 - [Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157](#)
 - [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 184](#)
 - [Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches on page 251](#)

CHAPTER 8

Configuring Loop Protection for Spanning-Tree Protocols

- [Understanding Loop Protection for Spanning-Tree Instance Interfaces on page 175](#)
- [Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 176](#)
- [Understanding Spanning Tree Protocol Used for Eliminating Bridge Loops in Ethernet LANs on page 177](#)
- [Example: Enabling Loop Protection for Spanning-Tree Protocols on page 183](#)
- [Configuring Loop Protection for a Spanning-Tree Instance Interface on page 183](#)
- [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 184](#)
- [Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches on page 189](#)

Understanding Loop Protection for Spanning-Tree Instance Interfaces

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

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

Ideally, a spanning-tree protocol bridge port remains blocked as long as a superior alternate path to the root bridge exists for a connected LAN segment. This designated port is determined by receiving superior BPDUs from a peer on that port. When other ports no longer receive BPDUs, the spanning-tree protocol considers the topology to be loop free. However, if a blocked or alternate port moves into a forwarding state, this creates a loop.

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

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

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



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

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

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

**Related
Documentation**

- [Configuring Loop Protection for a Spanning-Tree Instance Interface on page 183](#)
- [Example: Enabling Loop Protection for Spanning-Tree Protocols on page 183](#)

Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches

Juniper Networks EX Series Ethernet Switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), and Multiple Spanning Tree Protocol (MSTP). 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.

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.

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 that an interface can be configured for either loop protection or root protection, but not for both.

**Related
Documentation**

- [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 184](#)
- [Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 246](#)
- [Understanding MSTP on page 48](#)
- [Understanding RSTP on page 21](#)
- [Understanding STP on page 26](#)
- [Understanding VSTP on page 29](#)
- [Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133](#)

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

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

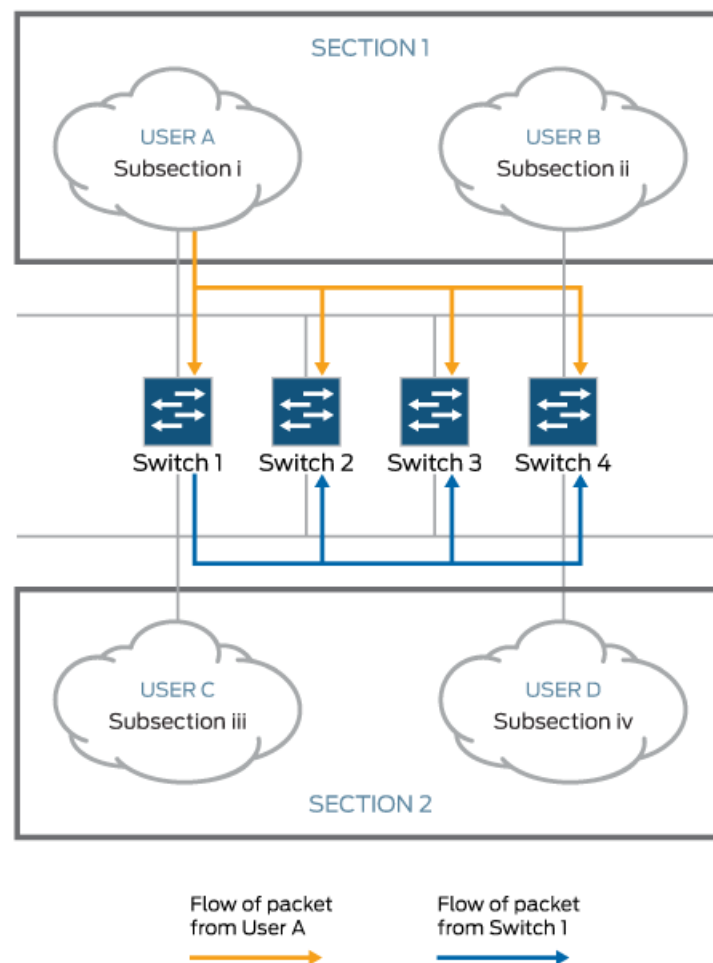
The sections describe bridge loops and how STP helps eliminate them.

- [Understanding Bridge Loops on page 178](#)
- [How STP Helps Eliminate Loops on page 179](#)
- [Types of Spanning-Tree Protocols Supported on page 181](#)

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 9 on page 178](#)). 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 9: Formation of Bridge Loops



When the switches are powered on, the bridge tables are empty. If User A in Subsection i tries to send a single packet Packet 1 to User D in Subsection iv, all the switches, which

are in listening mode, receive the packet. The switches make an entry in their respective bridging tables, as shown in the following table:

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

At this point, the switches do not know where Subsection iv is, and the packet is forwarded to all the ports except the source port (which results in flooding of the packet). In this example, after Subsection 1 sends the packet, the switches receive the packet on the ports facing Section 1. As a result, they start forwarding the packet through the ports facing Section 2. Which switch gets the first chance to send out the packet depends on the network configuration. In this example, suppose Switch 1 transmits the packet first. Because it received the packet from Section 1, it floods the packet toward Section 2. Similarly, Switches 2, 3, and 4, which are also in listening mode, receive the same packet from Switch 1 (originally sent from Section 1) on the ports facing Section 2. They readily update their bridging tables with incorrect information, as shown in the following table:

Bridge 1	Bridge 2	Bridge 3	Bridge 4
ID Port Facing Direction	ID Port Facing Direction	ID Port Facing Direction	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 9 on page 178](#), Switch 1 has information that the packet came from Subsection i in Section 1, whereas all other switches have incorrect information that the same packet came from Section 2.

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

Bridge 1	Bridge 2	Bridge 3	Bridge 4
ID Port Facing Direction	ID Port Facing Direction	ID Port Facing Direction	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

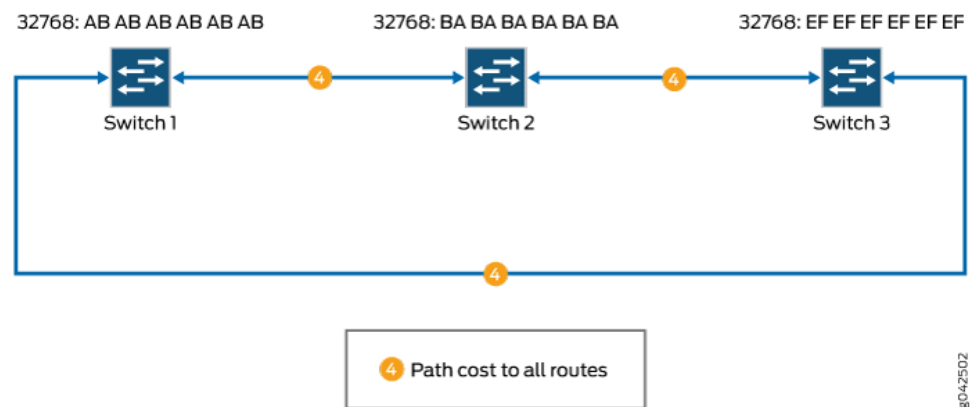
Spanning Tree Protocol helps eliminate loops in a network by turning off additional routes that can create a loop. The blocked routes are enabled automatically if the primary path gets deactivated.

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 10 on page 180](#)). 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.

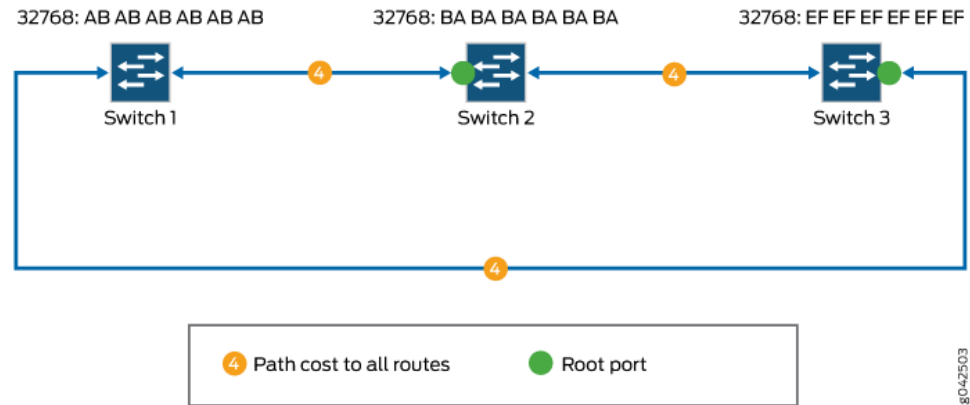
Figure 10: Simple Network with Redundant Links



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

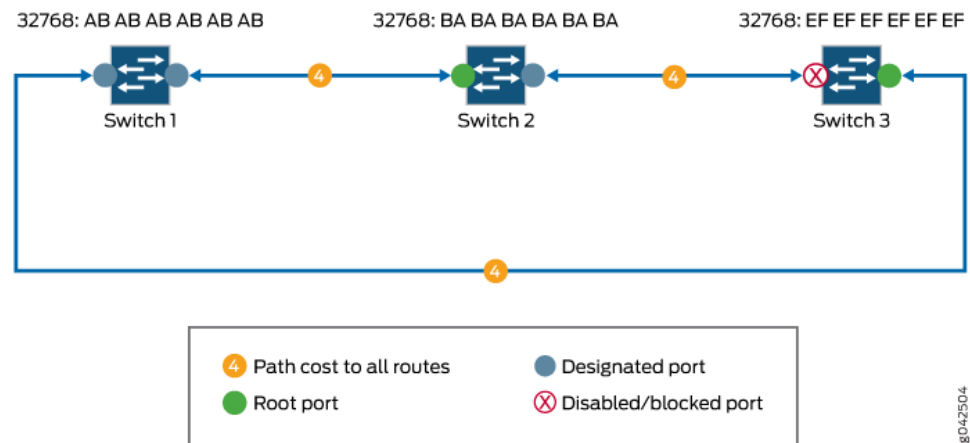
1. *Elects a root bridge (or switch).* To elect a root switch, STP uses the bridge ID. The bridge ID is 8 bytes in length and consists of two parts. The first part is 2 bytes of information known as bridge priority. The default bridge priority is 32,768. In this example, the default value is used for all the switches. The remaining 6 bytes consist of the MAC address of the switch. In this example, Switch 1 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 11 on page 181](#). Similarly, for Switch 3, the root port is the one that uses the direct path from Switch 1.

Figure 11: 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 12 on page 181](#), the designated ports are marked.

Figure 12: Selecting Designated Ports and Blocking Redundant Paths



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

Types of Spanning-Tree Protocols Supported

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

A spanning-tree protocol is a Layer 2 control protocol (L2CP) that calculates the best path through a switched network containing redundant paths. A spanning-tree protocol uses bridge protocol data unit (BPDU) data frames to exchange information with other switches. A spanning-tree protocol uses the information provided by the BPDUs to elect

a root bridge, identify root ports for each switch, identify designated ports for each physical LAN segment, and prune specific redundant links to create a loop-free tree topology. The resulting tree topology provides a single active Layer 2 data path between any two end stations.



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

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

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



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 {
      bpdn-timeout-action block;
    }
  }
}
```



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

Related Documentation

- [Loop Protection for a Spanning-Tree Instance Interface](#)
- [Understanding Loop Protection for Spanning-Tree Instance Interfaces on page 175](#)

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 **bpdn-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 {
      bpdn-timeout-action (log | block);
    }
  }
}
```

- For all MSTP instances on a physical interface:

```
[edit]
protocols {
  mstp {
    interface interface-name {
```

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

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

Related Documentation

- [Understanding Loop Protection for Spanning-Tree Instance Interfaces on page 175](#)
- [Loop Protection for a Spanning-Tree Instance Interface](#)
- [Example: Enabling Loop Protection for Spanning-Tree Protocols on page 183](#)

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

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 on page 184](#)
- [Overview and Topology on page 185](#)
- [Configuration on page 186](#)
- [Verification on page 187](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches

- Three EX Series switches in an RSTP topology

Before you configure the interface for loop protection, be sure you have:

- RSTP operating on the switches.



NOTE: By default, RSTP is enabled on all EX Series switches.

Overview and Topology

A loop-free network in spanning-tree topologies is supported through the exchange of a special type of frame called bridge protocol data unit (BPDU). Peer STP applications running on the switch interfaces use BPDUs to communicate. Ultimately, the exchange of BPDUs determines which interfaces block traffic (preventing loops) and which interfaces become root ports and forward traffic.

A blocking interface can transition to the forwarding state in error if the interface stops receiving BPDUs from its designated port on the segment. Such a transition error can occur when there is a hardware error on the switch or software configuration error between the switch and its neighbor. When this happens, a loop opens up in the spanning tree. Loops in a Layer 2 topology cause broadcast, unicast, and multicast frames to continuously circle the looped network. As a switch processes a flood of frames in a looped network, its resources become depleted and the ultimate result is a network outage.



CAUTION: An interface can be configured for either loop protection or root protection, but not for both.

Three EX Series switches are displayed in [Figure 13 on page 186](#). In this example, they are configured for RSTP and create a loop-free topology. Interface **ge-0/0/6** is blocking traffic between Switch 3 and Switch 1; thus, traffic is forwarded through interface **ge-0/0/7** on Switch 2. BPDUs are being sent from the root bridge on Switch 1 to both of these interfaces.

This example shows how to configure loop protection on interface **ge-0/0/6** to prevent it from transitioning from a blocking state to a forwarding state and creating a loop in the spanning-tree topology.

Figure 13: Network Topology for Loop Protection

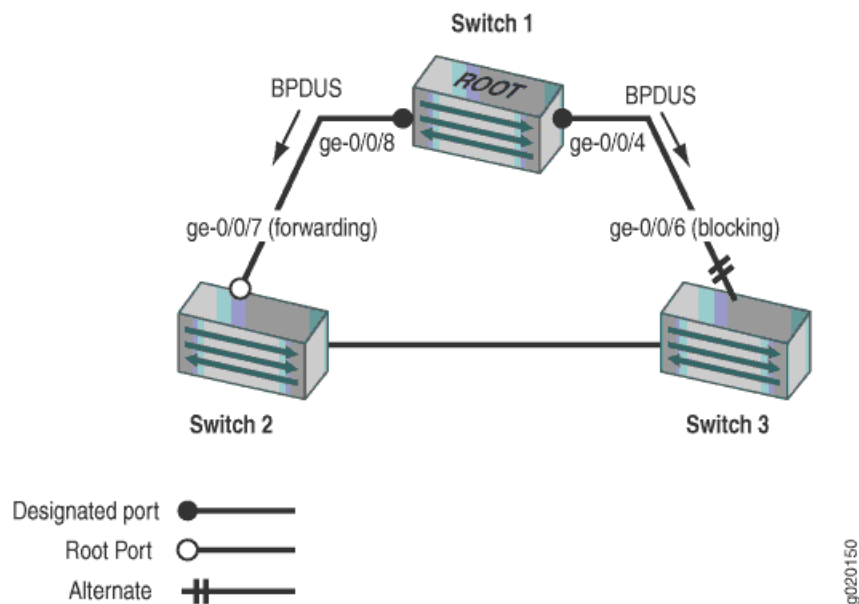


Table 15 on page 186 shows the components that will be configured for loop protection.

Table 15: Components of the Topology for Configuring Loop Protection on EX Series Switches

Property	Settings
Switch 1	Switch 1 is the root bridge.
Switch 2	Switch 2 has the root port ge-0/0/7 .
Switch 3	Switch 3 is connected to Switch 1 through interface ge-0/0/6 .

A spanning-tree topology contains ports that have specific roles:

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

This configuration example uses an RSTP topology. However, you also can configure loop protection for STP or MSTP topologies at the **[edit protocols (mstp | stp)]** hierarchy level.

Configuration

To configure loop protection on an interface:

CLI Quick Configuration To quickly configure loop protection on interface **ge-0/0/6**:

```
[edit]
set protocols rstp interface ge-0/0/6 bpdu-timeout-action block
```

Step-by-Step Procedure To configure loop protection:

1. Configure interface **ge-0/0/6** on Switch 3:

```
[edit protocols rstp]
user@switch# set interface ge-0/0/6 bpdu-timeout-action block
```

Results Check the results of the configuration:

```
user@switch> show configuration protocols rstp
interface ge-0/0/6.0 {
  bpdu-timeout-action {
    block;
  }
}
```

Verification

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

- [Displaying the Interface State Before Loop Protection Is Triggered on page 187](#)
- [Verifying That Loop Protection Is Working on an Interface on page 188](#)

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 port ID	Designated bridge ID	Port Cost	State	Role
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 port ID	Designated bridge ID	Port Cost	State	Role
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.

- Related Documentation**
- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
 - [Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches on page 251](#)
 - [Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157](#)
 - [Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167](#)
 - [Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 176](#)

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



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 184](#). 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 on page 189](#)
- [Overview and Topology on page 190](#)
- [Configuration on page 191](#)
- [Verification on page 192](#)

Requirements

This example uses the following software and hardware components:

- Junos OS Release 13.2X50-D10 or later or later for EX Series switches
- Three EX Series switches in an RSTP topology

Before you configure the interface for loop protection, be sure you have:

- RSTP operating on the switches.



NOTE: By default, RSTP is enabled on all EX Series switches.

Overview and Topology

A loop-free network in spanning-tree topologies is supported through the exchange of a special type of frame called bridge protocol data unit (BPDU). Peer STP applications running on the switch interfaces use BPDUs to communicate. Ultimately, the exchange of BPDUs determines which interfaces block traffic (preventing loops) and which interfaces become root ports and forward traffic.

A blocking interface can transition to the forwarding state in error if the interface stops receiving BPDUs from its designated port on the segment. Such a transition error can occur when there is a hardware error on the switch or software configuration error between the switch and its neighbor. When this happens, a loop opens up in the spanning tree. Loops in a Layer 2 topology cause broadcast, unicast, and multicast frames to continuously circle the looped network. As a switch processes a flood of frames in a looped network, its resources become depleted and the ultimate result is a network outage.



CAUTION: An interface can be configured for either loop protection or root protection, but not for both.

Three EX Series switches are displayed in [Figure 13 on page 186](#). In this example, they are configured for RSTP and create a loop-free topology. Interface **ge-0/0/6** is blocking traffic between Switch 3 and Switch 1; thus, traffic is forwarded through interface **ge-0/0/7** on Switch 2. BPDUs are being sent from the root bridge on Switch 1 to both of these interfaces.

This example shows how to configure loop protection on interface **ge-0/0/6** to prevent it from transitioning from a blocking state to a forwarding state and creating a loop in the spanning-tree topology.

Figure 14: Network Topology for Loop Protection

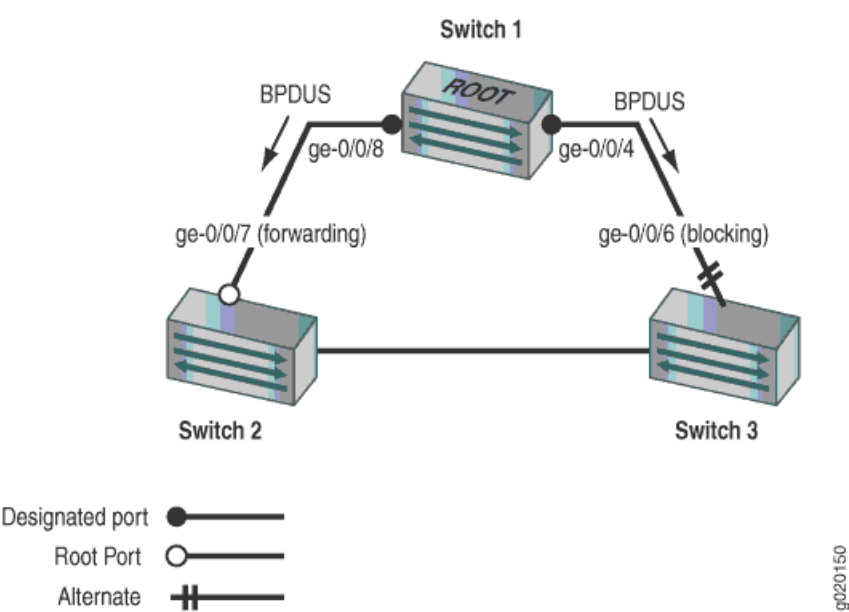


Table 15 on page 186 shows the components that will be configured for loop protection.

Table 16: 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 <code>ge-0/0/7</code> .
Switch 3	Switch 3 is connected to Switch 1 through interface <code>ge-0/0/6</code> .

A spanning-tree topology contains ports that have specific roles:

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

This configuration example uses an RSTP topology. However, you also can configure loop protection for MSTP topologies at the `[edit protocols mstp]` hierarchy level.

Configuration

To configure loop protection on an interface:

CLI Quick Configuration

To quickly configure loop protection on interface `ge-0/0/6`:

```
[edit]  
set protocols rstp interface ge-0/0/6 bpdn-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

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

- [Displaying the Interface State Before Loop Protection Is Triggered on page 192](#)
- [Verifying That Loop Protection Is Working on an Interface on page 193](#)

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 port ID	Designated bridge ID	Port Cost	State	Role
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 port ID	Designated bridge ID	Port Cost	State	Role
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 bpdv interface** on the switch. The interface recovers and transitions back to its original state as soon as it receives BPDUs.

- Related Documentation**
- [Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66](#)
 - [Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 176](#)

Configuring Network Regions for VLANs

- [Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195](#)
- [Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217](#)

Example: Configuring Network Regions for VLANs with MSTP on Switches



NOTE: This example uses Junos OS for EX Series and QFX 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 Network Regions for VLANs with MSTP on non-ELS EX Series Switches” on page 217](#). For ELS details, see *Using the Enhanced Layer 2 Software CLI*.

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 on page 196](#)
- [Overview and Topology on page 196](#)
- [Configuring MSTP on Switch 1 on page 199](#)
- [Configuring MSTP on Switch 2 on page 202](#)
- [Configuring MSTP on Switch 3 on page 205](#)
- [Configuring MSTP on Switch 4 on page 208](#)
- [Verification on page 210](#)

Requirements

This example uses the following software and hardware components:

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

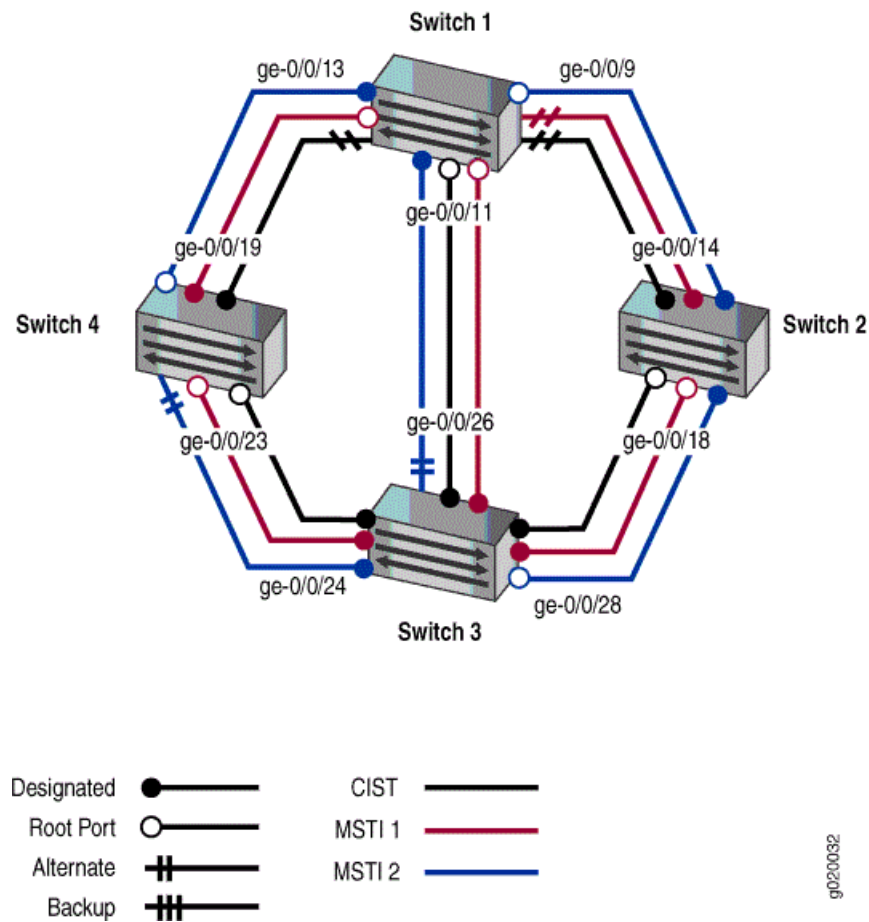
Before you configure the switches for MSTP, be sure you have:

- Installed and connected the four switches. See the hardware documentation for your switch.
- Performed the initial software configuration on all switches. See *Connecting and Configuring an EX Series Switch (CLI Procedure)* or *Connecting and Configuring an EX Series Switch (J-Web Procedure)*.

Overview and Topology

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

Figure 15: Network Topology for MSTP



The interfaces shown in [Figure 15 on page 197](#) will be configured for MSTP.



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

Table 17: Components of the Topology for Configuring MSTP on EX Series Switches

Property	Settings
Switch 1	<p>The following interfaces on Switch 1 are connected in this way:</p> <ul style="list-style-type: none"> • <code>ge-0/0/9</code> is connected to Switch 2 • <code>ge-0/0/13</code> is connected to Switch 4 • <code>ge-0/0/11</code> is connected to Switch 3
Switch 2	<p>The following interfaces on Switch 2 are connected in this way:</p> <ul style="list-style-type: none"> • <code>ge-0/0/14</code> is connected to Switch 1 • <code>ge-0/0/18</code> is connected to Switch 3

Table 17: Components of the Topology for Configuring MSTP on EX Series Switches (*continued*)

Property	Settings
Switch 3	<p>The following interfaces on Switch 3 are connected in this way:</p> <ul style="list-style-type: none"> • 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	<p>The following interfaces on Switch 4 are connected in this way:</p> <ul style="list-style-type: none"> • 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
MSTIs	1 2
MSTI region	region1

The topology in [Figure 15 on page 197](#) shows a common and internal spanning tree (CIST). The CIST is a single spanning tree connecting all devices in the network. The switch with the lowest bridge priority is elected as the root bridge of the CIST. You can control the election of the root bridge by configuring the bridge priority. Switch 3 is the root bridge of the CIST.

The ports in an MSTP topology have specific roles:

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

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

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

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

Configuring MSTP on Switch 1

CLI Quick Configuration To quickly configure interfaces and MSTP on Switch 1, 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 mstp configuration-name region1
set protocols mstp bridge-priority 16k
set protocols mstp interface ge-0/0/13 cost 1000
set protocols mstp interface ge-0/0/13 mode point-to-point
set protocols mstp interface ge-0/0/9 cost 1000
set protocols mstp interface ge-0/0/9 mode point-to-point
set protocols mstp interface ge-0/0/11 cost 1000
set protocols mstp interface ge-0/0/11 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 ge-0/0/11 cost 1000
set protocols mstp msti 2 bridge-priority 8k
set protocols mstp msti 2 vlan [30 40]
```

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 51](#) 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 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 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 ge-0/0/13 cost 1000
user@switch1# mstp interface ge-0/0/13 mode point-to-point
user@switch1# mstp interface ge-0/0/9 cost 1000
user@switch1# mstp interface ge-0/0/9 mode point-to-point
user@switch1# mstp interface ge-0/0/11 cost 1000
user@switch1# mstp interface ge-0/0/11 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 ge-0/0/11 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 {
  ge-0/0/13 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
  ge-0/0/9 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
  ge-0/0/11 {
    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 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;
}
msti 1 {
  bridge-priority 16k;
  vlan [ 10 20];
  interface ge-0/0/11 {
    cost 1000;
  }
}
msti 2 {
  bridge-priority 8k;
  vlan [ 30 40 ];
}
}
vlangs {
  voice-vlan {
    vlan-id 10;
  }
  employee-vlan {
    vlan-id 20;
  }
  guest-vlan {
    vlan-id 30;
  }
  camera-vlan {
    vlan-id 40;
  }
}
```

Configuring MSTP on Switch 2

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

```
[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces 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 mstp configuration-name region1
set protocols mstp bridge-priority 32k
set protocols mstp interface ge-0/0/14 cost 1000
set protocols mstp interface ge-0/0/14 mode point-to-point
set protocols mstp interface ge-0/0/18 cost 1000
set protocols mstp interface ge-0/0/18 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]

```

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 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 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 ge-0/0/14 cost 1000
user@switch2# mstp interface ge-0/0/14 mode point-to-point
user@switch2# mstp interface ge-0/0/18 cost 1000
user@switch2# mstp interface ge-0/0/18 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 {
  ge-0/0/14 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;

```

```
        vlan {
            members 10;
            members 20;
            members 30;
            members 40;
        }
    }
}
ge-0/0/18 {
    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 ge-0/0/14 {
            cost 1000;
            mode point-to-point;
        }
        interface ge-0/0/18 {
            cost 1000;
            mode point-to-point;
        }
        msti 1 {
            bridge-priority 32k;
            vlan [10 20];
        }
        msti 2 {
            bridge-priority 4k;
            vlan [30 40];
        }
    }
}
vlangs {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
```

```

        vlan-id 40;
    }
}

```

Configuring MSTP on Switch 3

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

```

[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces 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 mstp configuration-name region1
set protocols mstp bridge-priority 8k
set protocols mstp interface ge-0/0/26 cost 1000
set protocols mstp interface ge-0/0/26 mode point-to-point
set protocols mstp interface ge-0/0/28 cost 1000
set protocols mstp interface ge-0/0/28 mode point-to-point
set protocols mstp interface ge-0/0/24 cost 1000
set protocols mstp interface ge-0/0/24 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]

```

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 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 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 ge-0/0/26 cost 1000
user@switch3# mstp interface ge-0/0/26 mode point-to-point
user@switch3# mstp interface ge-0/0/28 cost 1000
user@switch3# mstp interface ge-0/0/28 mode point-to-point
user@switch3# mstp interface ge-0/0/24 cost 1000
user@switch3# mstp interface ge-0/0/24 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 {
  ge-0/0/26 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
  ge-0/0/28 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
}
```

```

    }
  }
}
ge-0/0/24 {
  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 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;
    }
    msti 1 {
      bridge-priority 4k;
      vlan [10 20];
    }
    msti 2 {
      bridge-priority 16k;
      vlan [30 40];
    }
  }
}
vpls {
  voice-vlan {
    vlan-id 10;
  }
  employee-vlan {
    vlan-id 20;
  }
  guest-vlan {
    vlan-id 30;
  }
  camera-vlan {

```

```
        vlan-id 40;
    }
}
```

Configuring MSTP on Switch 4

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

```
[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces 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 mstp configuration-name region1
set protocols mstp bridge-priority 16k
set protocols mstp interface ge-0/0/23 cost 1000
set protocols mstp interface ge-0/0/23 mode point-to-point
set protocols mstp interface ge-0/0/19 cost 1000
set protocols mstp interface ge-0/0/19 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]
```

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 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 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 ge-0/0/23 cost 1000
user@switch4# mstp interface ge-0/0/23 mode point-to-point
user@switch4# mstp interface ge-0/0/19 cost 1000
user@switch4# mstp interface ge-0/0/19 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 {
  ge-0/0/23 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
  ge-0/0/19 {
    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 ge-0/0/23 {
  cost 1000;
  mode point-to-point;
}
interface ge-0/0/19 {
  cost 1000;
  mode point-to-point;
}
msti 1 {
  bridge-priority 16k;
  vlan [10 20];
}
msti 2 {
  bridge-priority 32k;
  vlan [30 40];
}
}
}
vlangs {
  voice-vlan {
    vlan-id 10;
  }
  employee-vlan {
    vlan-id 20;
  }
  guest-vlan {
    vlan-id 30;
  }
  camera-vlan {
    vlan-id 40;
  }
}
```

Verification

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

- [Verifying MSTP Configuration on Switch 1 on page 210](#)
- [Verifying MSTP Configuration on Switch 2 on page 212](#)
- [Verifying MSTP Configuration on Switch 3 on page 213](#)
- [Verifying MSTP Configuration on Switch 4 on page 215](#)

[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 port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/9	128:490	128:490	16384.4c9614e9f841	1000	BLK	DIS
ge-0/0/11	128:491	128:491	16384.4c9614e9f841	1000	BLK	DIS
ge-0/0/13	128:492	128:492	16384.4c9614e9f841	1000	BLK	DIS

Spanning tree interface parameters for instance 1

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/9	128:490	128:490	16385.4c9614e9f841	1000	BLK	DIS
ge-0/0/11	128:491	128:491	16385.4c9614e9f841	1000	BLK	DIS
ge-0/0/13	128:492	128:492	16385.4c9614e9f841	1000	BLK	DIS

Spanning tree interface parameters for instance 2

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/9	128:490	128:490	8194.4c9614e9f841	1000	BLK	DIS
ge-0/0/11	128:491	128:491	8194.4c9614e9f841	1000	BLK	DIS
ge-0/0/13	128:492	128:492	8194.4c9614e9f841	1000	BLK	DIS

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                    : 16384.4c:96:14:e9:f8:41
CIST regional root         : 16384.4c:96:14:e9:f8:41
CIST internal root cost    : 0
Hello time                 : 2 seconds
Maximum age                : 20 seconds
Forward delay              : 15 seconds
Number of topology changes : 0
Local parameters
  Bridge ID                : 16384.4c:96:14:e9:f8:41
```

STP bridge parameters for MSTI 1

```
MSTI regional root        : 16385.4c:96:14:e9:f8:41
Hello time                 : 2 seconds
Maximum age                : 20 seconds
Forward delay              : 15 seconds
Number of topology changes : 0
Local parameters
  Bridge ID                : 16385.4c:96:14:e9:f8:41
```

STP bridge parameters for MSTI 2

```
MSTI regional root        : 8194.4c:96:14:e9:f8:41
Hello time                 : 2 seconds
Maximum age                : 20 seconds
Forward delay              : 15 seconds
Number of topology changes : 0
Local parameters
  Bridge ID                : 8194.4c:96:14:e9:f8:41
```

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 port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/14	128:513	128:513	32768.0019e2503d20	1000	FWD	DESG
ge-0/0/18	128:519	128:515	8192.0019e25051e0	1000	FWD	ROOT

Spanning tree interface parameters for instance 1

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/14	128:513	128:513	32769.0019e2503d20	1000	FWD	DESG
ge-0/0/18	128:519	128:515	4097.0019e25051e0	1000	FWD	ROOT

Spanning tree interface parameters for instance 2

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/14	128:513	128:513	4098.0019e2503d20	1000	FWD	DESG
ge-0/0/18	128:519	128:519	4098.0019e2503d20	1000	FWD	DESG

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

STP bridge parameters

```
Context ID           : 0
Enabled protocol     : MSTP
```

STP bridge parameters for CIST

```
Root ID              : 8192.00:19:e2:50:51:e0
Root cost             : 1000
Root port            : ge-0/0/18
CIST regional root    : 8192.00:19:e2:50:51:e0
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 : 1
Time since last topology change : 782 seconds
```

```

Local parameters
  Bridge ID           : 32768.00:19:e2:50:3d:20
  Extended system ID  : 0
  Internal instance ID : 0

STP bridge parameters for MSTI 1
  MSTI regional root   : 4096.00:19:e2:50:51:e0
  Root cost             : 1000
  Root port            : ge-0/0/18
  Hello time           : 2 seconds
  Maximum age          : 20 seconds
  Forward delay        : 15 seconds
  Hop count            : 19
  Local parameters
    Bridge ID           : 32768.00:19:e2:50:3d:20
    Extended system ID  : 0
    Internal instance ID : 1

STP bridge parameters for MSTI 2
  MSTI regional root   : 4096.00:19:e2:50:3d:20
  Hello time           : 2 seconds
  Maximum age          : 20 seconds
  Forward delay        : 15 seconds
  Local parameters
    Bridge ID           : 4096.00:19:e2:50:3d:20
    Extended system ID  : 0
    Internal instance ID : 2

```

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 port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/26	128:513	128:513	8192.0019e25051e0	1000	FWD	DESG
ge-0/0/28	128:515	128:515	8192.0019e25051e0	1000	FWD	DESG
ge-0/0/24	128:517	128:517	8192.0019e25051e0	1000	FWD	DESG

```
Spanning tree interface parameters for instance 1
```

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/26	128:513	128:513	4096.0019e25051e0	1000	FWD	DESG
ge-0/0/28	128:515	128:515	4096.0019e25051e0	1000	FWD	DESG
ge-0/0/24	128:517	128:517	4096.0019e25051e0	1000	FWD	DESG

Spanning tree interface parameters for instance 2

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/26	128:513	128:531	8192.0019e25044e0	1000	BLK	ALT
ge-0/0/28	128:515	128:519	4096.0019e2503d20	1000	FWD	ROOT
ge-0/0/24	128:517	128:517	16384.0019e25051e0	1000	FWD	DESG

user@switch3> [show spanning-tree bridge](#)

STP bridge parameters

Context ID : 0
Enabled protocol : MSTP

STP bridge parameters for CIST

Root ID : 8192.00:19:e2:50:51:e0
CIST regional root : 8192.00:19:e2:50:51:e0
CIST internal root cost : 0
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Number of topology changes : 3
Time since last topology change : 843 seconds
Local parameters
Bridge ID : 8192.00:19:e2:50:51:e0
Extended system ID : 0
Internal instance ID : 0

STP bridge parameters for MSTI 1

MSTI regional root : 4096.00:19:e2:50:51:e0
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Local parameters
Bridge ID : 4096.00:19:e2:50:51:e0
Extended system ID : 0
Internal instance ID : 1

STP bridge parameters for MSTI 2

MSTI regional root : 4096.00:19:e2:50:3d:20
Root cost : 1000
Root port : ge-0/0/28
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Hop count : 19
Local parameters
Bridge ID : 16384.00:19:e2:50:51:e0
Extended system ID : 0
Internal instance ID : 2

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 port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/23	128:523	128:517	8192.0019e25051e0	1000	FWD	ROOT
ge-0/0/19	128:525	128:525	16384.0019e25040e0	1000	FWD	DESG

```
Spanning tree interface parameters for instance 1
```

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/23	128:523	128:517	4096.0019e25051e0	1000	FWD	ROOT
ge-0/0/19	128:525	128:525	16384.0019e25040e0	1000	FWD	DESG

```
Spanning tree interface parameters for instance 2
```

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/23	128:523	128:517	16384.0019e25051e0	1000	BLK	ALT
ge-0/0/19	128:525	128:527	8192.0019e25044e0	1000	FWD	ROOT

```
user@switch4> show spanning-tree bridge
STP bridge parameters
Context ID                : 0
Enabled protocol          : MSTP

STP bridge parameters for CIST
Root ID                   : 8192.00:19:e2:50:51:e0
Root cost                  : 0
Root port                 : ge-0/0/23
CIST regional root        : 8192.00:19:e2:50:51:e0
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      : 4
Time since last topology change : 887 seconds
Local parameters
  Bridge ID                     : 16384.00:19:e2:50:40:e0
  Extended system ID            : 0
  Internal instance ID          : 0

STP bridge parameters for MSTI 1
MSTI regional root              : 4096.00:19:e2:50:51:e0
Root cost                       : 1000
Root port                      : ge-0/0/23
Hello time                      : 2 seconds
Maximum age                    : 20 seconds
Forward delay                   : 15 seconds
Hop count                      : 19
Local parameters
  Bridge ID                     : 16384.00:19:e2:50:40:e0
  Extended system ID            : 0
  Internal instance ID          : 1

STP bridge parameters for MSTI 2
MSTI regional root              : 4096.00:19:e2:50:3d:20
Root cost                       : 2000
Root port                      : ge-0/0/19
Hello time                      : 2 seconds
Maximum age                    : 20 seconds
Forward delay                   : 15 seconds
Hop count                      : 18
Local parameters
  Bridge ID                     : 32768.00:19:e2:50:40:e0
  Extended system ID            : 0
  Internal instance ID          : 2

```

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.

Release History Table

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

Related Documentation

- [Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66](#)
- [Understanding MSTP on page 48](#)

Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches

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 on page 217](#)
- [Overview and Topology on page 217](#)
- [Configuring MSTP on Switch 1 on page 220](#)
- [Configuring MSTP on Switch 2 on page 223](#)
- [Configuring MSTP on Switch 3 on page 225](#)
- [Configuring MSTP on Switch 4 on page 228](#)
- [Verification on page 231](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.0 or later for EX Series switches
- Four EX Series switches

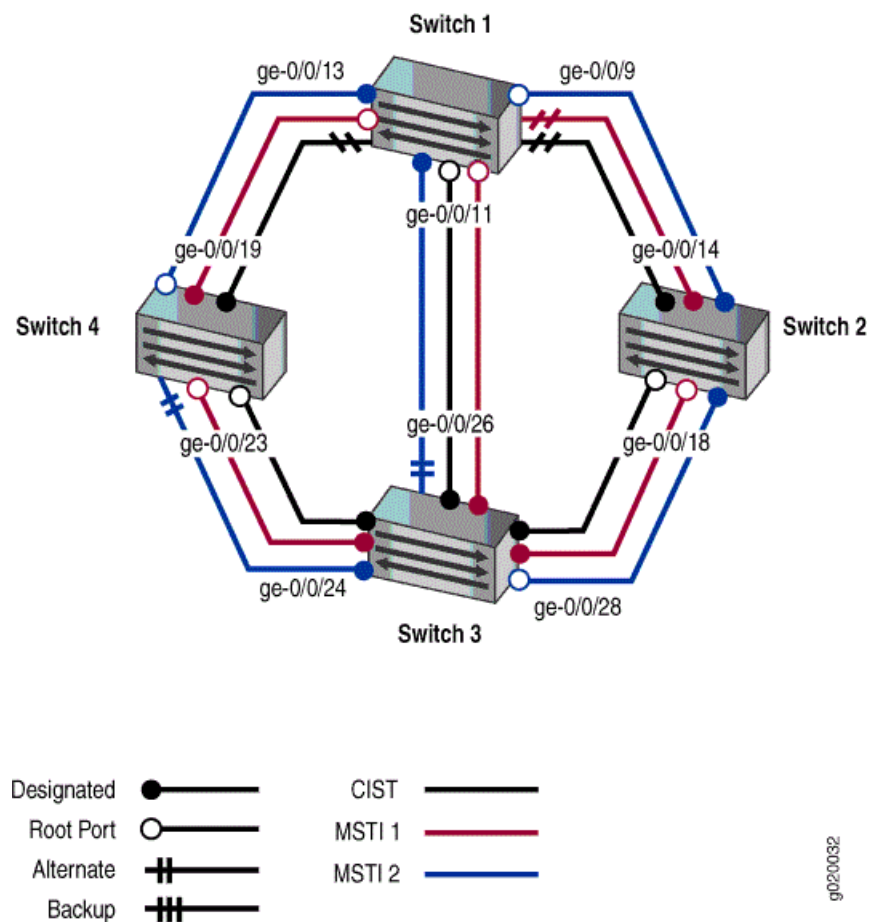
Before you configure the switches for MSTP, be sure you have:

- Installed and connected the four switches. See the hardware documentation for your switch.
- Performed the initial software configuration on all switches. See *Connecting and Configuring an EX Series Switch (CLI Procedure)* or *Connecting and Configuring an EX Series Switch (J-Web Procedure)*.

Overview and Topology

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

Figure 16: Network Topology for MSTP



The interfaces shown in [Figure 15](#) on page 197 will be configured for MSTP.



NOTE: You can configure MSTP on logical or physical interfaces. This example shows configuring MSTP on logical interfaces.

Table 18: Components of the Topology for Configuring MSTP on EX Series Switches

Property	Settings
Switch 1	<p>The following interfaces on Switch 1 are connected in this way:</p> <ul style="list-style-type: none"> • <code>ge-0/0/9</code> is connected to Switch 2 • <code>ge-0/0/13</code> is connected to Switch 4 • <code>ge-0/0/11</code> is connected to Switch 3
Switch 2	<p>The following interfaces on Switch 2 are connected in this way:</p> <ul style="list-style-type: none"> • <code>ge-0/0/14</code> is connected to Switch 1 • <code>ge-0/0/18</code> is connected to Switch 3

Table 18: Components of the Topology for Configuring MSTP on EX Series Switches (*continued*)

Property	Settings
Switch 3	<p>The following interfaces on Switch 3 are connected in this way:</p> <ul style="list-style-type: none"> • 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	<p>The following interfaces on Switch 4 are connected in this way:</p> <ul style="list-style-type: none"> • 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
MSTIs	1 2
MSTI region	region1

The topology in [Figure 15 on page 197](#) shows a common and internal spanning tree (CIST). The CIST is a single spanning tree connecting all devices in the network. The switch with the lowest bridge priority is elected as the root bridge of the CIST. You can control the election of the root bridge by configuring the bridge priority. Switch 3 is the root bridge of the CIST.

The ports in an MSTP topology have specific roles:

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

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

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

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

Configuring MSTP on Switch 1

CLI Quick Configuration To quickly configure interfaces and MSTP on Switch 1, 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 mstp configuration-name region1
set protocols mstp bridge-priority 16k
set protocols mstp interface ge-0/0/13.0 cost 1000
set protocols mstp interface ge-0/0/13.0 mode point-to-point
set protocols mstp interface ge-0/0/9.0 cost 1000
set protocols mstp interface ge-0/0/9.0 mode point-to-point
set protocols mstp interface ge-0/0/11.0 cost 1000
set protocols mstp interface ge-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 ge-0/0/11.0 cost 1000
set protocols mstp msti 2 bridge-priority 8k
set protocols mstp msti 2 vlan [30 40]
```

Step-by-Step Procedure To configure interfaces and MSTP 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 guest-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 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 ge-0/0/13.0 cost 1000
user@switch1# mstp interface ge-0/0/13.0 mode point-to-point
user@switch1# mstp interface ge-0/0/9.0 cost 1000
user@switch1# mstp interface ge-0/0/9.0 mode point-to-point
user@switch1# mstp interface ge-0/0/11.0 cost 1000
user@switch1# mstp interface ge-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 ge-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 {
  ge-0/0/13 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
  ge-0/0/9 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;

```

```
        members 40;
    }
}
}
ge-0/0/11 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            vlan {
                members 10;
                members 20;
                members 30;
                members 40;
            }
        }
    }
}
}
protocols {
    mstp {
        configuration-name region1;
        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;
        }
    }
    msti 1 {
        bridge-priority 16k;
        vlan [ 10 20];
        interface ge-0/0/11.0 {
            cost 1000;
        }
    }
    msti 2 {
        bridge-priority 8k;
        vlan [ 30 40 ];
    }
}
vlangs {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
}
```

```

    }
    camera-vlan {
        vlan-id 40;
    }
}

```

Configuring MSTP on Switch 2

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

```

[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces 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 mstp configuration-name region1
set protocols mstp bridge-priority 32k
set protocols mstp interface ge-0/0/14.0 cost 1000
set protocols mstp interface ge-0/0/14.0 mode point-to-point
set protocols mstp interface ge-0/0/18.0 cost 1000
set protocols mstp interface ge-0/0/18.0 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]

```

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 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 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 ge-0/0/14.0 cost 1000
user@switch2# mstp interface ge-0/0/14.0 mode point-to-point
user@switch2# mstp interface ge-0/0/18.0 cost 1000
user@switch2# mstp interface ge-0/0/18.0 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 {
  ge-0/0/14 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
  ge-0/0/18 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
}
protocols {
```



```

mstp {
  configuration-name region1;
  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;
  }
  msti 1 {
    bridge-priority 32k;
    vlan [10 20];
  }
  msti 2 {
    bridge-priority 4k;
    vlan [30 40];
  }
}
}
vlangs {
  voice-vlan {
    vlan-id 10;
  }
  employee-vlan {
    vlan-id 20;
  }
  guest-vlan {
    vlan-id 30;
  }
  camera-vlan {
    vlan-id 40;
  }
}
}

```

Configuring MSTP on Switch 3

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

```

[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces 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 mstp configuration-name region1
set protocols mstp bridge-priority 8k
set protocols mstp interface ge-0/0/26.0 cost 1000
set protocols mstp interface ge-0/0/26.0 mode point-to-point
set protocols mstp interface ge-0/0/28.0 cost 1000
set protocols mstp interface ge-0/0/28.0 mode point-to-point
set protocols mstp interface ge-0/0/24.0 cost 1000
set protocols mstp interface ge-0/0/24.0 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]
```

**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 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 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 ge-0/0/26.0 cost 1000
user@switch3# mstp interface ge-0/0/26.0 mode point-to-point
user@switch3# mstp interface ge-0/0/28.0 cost 1000
user@switch3# mstp interface ge-0/0/28.0 mode point-to-point
user@switch3# mstp interface ge-0/0/24.0 cost 1000
user@switch3# mstp interface ge-0/0/24.0 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 {
  ge-0/0/26 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
  ge-0/0/28 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
  ge-0/0/24 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
}
protocols {
  mstp {
    configuration-name region1;
    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;
    }
    msti 1 {
        bridge-priority 4k;
        vlan [10 20];
    }
    msti 2 {
        bridge-priority 16k;
        vlan [30 40];
    }
}
vpls {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}
```

Configuring MSTP on Switch 4

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

```
[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces 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 mstp configuration-name region1
set protocols mstp bridge-priority 16k
```

```

set protocols mstp interface ge-0/0/23.0 cost 1000
set protocols mstp interface ge-0/0/23.0 mode point-to-point
set protocols mstp interface ge-0/0/19.0 cost 1000
set protocols mstp interface ge-0/0/19.0 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]

```

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 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 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 ge-0/0/23.0 cost 1000
user@switch4# mstp interface ge-0/0/23.0 mode point-to-point
user@switch4# mstp interface ge-0/0/19.0 cost 1000
user@switch4# mstp interface ge-0/0/19.0 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 {
  ge-0/0/23 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
  ge-0/0/19 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
}
protocols {
  mstp {
    configuration-name region1;
    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;
    }
    msti 1 {
      bridge-priority 16k;
      vlan [10 20];
    }
    msti 2 {
      bridge-priority 32k;
      vlan [30 40];
    }
  }
}
vlangs {
  voice-vlan {
    vlan-id 10;
  }
  employee-vlan {
    vlan-id 20;
  }
}
```

```

}
guest-vlan {
  vlan-id 30;
}
camera-vlan {
  vlan-id 40;
}
}

```

Verification

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

- [Verifying MSTP Configuration on Switch 1 on page 231](#)
- [Verifying MSTP Configuration on Switch 2 on page 232](#)
- [Verifying MSTP Configuration on Switch 3 on page 234](#)
- [Verifying MSTP Configuration on Switch 4 on page 235](#)

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 port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/13.0	128:527	128:525	16384.0019e25040e0	1000	BLK	ALT
ge-0/0/9.0	128:529	128:513	32768.0019e2503d20	1000	BLK	ALT
ge-0/0/11.0	128:531	128:513	8192.0019e25051e0	1000	FWD	ROOT

Spanning tree interface parameters for instance 1

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/13.0	128:527	128:525	16384.0019e25040e0	1000	BLK	ALT
ge-0/0/9.0	128:529	128:513	32768.0019e2503d20	1000	BLK	ALT
ge-0/0/11.0	128:531	128:513	4096.0019e25051e0	1000	FWD	ROOT

Spanning tree interface parameters for instance 2

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/13.0	128:527	128:527	8192.0019e25044e0	1000	FWD	DESG
ge-0/0/9.0	128:529	128:513	4096.0019e2503d20	1000	FWD	ROOT
ge-0/0/11.0	128:531	128:531	8192.0019e25044e0	1000	FWD	DESG

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

STP bridge parameters

```
Context ID           : 0
Enabled protocol     : MSTP
```

```
STP bridge parameters for CIST
  Root ID                : 8192.00:19:e2:50:51:e0
  Root cost               : 1000
  Root port              : ge-0/0/13.0
  CIST regional root     : 8192.00:19:e2:50:51:e0
  CIST internal root cost : 2000
  Hello time             : 2 seconds
  Maximum age            : 20 seconds
  Forward delay          : 15 seconds
  Hop count              : 18
  Message age            : 0
  Number of topology changes : 3
  Time since last topology change : 921 seconds
  Local parameters
    Bridge ID            : 16384.00:19:e2:50:44:e0
    Extended system ID   : 0
    Internal instance ID  : 0

STP bridge parameters for MSTI 1
  MSTI regional root     : 4096.00:19:e2:50:51:e0
  Root cost              : 1000
  Root port              : ge-0/0/13.0
  Hello time             : 2 seconds
  Maximum age            : 20 seconds
  Forward delay          : 15 seconds
  Hop count              : 18
  Local parameters
    Bridge ID            : 16384.00:19:e2:50:44:e0
    Extended system ID   : 0
    Internal instance ID  : 1

STP bridge parameters for MSTI 2
  MSTI regional root     : 4096.00:19:e2:50:3d:20
  Root cost              : 1000
  Root port              : ge-0/0/9.0
  Hello time             : 2 seconds
  Maximum age            : 20 seconds
  Forward delay          : 15 seconds
  Hop count              : 19
  Local parameters
    Bridge ID            : 8192.00:19:e2:50:44:e0
    Extended system ID   : 0
    Internal instance ID  : 2
```

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 interface
```

Spanning tree interface parameters for instance 0

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/14.0	128:513	128:513	32768.0019e2503d20	1000	FWD	DESC
ge-0/0/18.0	128:519	128:515	8192.0019e25051e0	1000	FWD	ROOT

Spanning tree interface parameters for instance 1

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/14.0	128:513	128:513	32769.0019e2503d20	1000	FWD	DESC
ge-0/0/18.0	128:519	128:515	4097.0019e25051e0	1000	FWD	ROOT

Spanning tree interface parameters for instance 2

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/14.0	128:513	128:513	4098.0019e2503d20	1000	FWD	DESC
ge-0/0/18.0	128:519	128:519	4098.0019e2503d20	1000	FWD	DESC

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

STP bridge parameters

```
Context ID          : 0
Enabled protocol    : MSTP
```

STP bridge parameters for CIST

```
Root ID              : 8192.00:19:e2:50:51:e0
Root cost             : 1000
Root port            : ge-0/0/18.0
CIST regional root    : 8192.00:19:e2:50:51:e0
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 : 1
Time since last topology change : 782 seconds
Local parameters
  Bridge ID           : 32768.00:19:e2:50:3d:20
  Extended system ID  : 0
  Internal instance ID : 0
```

STP bridge parameters for MSTI 1

```
MSTI regional root   : 4096.00:19:e2:50:51:e0
Root cost             : 1000
Root port            : ge-0/0/18.0
Hello time            : 2 seconds
Maximum age           : 20 seconds
Forward delay         : 15 seconds
Hop count             : 19
Local parameters
```

```

Bridge ID                : 32768.00:19:e2:50:3d:20
Extended system ID       : 0
Internal instance ID     : 1

STP bridge parameters for MSTI 2
MSTI regional root       : 4096.00:19:e2:50:3d:20
Hello time                : 2 seconds
Maximum age               : 20 seconds
Forward delay             : 15 seconds
Local parameters
  Bridge ID               : 4096.00:19:e2:50:3d:20
  Extended system ID      : 0
  Internal instance ID    : 2

```

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 port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/26.0	128:513	128:513	8192.0019e25051e0	1000	FWD	DESC
ge-0/0/28.0	128:515	128:515	8192.0019e25051e0	1000	FWD	DESC
ge-0/0/24.0	128:517	128:517	8192.0019e25051e0	1000	FWD	DESC

Spanning tree interface parameters for instance 1

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/26.0	128:513	128:513	4096.0019e25051e0	1000	FWD	DESC
ge-0/0/28.0	128:515	128:515	4096.0019e25051e0	1000	FWD	DESC
ge-0/0/24.0	128:517	128:517	4096.0019e25051e0	1000	FWD	DESC

Spanning tree interface parameters for instance 2

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/26.0	128:513	128:531	8192.0019e25044e0	1000	BLK	ALT
ge-0/0/28.0	128:515	128:519	4096.0019e2503d20	1000	FWD	ROOT

```
ge-0/0/24.0    128:517    128:517  16384.0019e25051e0    1000  FWD    DESG
```

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

```
STP bridge parameters
```

```
Context ID           : 0
Enabled protocol     : MSTP
```

```
STP bridge parameters for CIST
```

```
Root ID              : 8192.00:19:e2:50:51:e0
CIST regional root   : 8192.00:19:e2:50:51:e0
CIST internal root cost : 0
Hello time           : 2 seconds
Maximum age          : 20 seconds
Forward delay        : 15 seconds
Number of topology changes : 3
Time since last topology change : 843 seconds
Local parameters
  Bridge ID          : 8192.00:19:e2:50:51:e0
  Extended system ID : 0
  Internal instance ID : 0
```

```
STP bridge parameters for MSTI 1
```

```
MSTI regional root   : 4096.00:19:e2:50:51:e0
Hello time           : 2 seconds
Maximum age          : 20 seconds
Forward delay        : 15 seconds
Local parameters
  Bridge ID          : 4096.00:19:e2:50:51:e0
  Extended system ID : 0
  Internal instance ID : 1
```

```
STP bridge parameters for MSTI 2
```

```
MSTI regional root   : 4096.00:19:e2:50:3d:20
Root cost             : 1000
Root port             : ge-0/0/28.0
Hello time           : 2 seconds
Maximum age          : 20 seconds
Forward delay        : 15 seconds
Hop count            : 19
Local parameters
  Bridge ID          : 16384.00:19:e2:50:51:e0
  Extended system ID : 0
  Internal instance ID : 2
```

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 port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/23.0	128:523	128:517	8192.0019e25051e0	1000	FWD	ROOT
ge-0/0/19.0	128:525	128:525	16384.0019e25040e0	1000	FWD	DESG

```
Spanning tree interface parameters for instance 1
```

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/23.0	128:523	128:517	4096.0019e25051e0	1000	FWD	ROOT
ge-0/0/19.0	128:525	128:525	16384.0019e25040e0	1000	FWD	DESG

```
Spanning tree interface parameters for instance 2
```

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/23.0	128:523	128:517	16384.0019e25051e0	1000	BLK	ALT
ge-0/0/19.0	128:525	128:527	8192.0019e25044e0	1000	FWD	ROOT

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

```
STP bridge parameters
```

```
Context ID : 0
Enabled protocol : MSTP
```

```
STP bridge parameters for CIST
```

```
Root ID : 8192.00:19:e2:50:51:e0
Root cost : 0
Root port : ge-0/0/23.0
CIST regional root : 8192.00:19:e2:50:51:e0
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 : 4
Time since last topology change : 887 seconds
Local parameters
  Bridge ID : 16384.00:19:e2:50:40:e0
  Extended system ID : 0
  Internal instance ID : 0
```

```
STP bridge parameters for MSTI 1
```

```
MSTI regional root : 4096.00:19:e2:50:51:e0
Root cost : 1000
Root port : ge-0/0/23.0
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Hop count : 19
Local parameters
  Bridge ID : 16384.00:19:e2:50:40:e0
```

```
Extended system ID      : 0
Internal instance ID    : 1

STP bridge parameters for MSTI 2
MSTI regional root      : 4096.00:19:e2:50:3d:20
Root cost                : 2000
Root port               : ge-0/0/19.0
Hello time              : 2 seconds
Maximum age             : 20 seconds
Forward delay           : 15 seconds
Hop count               : 18
Local parameters
  Bridge ID             : 32768.00:19:e2:50:40:e0
  Extended system ID    : 0
  Internal instance ID  : 2
```

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.

- Related Documentation**
- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
 - [Understanding MSTP on page 48](#)

CHAPTER 10

Configuring Root Protection in a VPLS Multihoming Environment

- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240
- Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 241
- Understanding Bridge Priority for Election of Root Bridge and Designated Bridge on page 242
- Understanding VPLS Multihoming: Priority of the Backup Bridge on page 243
- Understanding VPLS Multihoming: Hold Time Before Switching to Primary Priority on page 243
- Understanding VPLS Multihoming: System Identifier for Bridges in the Ring on page 244
- Understanding VPLS Multihoming: Bridge Flush of MAC Cache on Topology Change on page 245
- Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 246
- Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247
- Example: Configuring VPLS Root Topology Change Actions on page 247
- Enabling Root Protection for a Spanning-Tree Instance Interface on page 248
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 249
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 250
- Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches on page 251
- Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on EX Series Switches on page 256

Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure

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

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

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

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

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

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

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

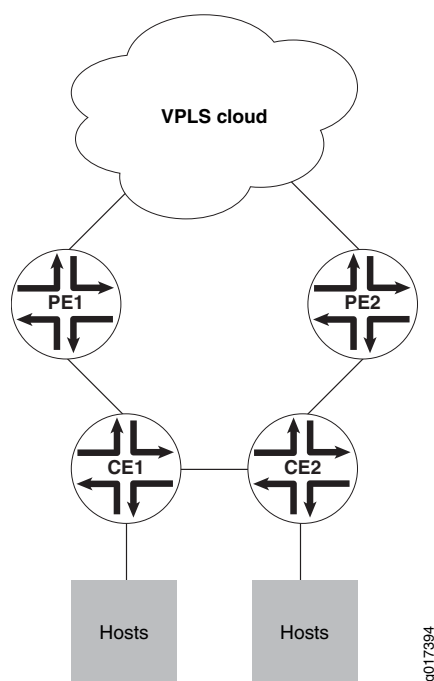
Related Documentation

- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 241](#)
- [Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 249](#)
- [Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 250](#)
- [Example: Configuring VPLS Root Topology Change Actions on page 247](#)

Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology

Figure 17 on page 241 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 17: VPLS Multihoming Configuration



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

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

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

- Related Documentation**
- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240](#)
 - [Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 249](#)
 - [Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 250](#)
 - [Example: Configuring VPLS Root Topology Change Actions on page 247](#)

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

- Related Documentation**
- [Configuring Rapid Spanning Tree Protocol on page 62](#)
 - [Configuring Multiple Spanning Tree Protocol on page 54](#)
 - [Configuring VLAN SpanningTree Protocol on page 106](#)
 - [bridge-priority on page 288](#)

Understanding VPLS Multihoming: Priority of the Backup Bridge

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

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

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

backup-bridge-priority *vpls-ring-backup-bridge-priority*

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



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

Related Documentation

- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240](#)
- [Understanding VPLS Multihoming: Hold Time Before Switching to Primary Priority on page 243](#)
- [Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 249](#)
- [Example: Configuring VPLS Root Topology Change Actions on page 247](#)

Understanding VPLS Multihoming: Hold Time Before Switching to Primary Priority

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

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

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

priority-hold-time *seconds*

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



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

**Related
Documentation**

- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240](#)
- [Understanding VPLS Multihoming: Priority of the Backup Bridge on page 243](#)
- [Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 249](#)
- [Example: Configuring VPLS Root Topology Change Actions on page 247](#)

Understanding VPLS Multihoming: System Identifier for Bridges in the Ring

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

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

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

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



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

**Related
Documentation**

- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240](#)
- [Understanding VPLS Multihoming: Priority of the Backup Bridge on page 243](#)
- [Understanding VPLS Multihoming: Hold Time Before Switching to Primary Priority on page 243](#)
- [Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 249](#)
- [Example: Configuring VPLS Root Topology Change Actions on page 247](#)

Understanding VPLS Multihoming: Bridge Flush of MAC Cache on Topology Change

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

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

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

vpls-flush-on-topology-change

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

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



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

Related Documentation

- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240](#)
- [Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 249](#)
- [Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 250](#)
- [Example: Configuring VPLS Root Topology Change Actions on page 247](#)

Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches

Juniper Networks EX Series Ethernet Switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), and Multiple Spanning Tree Protocol (MSTP). A loop-free network 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 and which interfaces become root ports and forward traffic.

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. Root protection allows network administrators to manually enforce the root bridge placement in the network.

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 become designated ports and 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.

When root protection is enabled on an interface, it is enabled for all the 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.

An interface can be configured for either root protection or loop protection, but not for both.

Related Documentation

- [Configuring BPDU Protection on Switch Spanning Tree Interfaces on page 139](#)
- [Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches on page 251](#)
- [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 184](#)
- [Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157](#)
- [Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167](#)
- [Understanding MSTP on page 48](#)
- [Understanding RSTP on page 21](#)
- [Understanding STP on page 26](#)
- [Understanding VSTP on page 29](#)

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

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

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

By default, root protect is disabled.

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

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

Related Documentation

- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)
- [Enabling Root Protection for a Spanning-Tree Instance Interface on page 248](#)

Example: Configuring VPLS Root Topology Change Actions

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

```
[edit]
protocols {
  mstp {
    bridge-priority 36k;
    backup-bridge-priority 44k;
    priority-hold-time 60;
    system-id 000203:040506 {
      10.1.1.1/32;
    }
    vpls-flush-on-topology-change;
  }
}
```



NOTE: This is not a complete configuration.

- Related Documentation**
- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240](#)
 - [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 241](#)
 - [Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 249](#)
 - [Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 250](#)

Enabling Root Protection for a Spanning-Tree Instance Interface

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

1. Enable configuration of the spanning-tree protocol:

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

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

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

3. Enable root protection on the interface:

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

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

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

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



NOTE: This is not a complete configuration.

- Related Documentation**
- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)

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

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

1. Enable configuration of the spanning-tree protocol:

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

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

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

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

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

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

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

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

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



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

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

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

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

```
[edit]
protocols {
  (mstp | rstp | vstp) {
    backup-bridge-priority priority; # Default is 32,768.
    priority-hold-time seconds; # Default is 2 seconds.
    system-id system-id-value {
```

```
        ip-address;  
    }  
    vpls-flush-on-topology-change;  
  }  
}
```

Related Documentation

- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240](#)
- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 241](#)
- [Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 250](#)
- [Example: Configuring VPLS Root Topology Change Actions on page 247](#)

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

Related Documentation

- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240](#)
- [Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 241](#)
- [Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 249](#)
- [Example: Configuring VPLS Root Topology Change Actions on page 247](#)

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

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 on page 252](#)
- [Overview and Topology on page 252](#)
- [Configuration on page 254](#)
- [Verification on page 254](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- Four EX Series switches in an RSTP topology

Before you configure the interface for root protection, be sure you have:

- RSTP operating on the switches.



NOTE: By default, RSTP is enabled on all EX Series switches.

Overview and Topology

Peer STP applications running on switch interfaces exchange a special type of frame called a bridge protocol data unit (BPDU). Switches communicate interface information using BPDUs to create a loop-free topology that ultimately determines the root bridge and which interfaces block or forward traffic in the spanning tree.

However, a root port elected through this process has the possibility of being wrongly elected. A user bridge application running on a PC can generate BPDUs, too, and interfere with root port election.

To prevent this from happening, enable root protection on interfaces that should not receive superior BPDUs from the root bridge and should not be elected as the root port. These interfaces are typically located on an administrative boundary and are designated ports.

When root protection is enabled on an interface:

- The interface is blocked from becoming the root port.
- Root protection is enabled for all STP instances on that interface.
- The interface is blocked only for instances for which it receives superior BPDUs. Otherwise, it participates in the spanning-tree topology.



CAUTION: An interface can be configured for either root protection or loop protection, but not for both.

Four EX Series switches are displayed in [Figure 18 on page 253](#). In this example, they are configured for RSTP and create a loop-free topology. Interface **ge-0/0/7** on Switch 1 is a designated port on an administrative boundary. It connects to Switch 4. Switch 3 is the root bridge. Interface **ge-0/0/6** on Switch 1 is the root port.

This example shows how to configure root protection on interface **ge-0/0/7** to prevent it from transitioning to become the root port.

Figure 18: Network Topology for Root Protection

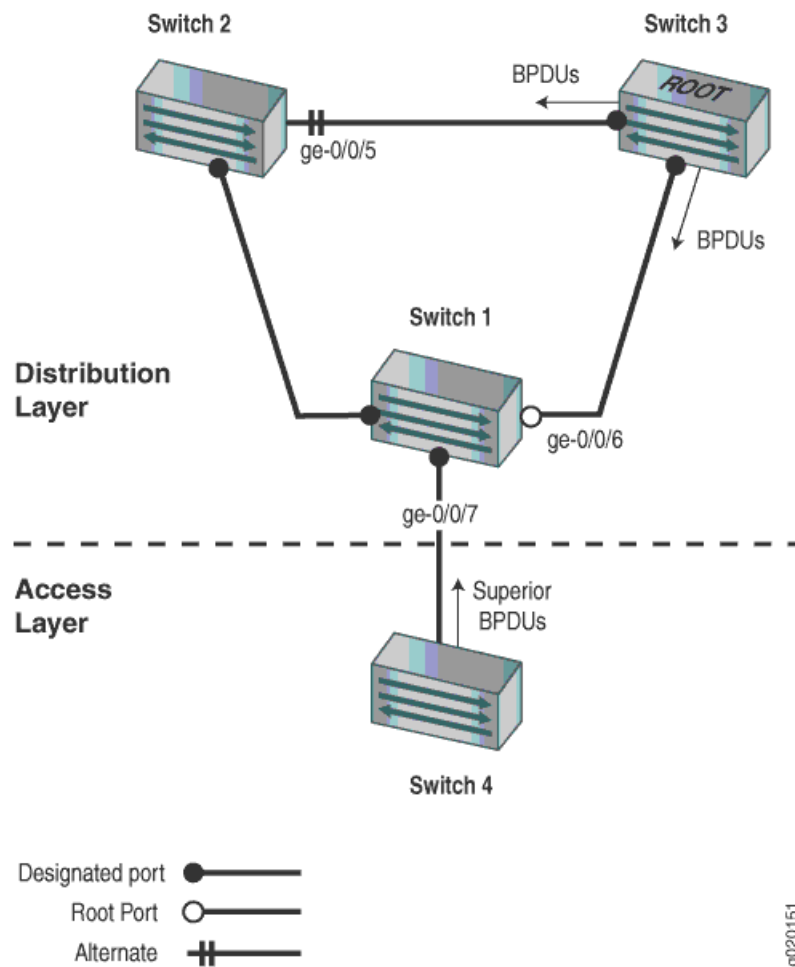


Table 19 on page 253 shows the components that will be configured for root protection.

Table 19: Components of the Topology for Configuring Root Protection on EX Series Switches

Property	Settings
Switch 1	Switch 1 is connected to Switch 4 through interface ge-0/0/7 .
Switch 2	Switch 2 is connected to Switch 1 and Switch 3. Interface ge-0/0/4 is the alternate port in the RSTP topology.
Switch 3	Switch 3 is the root bridge and is connected to Switch 1 and Switch 2.
Switch 4	Switch 4 is connected to Switch 1. After root protection is configured on interface ge-0/0/7 , Switch 4 will send superior BPDUs that will trigger root protection on interface ge-0/0/7 .

A spanning tree topology contains ports that have specific roles:

- The *root port* is responsible for forwarding data to the root bridge.

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

This configuration example uses an RSTP topology. However, you also can configure root protection for STP or MSTP topologies at the `[edit protocols (mstp | stp)]` hierarchy level.

Configuration

To configure root protection on an interface:

CLI Quick Configuration

To quickly configure root protection on interface **ge-0/0/7**, copy the following command and paste it into the switch terminal window:

```
[edit]
set protocols rstp interface ge-0/0/7 no-root-port
```

Step-by-Step Procedure

To configure root protection:

1. Configure interface **ge-0/0/7**:

```
[edit protocols rstp]
user@switch#
set interface ge-0/0/7 no-root-port
```

Results

Check the results of the configuration:

```
user@switch> show configuration protocols rstp
interface ge-0/0/7.0 {
  no-root-port;
}
```

Verification

To confirm that the configuration is working properly:

- [Displaying the Interface State Before Root Protection Is Triggered on page 254](#)
- [Verifying That Root Protection Is Working on the Interface on page 255](#)

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 port ID	Designated bridge ID	Port Cost	State	Role
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 port ID	Designated bridge ID	Port Cost	State	Role
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.

Related Documentation

- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
- [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 184](#)
- [Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157](#)
- [Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167](#)
- [Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 246](#)

Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on EX Series Switches



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 Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches” on page 251](#). 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 on page 256](#)
- [Overview and Topology on page 257](#)
- [Configuration on page 259](#)
- [Verification on page 259](#)

Requirements

This example uses the following software and hardware components:

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

- Four EX Series switches in an RSTP topology

Before you configure the interface for root protection, be sure you have:

- RSTP operating on the switches.



NOTE: By default, RSTP is enabled on all EX Series switches.

Overview and Topology

Peer STP applications running on switch interfaces exchange a special type of frame called a bridge protocol data unit (BPDU). Switches communicate interface information using BPDUs to create a loop-free topology that ultimately determines the root bridge and which interfaces block or forward traffic in the spanning tree.

However, a root port elected through this process has the possibility of being wrongly elected. A user bridge application running on a PC can generate BPDUs, too, and interfere with root port election.

To prevent this from happening, enable root protection on interfaces that must not receive superior BPDUs from the root bridge and must not be elected as the root port. These interfaces are typically located on an administrative boundary and are designated ports.

When root protection is enabled on an interface:

- The interface is blocked from becoming the root port.
- Root protection is enabled for all STP instances on that interface.
- The interface is blocked only for instances for which it receives superior BPDUs. Otherwise, it participates in the spanning-tree topology.



CAUTION: An interface can be configured for either root protection or loop protection, but not for both.

Four EX Series switches are displayed in [Figure 18 on page 253](#). 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 19: Network Topology for Root Protection

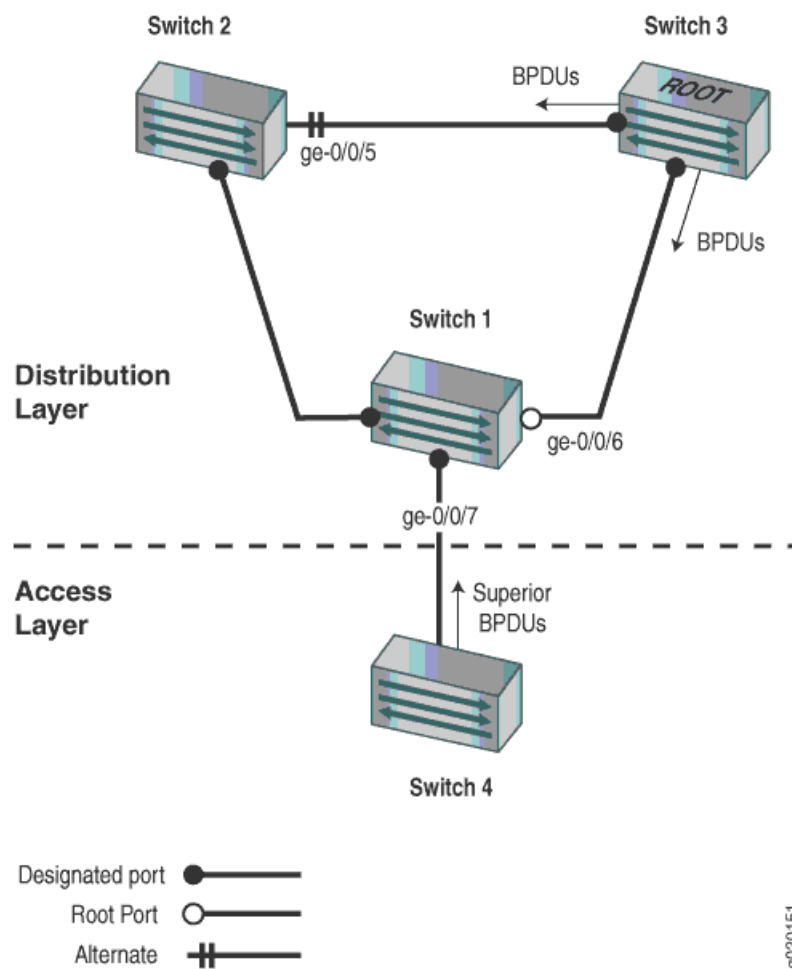


Table 19 on page 253 shows the components that will be configured for root protection.

Table 20: Components of the Topology for Configuring Root Protection on EX Series Switches

Property	Settings
Switch 1	Switch 1 is connected to Switch 4 through interface ge-0/0/7 .
Switch 2	Switch 2 is connected to Switch 1 and Switch 3. Interface ge-0/0/4 is the alternate port in the RSTP topology.
Switch 3	Switch 3 is the root bridge and is connected to Switch 1 and Switch 2.
Switch 4	Switch 4 is connected to Switch 1. After root protection is configured on interface ge-0/0/7 , Switch 4 will send superior BPDUs that will trigger root protection on interface ge-0/0/7 .

A spanning tree topology contains ports that have specific roles:

- The *root port* is responsible for forwarding data to the root bridge.

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

This configuration example uses an RSTP topology. However, you also can configure root protection for STP or MSTP topologies at the `[edit protocols mstp]` hierarchy level.

Configuration

To configure root protection on an interface:

CLI Quick Configuration To quickly configure root protection on interface **ge-0/0/7**, copy the following command and paste it into the switch terminal window:

```
[edit]
set protocols rstp interface ge-0/0/7 no-root-port
```

Step-by-Step Procedure To configure root protection:

1. Configure interface **ge-0/0/7**:

```
[edit protocols rstp]
user@switch#
set interface ge-0/0/7 no-root-port
```

Results Check the results of the configuration:

```
user@switch> show configuration protocols rstp
interface ge-0/0/7 {
  no-root-port;
}
```

Verification

To confirm that the configuration is working properly:

- [Displaying the Interface State Before Root Protection Is Triggered on page 259](#)
- [Verifying That Root Protection Is Working on the Interface on page 260](#)

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 port ID	Designated bridge ID	Port Cost	State	Role
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 port ID	Designated bridge ID	Port Cost	State	Role
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.

**Related
Documentation**

- [Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66](#)
- [Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches on page 189](#)
- [Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 246](#)

Configuring Layer 2 Protocol Tunneling

- [Understanding Layer 2 Protocol Tunneling Through a Network on page 263](#)
- [Understanding Layer 2 Protocol Tunneling Configuration Guidelines on page 265](#)
- [Configuring Layer 2 Protocol Tunneling on page 266](#)

Understanding Layer 2 Protocol Tunneling Through a Network

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

Layer 2 protocol tunneling is supported on MX Series routers with Enhanced (Dense Port Concentrators) DPCs and Enhanced Queuing (DPCs), see [Table 22 on page 264](#) for a list of the DPCs supported. Layer 2 protocol tunneling is supported on all Modular Port Concentrators (MPCs),



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

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

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

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

[Table 21 on page 264](#) shows the MPCs and Enhanced DPCs supported when configuring Layer 2 protocol tunneling and VPLS.

Table 21: MAC Rewrite and VPLS Configurations

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

Table 22 on page 264 lists the DPCs that support the Layer 2 tunneling protocol.

Table 22: DPCs Supported for Layer 2 Protocol Tunneling

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

Table 22: DPCs Supported for Layer 2 Protocol Tunneling (*continued*)

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



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

Related Documentation

- [Configuring Layer 2 Protocol Tunneling on page 266](#)
- [Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 273](#)
- [Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 273](#)

Understanding Layer 2 Protocol Tunneling Configuration Guidelines

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

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

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

- Related Documentation**
- [Understanding Layer 2 Protocol Tunneling Through a Network on page 263](#)
 - [MAC Address Rewriting Enabled for Layer 2 Protocol Tunneling](#)
 - [Configuring Layer 2 Protocol Tunneling on page 266](#)

Configuring Layer 2 Protocol Tunneling

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

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

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

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



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

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

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

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

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

To configure Layer 2 protocol tunneling:

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

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

2. Configure the Layer 2 protocol tunnel interface.

```
[edit protocols layer2-control mac-rewrite]
user@host# set interface ge-fpc/pic/port
```

3. Configure the Layer 2 protocol to be tunneled.

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

4. Verify the configuration.

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

**Related
Documentation**

- [Understanding Layer 2 Protocol Tunneling Through a Network on page 263](#)
- [Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 273](#)
- [Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 273](#)

CHAPTER 12

Monitoring Layer 2 Spanning-Tree Protocol

- [Monitoring Spanning Tree Protocols on Switches on page 269](#)
- [Checking the Status of Spanning-Tree Instance Interfaces on page 272](#)
- [Clearing the Blocked Status of a Spanning-Tree Instance Interface on page 272](#)
- [Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 273](#)
- [Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 273](#)
- [Configuring Tracing Spanning-Tree Operations on page 274](#)
- [Example: Tracing Spanning-Tree Protocol Operations on page 276](#)

Monitoring Spanning Tree Protocols on Switches

Purpose



NOTE: This topic applies only to the J-Web Application package.

Use the monitoring feature to view status and information about the spanning-tree protocol parameters on your EX Series switch.

Action

To display spanning-tree protocol parameter details in the J-Web interface, select **Monitor** > **Switching** > **STP**.

To display spanning-tree protocol parameter details in the CLI, enter the following commands:

- **show spanning-tree interface**
- **show spanning-tree bridge**

Meaning

[Table 23 on page 270](#) summarizes the spanning-tree protocol parameters.

Table 23: Summary of Spanning Tree Protocols Output Fields

Field	Values
Bridge Parameters	
Routing instance name	Displays bridge information for the specified routing instance. NOTE: The option is supported only on EX4300 switches.
Context ID	An internally generated identifier.
Enabled Protocol	Spanning-tree protocol type enabled.
Root ID	Bridge ID of the elected spanning-tree root bridge. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.
Root cost	Calculated cost to reach the root bridge from the bridge where the command is entered.
Root port	Interface that is the current elected root port for this bridge.
Bridge ID	Locally configured bridge ID.
Hello time	The time for which the bridge interface remains in the listening or learning state.
Forward delay	The time for which the bridge interface remains in the listening or learning state before transitioning to the forwarding state.
Extended System ID	The system ID.
Inter Instance ID	An internally generated instance identifier.
Maximum age	Maximum age of received bridge protocol data units (BPDUs).
Number of topology changes	Total number of spanning-tree protocol topology changes detected since the switch last booted.
Time since last topology change	Number of seconds elapsed since the last topology change. NOTE: This option is supported only on EX4300 switches.
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.

Table 23: Summary of Spanning Tree Protocols Output Fields (*continued*)

Field	Values
Designated Port ID	Port ID of the designated port for the LAN segment to which the interface is attached.
Designated Bridge ID	ID of the designated bridge to which the interface is attached.
Port Cost	Configured cost for the interface.
Port State	Spanning-tree protocol port state: <ul style="list-style-type: none"> • 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.

- Related Documentation**
- [show spanning-tree interface on page 377](#)
 - [show spanning-tree bridge on page 372](#)
 - [Configuring Spanning Tree Protocols on EX Series Switches \(J-Web Procedure\) on page 36](#)

Checking the Status of Spanning-Tree Instance Interfaces

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

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

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

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

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

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

Related Documentation

- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)
- [Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35](#)
- [Understanding BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 134](#)
- [Understanding BPDU Protection on All Edge Ports of the Bridge on page 136](#)
- [Clearing the Blocked Status of a Spanning-Tree Instance Interface on page 272](#)

Clearing the Blocked Status of a Spanning-Tree Instance Interface

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

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

```
user@host> clear error bpd interface interface interface-name
```



NOTE: When you configure BPDU protection on individual interfaces (as opposed to on all the edge ports of the bridge), you can use the **disable-timeout seconds** option to specify that a blocked interface is automatically cleared after the specified time interval elapses (unless the interval is 0). For configuration details, see “[Configuring BPDU Protection for Spanning-Tree Instance Interfaces](#)” on page 137.

Related Documentation

- [Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247](#)

- [Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35](#)
- [Understanding BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 134](#)
- [Understanding BPDU Protection on All Edge Ports of the Bridge on page 136](#)
- [Checking the Status of Spanning-Tree Instance Interfaces on page 272](#)

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

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

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

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

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

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

Related Documentation

- [Understanding Layer 2 Protocol Tunneling Through a Network on page 263](#)
- [Configuring Layer 2 Protocol Tunneling on page 266](#)
- [Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 273](#)

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

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

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

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

Related Documentation

- [Understanding Layer 2 Protocol Tunneling Through a Network on page 263](#)
- [Configuring Layer 2 Protocol Tunneling on page 266](#)
- [Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface on page 273](#)

Configuring Tracing Spanning-Tree Operations

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

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

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

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

To enable tracing of spanning-tree protocol operations:

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

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

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

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

3. Configure the files that contain trace logging information:

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

4. Configure spanning-tree protocol-specific options.

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

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

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

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



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

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

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

```
[edit]
...
routing-options {
  traceoptions {
    ..global-trace-options-configuration...
  }
}
```

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

Related Documentation • [Example: Tracing Spanning-Tree Protocol Operations on page 276](#)

Example: Tracing Spanning-Tree Protocol Operations

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

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

Related Documentation • [Configuring Tracing Spanning-Tree Operations on page 274](#)

CHAPTER 13

Configuration Statements for Spanning-Tree Protocols

- [access-trunk on page 278](#)
- [arp-on-stp on page 279](#)
- [backup-bridge-priority on page 280](#)
- [block \(Spanning Trees\) on page 281](#)
- [bpdu-destination-mac-address \(Spanning Tree\) on page 282](#)
- [bpdu-block on page 283](#)
- [bpdu-block-on-edge on page 284](#)
- [bpdu-timeout-action on page 286](#)
- [bridge-priority on page 288](#)
- [configuration-name on page 290](#)
- [cost on page 291](#)
- [disable on page 293](#)
- [disable-timeout on page 295](#)
- [drop \(BPDU Block\) on page 296](#)
- [edge on page 297](#)
- [enable-all-ifl on page 298](#)
- [extended-system-id on page 299](#)
- [force-version \(IEEE 802.1D STP\) on page 300](#)
- [forward-delay on page 301](#)
- [hello-time on page 303](#)
- [interface \(BPDU Blocking\) on page 305](#)
- [interface \(Spanning Tree\) on page 307](#)
- [layer2-control on page 309](#)
- [log \(Spanning Trees\) on page 310](#)
- [mac-rewrite on page 311](#)
- [max-age on page 313](#)

- [max-hops on page 315](#)
- [mode on page 316](#)
- [msti on page 318](#)
- [mstp on page 320](#)
- [no-root-port on page 324](#)
- [priority \(Protocols STP\) on page 326](#)
- [priority-hold-time on page 327](#)
- [protocol on page 328](#)
- [protocols \(STP Type\) on page 330](#)
- [revision-level on page 331](#)
- [rstp on page 332](#)
- [shutdown \(BPDU Block\) on page 335](#)
- [stp on page 336](#)
- [system-id on page 338](#)
- [traceoptions \(Spanning Tree\) on page 339](#)
- [vlan \(MSTP\) on page 343](#)
- [vlan \(VSTP\) on page 345](#)
- [vlan-group on page 347](#)
- [vpls-flush-on-topology-change on page 348](#)
- [vstp on page 349](#)

access-trunk

Syntax	access-trunk;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols vstp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vstp], [edit protocols vstp vlan <i>vlan-identifier</i> interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> instance-type (layer2-control virtual-switch)]
Description	Enable untagged RTSP BDPUs to be sent and received on the interface.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	

arp-on-stp

Syntax	arp-on-stp;
Hierarchy Level	[edit protocols mstp interface (all <i>interface-name</i>)], [edit protocols rstp interface (all <i>interface-name</i>)], [edit protocols stp interface (all <i>interface-name</i>)], [edit protocols vstp (all <i>vlan--id</i> <i>vlan--name</i>) interface (all <i>interface-name</i>)]
Release Information	Statement introduced in Junos OS Release 11.2 for EX Series switches.
Description	<p>Configure the Address Resolution Protocol (ARP) in a spanning-tree network so that when a spanning-tree protocol topology change notification (TCN) is issued, the VLAN with a broken link can relearn MAC addresses from another, redundant VLAN in the network. The network must include a routed VLAN interface (RVI).</p> <p>When a link fails in a spanning-tree network (RSTP, STP, MSTP, or VSTP), a message called a TCN is issued that causes all affected Ethernet switching table entries to be flushed. The network must then relearn the MAC addresses using flooding. If you have configured an RVI on the network, you have the option of having the VLAN with the broken link relearn MAC addresses from another VLAN using ARP, thereby avoiding excessive flooding on the VLAN with the broken link.</p>
Default	ARP on STP is disabled.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring STP on EX Series Switches (CLI Procedure) on page 45 • Configuring VSTP on EX Series Switches (CLI Procedure) on page 113

backup-bridge-priority

Syntax	<code>backup-bridge-priority <i>priority</i>;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> protocols (<i>mstp</i> <i>rstp</i>)],</code> <code>[edit logical-systems <i>logical-system-name</i> protocols <i>vstp</i> <i>vlan</i> <i>vlan-id</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols</code> <code> (<i>mstp</i> <i>rstp</i>)],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols</code> <code> <i>vstp</i> <i>vlan</i> <i>vlan-id</i>],</code> <code>[edit protocols (<i>mstp</i> <i>rstp</i>)],</code> <code>[edit protocols <i>vstp</i> <i>vlan</i> <i>vlan-id</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols (<i>mstp</i> <i>rstp</i>)],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols <i>vstp</i> <i>vlan</i> <i>vlan-id</i>]</code>
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Determine the priority of the backup bridge in a VPLS multihomed Layer 2 ring with MPLS infrastructure.
Options	<i>priority</i> —The backup bridge priority can be set only in increments of 4096. Range: 0 through 61,440 Default: 32,768
Required Privilege Level	routing —To view this statement in the configuration. routing-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240• Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning-Tree Behavior on page 250• Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning-Tree Behavior on page 249• Understanding VPLS Multihoming: Priority of the Backup Bridge on page 243

block (Spanning Trees)

Syntax	block;
Hierarchy Level	[edit protocols mstp interface (all <i>interface-name</i>) bpdu-timeout-action], [edit protocols rstp interface (all <i>interface-name</i>) bpdu-timeout-action], [edit protocols stp interface (all <i>interface-name</i>) bpdu-timeout-action], [edit protocols vstp vlan <i>vlan-id</i> interface (all <i>interface-name</i>) bpdu-timeout-action]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches. Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	Configures loop protection on a specific interface.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Understanding Loop Protection for STP, RSTP, VSTP, and MSTP • Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 176 • Understanding VSTP • Understanding VSTP on page 29 • Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217 • Example: Configuring Faster Convergence and Improving Network Stability with RSTP • Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84 • Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree • Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on non-ELS EX Series Switches on page 184 • Example: Configuring Network Regions for VLANs with MSTP • show spanning-tree bridge on page 372 • show spanning-tree interface on page 377

bpdu-destination-mac-address (Spanning Tree)

Syntax	<code>bpdu-destination-mac-address provider-bridge-group;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp)], [edit protocols (mstp rstp)], [edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp)]
Release Information	Statement introduced in Junos OS Release 9.2. Support for logical systems added in Junos OS Release 9.6.
Description	Enable MX Series router to participate in the provider Rapid Spanning Tree Protocol (RSTP) instance or a provider Multiple Spanning Tree Protocol (MSTP) instance.
Default	If the bpdu-destination-mac-address statement is not configured, the bridge participates in the customer RSTP instance, transmitting and receiving standard RSTP BPDU packets.
Options	provider-bridge-group —The destination MAC address of the BPDU packets transmitted is the provider bridge group address 01:80:c2:00:00:08 . Received BPDU packets with this destination MAC address are accepted and passed to the Routing Engine.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding BPDUs Used for Exchanging Information Among Bridges on page 135• Understanding Provider Bridge Participation in RSTP or MSTP Instances on page 31• Configuring Rapid Spanning Tree Protocol on page 62• Configuring Multiple Spanning Tree Protocol on page 54

bpdu-block

Syntax	<pre>bpdu-block { interface (interface-name disable all); disable-timeout seconds; }</pre>
Hierarchy Level	<p>[edit protocols layer2-control]</p> <p>[edit ethernet-switching-options]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	<p>Configures bridge protocol data unit (BPDU) protection on a specified interface or on all interfaces. If the interface receives incompatible BPDUs, it is disabled.</p> <p>If the disable-timeout statement is included in the BPDU configuration, the interface is automatically reenabled after the timer expires. Otherwise, you must use the operational mode command clear bpdu-error to unblock and reenable the interface.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35 • Understanding BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 134 • Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 137 • Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133 • Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167 • Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error (CLI Procedure) on page 147 • Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133 • show spanning-tree bridge on page 372 • show spanning-tree interface on page 377 • clear bpdu-error on page 356

bpdu-block-on-edge

Syntax	<code>bpdu-block-on-edge;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp vstp)],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols</code> <code> (mstp rstp vstp)],</code> <code>[edit protocols (mstp rstp vstp)],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp)]</code>
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches. Statement introduced in Junos OS Release 9.4 for additional devices. Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support. Statement updated in Junos OS Release 11.1 for EX Series switches to change blocking behavior to port shutdown. Support for logical systems added in Junos OS Release 9.6. Statement introduced in Junos OS Release 17.1 for ACX Series routers.
Description	Configure bridge protocol data unit (BPDU) protection on all edge ports of a switch. When the bpdu-block-on-edge statement is configured and the interface encounters an incompatible BPDU, the interface shuts down. If the disable-timeout statement is included in the BPDU configuration, the interface is automatically reenabled after the timer expires. Otherwise, you must use the operational mode command clear bpdu-error to unblock and reenable the interface.
Default	Not enabled.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35• Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133• Understanding BPDU Protection on All Edge Ports of the Bridge on page 136• Configuring BPDU Protection on All Edge Ports on page 145• Configuring BPDU Protection on Switch Spanning Tree Interfaces on page 139• Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217• Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84• Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157

- [rstp on page 332](#)
- [mstp on page 320](#)
- [vstp on page 349](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)
- [clear bpdu-error on page 356](#)

bpdu-timeout-action

Syntax	<pre>bpdu-timeout-action { block; log; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp vstp)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp)],
Switches supporting ELS	[edit protocols mstp interface (all <i>interface-name</i>)], [edit protocols mstp interface (all <i>interface-name</i>) arp-on-stp], [edit protocols rstp interface (all <i>interface-name</i>)], [edit protocols rstp interface (all <i>interface-name</i>) arp-on-stp], [edit protocols stp interface (all <i>interface-name</i>)], [edit protocols stp interface (all <i>interface-name</i>) arp-on-stp], [edit protocols vstp vlan <i>vlan-id interface</i> (all <i>interface-name</i>)], [edit protocols vstp vlan <i>vlan-id interface</i> (all <i>interface-name</i>) arp-on-stp]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches. Statement introduced in Junos OS Release 9.4 for other devices. Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support. Support for logical systems added in Junos OS Release 9.6. Statement introduced in Junos OS Release 17.1 for ACX Series routers.
Description	<p>Provide STP loop protection for a given STP family protocol interface. Configure the BPDU timeout action on a specific interface. You must configure at least one action (log, block, or both).</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Default	If the bpdu-timeout-action statement is not configured, an interface that stops receiving BPDUs will transition to the designated port (forwarding) state, creating a potential loop.
Options	<p>log—The interface logs the fact that it has not received BPDUs during the timeout interval.</p> <p>block—The interface is blocked and the fact that the interface has not received BPDUs during the timeout interval is logged.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Understanding Loop Protection for Spanning-Tree Instance Interfaces on page 175 • Understanding VSTP on page 29 • Configuring Loop Protection for a Spanning-Tree Instance Interface on page 183

- [Example: Enabling Loop Protection for Spanning-Tree Protocols on page 183](#)
- [Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217](#)
- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
- [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 184](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)
- [rstp on page 332](#)
- [mstp on page 320](#)
- [vstp on page 349](#)

bridge-priority

Syntax	<code>bridge-priority <i>priority</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp)],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols mstp msti <i>msti-id</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols vstp vlan <i>vlan-id</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mstp msti <i>msti-id</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp)],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols mstp msti <i>msti-id</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i>]</p> <p>[edit protocols mstp],</p> <p>[edit protocols mstp msti <i>msti-id</i>],</p> <p>[edit protocols rstp],</p> <p>[edit protocols stp],</p> <p>[edit protocols vstp vlan <i>vlan-id</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	<p>Configures the bridge priority, which determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.</p>
Default	32,768
Options	<p>priority—The bridge priority can be set only in increments of 4096.</p> <p>Range: 0 through 61,440</p> <p>Default: 32,768</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding MSTP on page 48 • Understanding VSTP on page 29 • Understanding Bridge Priority for Election of Root Bridge and Designated Bridge on page 242

- [Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195](#)
- [Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)

configuration-name


Syntax	<code>configuration-name <i>configuration-name</i>;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> protocols mstp],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i></code> <code>protocols mstp],</code> <code>[edit protocols mstp],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols mstp]</code>
Release Information	Statement introduced in Junos OS Release 8.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for logical systems added in Junos OS Release 9.6. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Specify the configuration name, which is the MSTP region name carried in the MSTP BPDUs.
Required Privilege Level	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding MSTP on page 48• Understanding BPDUs Used for Exchanging Information Among Bridges on page 135• Configuring Multiple Spanning Tree Protocol on page 54• Configuring MSTP on Switches on page 51• Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217• Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84• show spanning-tree bridge on page 372• show spanning-tree interface on page 377• Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195• Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66• Understanding MSTP on page 48

cost

Syntax	<code>cost cost;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols mstp msti msti-id interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols vstp vlan vlan-id interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mstp msti msti-id interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vstp vlan vlan-id interface <i>interface-name</i>],</p> <p>[edit protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit protocols mstp msti msti-id interface <i>interface-name</i>],</p> <p>[edit protocols vstp vlan vlan-id interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols mstp msti msti-id interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vstp vlan vlan-id interface <i>interface-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p>
Description	For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), configure the link cost to control which bridge is the designated bridge and which interface is the designated interface.
Default	The link cost is determined by the link speed.
Options	<p>cost—(Optional) Link cost associated with the port.</p> <p>Range: 1 through 200,000,000</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Spanning-Tree Instance Interface on page 33 • Understanding Spanning-Tree Instance Interface Cost on page 34

- [Understanding STP on page 26](#)
- [Understanding RSTP on page 21](#)
- [Understanding MSTP on page 48](#)
- [Understanding VSTP on page 29](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)

disable

Syntax	<code>disable;</code>
Hierarchy Level	<pre> [edit logical-systems <i>logical-system-name</i> protocols mstp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mstp], [edit protocols mpls], [edit protocols mpls interface (all <i>interface-name</i>)], [edit protocols mstp], [edit protocols mstp (all <i>interface-name</i>)], [edit protocols mstp (all <i>interface-name</i>) arp-on-stp], [edit protocols mstp msti <i>msti-id</i> vlan (<i>vlan-id</i> <i>vlan-name</i>) interface (all <i>interface-name</i>)], [edit protocols mstp msti <i>msti-id</i> vlan (<i>vlan-id</i> <i>vlan-name</i>) interface <i>interface-name</i> arp-on-stp], [edit protocols rstp], [edit protocols rstp interface (all <i>interface-name</i>)], [edit protocols rstp interface (all <i>interface-name</i>) arp-on-stp], [edit protocols stp], [edit protocols stp interface (all <i>interface-name</i>)], [edit protocols stp interface (all <i>interface-name</i>) arp-on-stp], [edit protocols vstp], [edit protocols vstp vlan <i>vlan-id</i> interface (all <i>interface-name</i>)], [edit protocols vstp vlan <i>vlan-id</i> interface (all <i>interface-name</i>) arp-on-stp], [edit protocols mstp interface <i>interface-name</i>], [edit protocols mstp msti <i>msti-id</i> vlan (all <i>vlan-id</i> <i>vlan-name</i>) interface <i>interface-name</i>], [edit protocols rstp interface <i>interface-name</i>], [edit protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>] [edit routing-instances <i>routing-instance-name</i> protocols mstp] [edit ethernet-switching-options bpdu-block interface]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.</p> <p>Statement introduced in Junos OS Release 12.2 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p> <p>Statement updated in Junos OS Release 15.1 for EX Series switches.</p>
Description	Disable the entire MSTP, RSTP, or VSTP instance on a specific interface.
<div>  NOTE: You cannot disable spanning tree parameters for all interfaces. </div>	
Default	Not enabled

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

Related Documentation


- [Understanding RSTP on page 21](#)
- [Understanding VSTP on page 29](#)
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [Configuring VLAN Spanning Tree Protocol on Switches on page 111](#)
- [Configuring RSTP on EX Series Switches \(CLI Procedure\) on page 65](#)
- [Configuring MSTP on Switches on page 51](#)
- [Disabling MSTP on page 59](#)
- [Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167](#)
- [Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195](#)
- [Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66](#)
- [interface on page 305](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)

disable-timeout

Syntax	<code>disable-timeout <i>seconds</i>;</code>
Hierarchy Level	<p>[edit protocols layer2-control bpdud-block]</p> <p>[edit ethernet-switching-options bpdud-block]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 9.4.</p>
Description	<p>For interfaces configured for BPDU protection, specify the amount of time an interface receiving BPDUs is disabled.</p> <p>Configure the timeout value to periodically check to see if an interface is still disabled with BPDU blocking. If this option is not configured, the interface is not periodically checked and remains disabled.</p>
Default	The disable timeout is not enabled.
Options	<p><i>seconds</i>—Amount of time, in seconds, the interface receiving BPDUs is disabled. Once the timeout expires, the interface is brought back into service.</p> <p>Range: 10 through 3600</p> <p>Default: If this option is not configured, the interface is not periodically checked and remains disabled.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p> <p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35 • Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133 • Understanding BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 134 • Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217 • Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84 • Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167 • Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195

- [Example: Configuring BPDU Protection on Switch Edge Interfaces to Prevent STP Miscalculations on page 152](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)

drop (BPDU Block)

Syntax	drop;
Hierarchy Level	[edit ethernet-switching-options bpdu-block bpdu-block (all [<i>interface-name</i>])]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Drop bridge protocol data units (BPDUs) that enter any interface or a specified interface, but do not disable the interface. Configure the drop statement <i>only</i> on interfaces on which no spanning-tree protocol (STP, MSTP, or RSTP) is configured.
	<div> NOTE: Do not configure drop on any interface on which a spanning-tree protocol has been configured. Doing so could cause STP misconfiguration and consequent network outages.</div>
Default	Not enabled.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133• Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157• Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167• bpdu-block-on-edge on page 284

edge

Syntax `edge;`

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

 [edit protocols (**mstp** | **rstp** | **vstp**) **interface** (all | *interface-name*)],)arp-on-stp],
 [edit protocols **mstp msti msti-id** **interface** (all | *interface-name*)],)arp-on-stp],
 [edit protocols **vstp vlan vlan-id** **interface** (all | *interface-name*)],)arp-on-stp],

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

Release Information Statement introduced in Junos OS Release 8.4.
 Statement introduced in Junos OS Release 9.0 for EX Series switches.
 Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
 Support for logical systems added in Junos OS Release 9.6.
 Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description For Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), configure interfaces as edge ports or edge interfaces. Edge ports do not expect to receive BPDUs. If a BPDU is received, the port becomes a nonedge port and the Edge interfaces immediately transition to a forwarding state.



NOTE: Although the edge configuration statement appears in the [edit protocols stp interface (all | *interface-name*)] or [edit protocols rstp force-version stp interface (all | *interface-name*)] hierarchy on the switch, this statement has no effect on the switch operation if you configure it.

Default Edge interfaces are not enabled.

Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding STP on page 26• Understanding VSTP on page 29• Understanding Spanning-Tree Instance Interface on page 33• Configuring a Spanning-Tree Instance Interface as an Edge Port for Faster Convergence on page 42• Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195• Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66• Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217• Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84• show spanning-tree bridge on page 372• show spanning-tree interface on page 377

enable-all-ifl

Syntax	enable-all-ifl;
Hierarchy Level	[edit protocols layer2-control mac-rewrite interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	Enable tunneling for STP, VTP, CDP, and other supported protocols on all logical interfaces (VLANs) configured on the interface.



NOTE: Tunneling on all logical interfaces is enabled automatically for PVST/PVST+.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Layer 2 Protocol Tunneling Through a Network on page 263• Understanding Layer 2 Protocol Tunneling on EX Series Switches• protocol on page 328

extended-system-id

Syntax	<code>extended-system-id <i>identifier</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols rstp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols rstp],</p> <p>[edit protocols rstp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols rstp]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p>
Description	The extended system ID is used to specify different bridge identifiers for different RSTP or STP routing instances.
Options	<p><i>identifier</i>—Specify the system identifier to use for the RSTP or STP instance.</p> <p>Range: 0 through 4095</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Rapid Spanning Tree Protocol on page 62 • Configuring RSTP on EX Series Switches (CLI Procedure) on page 65 • Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66 • Understanding RSTP on page 21

force-version (IEEE 802.1D STP)

Syntax	force-version stp;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols (rstp vstp)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (rstp vstp)], [edit protocols (rstp vstp)], [edit routing-instances <i>routing-instance-name</i> protocols (rstp vstp)]
Release Information	Statement introduced in Junos OS Release 8.4. Statement introduced in Junos OS Release 9.4 for EX Series switches. Support for logical systems added in Junos OS Release 9.6. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Support for logical systems added in Junos OS Release 9.6.
Description	Forces the spanning-tree version to be the original IEEE 803.1D STP protocol.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 103• Understanding VSTP on page 29• Understanding VSTP on page 29• Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 103• show spanning-tree bridge on page 372• show spanning-tree interface on page 377

forward-delay

Syntax	<code>forward-delay seconds;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp)], [edit logical-systems <i>logical-system-name</i> protocols vstp vlan <i>vlan-id</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i>],</p> <p>[edit protocols (mstp rstp)], [edit protocols vstp vlan <i>vlan-id</i>], [edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp)], [edit routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specifies the length of time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Options	<p>seconds—(Optional) Number of seconds the bridge port remains in the listening and learning states.</p> <p>Range: 4 through 30</p> <p>Default: 15 seconds</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Forward Delay Before Ports Transition to Forwarding State on page 36 • Understanding STP on page 26 • Understanding MSTP on page 48 • Understanding VSTP on page 29 • Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195 • Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66 • Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84

- [Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)

hello-time

Syntax	<code>hello-time seconds;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp)],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols vstp vlan <i>vlan-id</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i>],</p> <p>[edit protocols (mstp rstp)],</p> <p>[edit protocols vstp vlan <i>vlan-id</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp)],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p>
Description	For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specifies the number of seconds between transmissions of configuration BPDUs by the root bridge.
Default	2 seconds
Options	<p>seconds—(Optional) Number of seconds between transmissions of configuration BPDUs.</p> <p>Range: 1 through 10</p> <p>Default: 2 seconds</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Hello Time for Root Bridge to Transmit Hello BPDUs on page 136 • Understanding MSTP on page 48 • Understanding VSTP on page 29 • Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195 • Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217 • Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66

- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)

interface (BPDU Blocking)

Syntax	interface (all [<i>interface-name</i>]);
Hierarchy Level	[edit protocols layer2-control bpdu-block] [edit ethernet-switching-options bpdu-block]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches. Statement introduced in Junos OS Release 9.4. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	<p>Applies Bridge Protocol Data Unit (BPDU) protection on all interfaces or on one or more specified interfaces.</p> <p>Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP) provide Layer 2 loop prevention for EX Series switches. The spanning-tree protocols use BPDU frames to communicate. Through their exchange, spanning-tree topologies determine which interfaces block traffic and which interfaces become root ports and forward traffic. User bridge applications running on a PC can also generate BPDUs. If these BPDUs are picked up by STP applications running on the switch, they can trigger STP miscalculations that can lead to network outages.</p> <p>To block outside BPDUs from reaching a switch interface connected to devices that are not part of a spanning-tree topology, configure BPDU protection on interfaces in the topology.</p>



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



NOTE: Interfaces that are configured as edge interfaces can transition to a forwarding state immediately because they cannot create network loops. As edge ports are connected to end devices, it is imperative that you configure BPDU protection on edge ports to protect the switch from outside BPDUs. When BPDU protection is enabled on an edge interface, the interface shuts down on encountering an outside BPDU thereby preventing any traffic from passing through the interface. To enable BPDU protection on an edge interface, see [“Configuring BPDU Protection on an EX Series Interface \(CLI Procedure\)”](#) on page 140

Options **all**—All interfaces.

[*interface-name*]—One or more Ethernet interface names.

The remaining statements are explained separately. See [CLI Explorer](#).

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

- | | |
|------------------------------|---|
| Related Documentation | <ul style="list-style-type: none">• Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133• Understanding BPDU Protection for Spanning-Tree Instance Interfaces on page 35• Understanding BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 134• Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 137• Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217• Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84• Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 167• show spanning-tree bridge on page 372• show spanning-tree interface on page 377 |
|------------------------------|---|

interface (Spanning Tree)

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

Syntax `interface interface-name {
 arp-on-stp;
 bpdu-timeout-action
 block;
 log;
 cost cost;
 disable;
 edge;
 mode mode;
 no-root-port;
 priority priority;
 }`

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

Release Information Statement introduced in Junos OS Release 8.4.
 Statement introduced in Junos OS Release 9.0 for EX Series switches.
 Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
 Support for logical systems added in Junos OS Release 9.6.
 Statement introduced in Junos OS Release 11.1 for the QFX Series.
 Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
 Statement updated in Junos OS Release 15.1 for EX Series switches to support
 configuration of spanning tree parameters globally on all interfaces.



NOTE: You cannot disable spanning tree parameters globally on all interfaces.

Description	Configures the interface to participate in the RSTP, MSTP, or VSTP instance. The edge , mode , and no-root-port options are not available at the <code>[edit protocols mstp msti <i>msti-id</i>]</code> hierarchy level.
Options	<i>interface-name</i> —Name of a Gigabit Ethernet or 10-Gigabit Ethernet interface. The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Spanning-Tree Instance Interface on page 33• Understanding RSTP on page 21• Understanding MSTP on page 48• Understanding VSTP on page 29• Configuring RSTP on EX Series Switches (CLI Procedure) on page 65• Configuring MSTP on Switches on page 51• Configuring VLAN Spanning Tree Protocol on Switches on page 111• Configuring VSTP on EX Series Switches (CLI Procedure) on page 113• Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217• Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84• show spanning-tree bridge on page 372• show spanning-tree interface on page 377

layer2-control

Syntax

```
layer2-control {
  bpd-block {
    disable-timeout seconds;
    interface interface-name;
  }
  mac-rewrite {
    interface interface-name {
      enable-all-ifl;
      protocol protocol-name;
    }
  }
  nonstop-bridging;
  traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag <disable>;
  }
}
```

Hierarchy Level [edit protocols]

Release Information Statement introduced in Junos OS Release 8.4.
bpd-block statement added in Junos OS Release 9.4.
enable-all-if statement added in Junos OS Release 13.3.
Statement introduced in Junos OS Release 14.1X53-D10 for EX4300 switches.
Statement introduced in Junos OS Release 15.1X53-D50 for EX2300 and EX3400 switches.
Statement introduced in Junos OS Release 17.4R1 for EX4600 switches.

Description Configure Layer 2 control protocols to enable features such as Layer 2 protocol tunneling or nonstop bridging.

The remaining statements are explained separately. See [CLI Explorer](#).



NOTE: For a detailed description of configuring the nonstop-bridging statement, see the *Junos OS High Availability Library for Routing Devices*. When this statement is configured on routing platforms with two Routing Engines, a master Routing Engine switches over gracefully to a backup Routing Engine and preserves Layer 2 Control Protocol (L2CP) information.

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

Related Documentation

- [Understanding Layer 2 Protocol Tunneling Through a Network on page 263](#)
- [Understanding Layer 2 Protocol Tunneling Configuration Guidelines on page 265](#)

- [Configuring Layer 2 Protocol Tunneling on page 266](#)
- [Understanding Layer 2 Protocol Tunneling on EX Series Switches](#)
- [Configuring Layer 2 Protocol Tunneling on EX Series Switches with ELS Support \(CLI Procedure\)](#)
- *instance-type*

log (Spanning Trees)

Syntax	log;
Hierarchy Level	[edit protocols mstp interface (all <i>interface-name</i>) bpdu-timeout-action], [edit protocols rstp interface (all <i>interface-name</i>) bpdu-timeout-action], [edit protocols stp interface (all <i>interface-name</i>) bpdu-timeout-action], [edit protocols vstp vlan <i>vlan-id</i> interface (all <i>interface-name</i>) bpdu-timeout-action]
Release Information	Statement introduced in Junos OS Release 9.1 for EX Series switches. Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Description	For interfaces configured for loop protection, configure the software to generate a message to be sent to the system log file /var/log/messages to record the loop-protection event.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• show spanning-tree bridge on page 372• show spanning-tree interface on page 377• Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217• Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84• 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 184• Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 176• Understanding VSTP on page 29

mac-rewrite

Syntax	<pre> mac-rewrite { interface <i>interface-name</i> { enable-all-ifl; protocol <i>protocol-name</i>; } } </pre>
Hierarchy Level	[edit protocols layer2-control]
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>enable-all-if statement added in Junos OS Release 13.3.</p> <p>Support for PVSTP protocol introduced in Junos OS Release 13.3 for MX Series routers and EX9200 switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D10 for EX4300 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D55 for EX2300 and EX3400 switches.</p> <p>Statement introduced in Junos OS Release 17.4R1 for EX4600 switches.</p>
Description	<p>Enable rewriting of the MAC address for Layer 2 protocol tunneling. When a control packet for a supported protocol is received on a service provider edge port configured for Layer 2 protocol tunneling (L2PT), the multicast destination MAC address is rewritten with the predefined multicast tunneling MAC address of 01:00:0c:cd:cd:d0. The packet is transported across the provider network transparently to the other end of the tunnel, and the original multicast destination MAC address is restored when the packet is transmitted.</p> <p>Refer to protocol for the list of protocols that can be configured for L2PT on different devices.</p> <p>To see the protocols for which L2PT tunneling is enabled for an interface, enter the show mac-rewrite interface command.</p> <p>On MX Series routers and EX9200 switches with L2PT configured, customer-facing ports should not receive packets with the L2PT MAC address as the destination address unless there is a network topology or configuration error. Any such interface receiving an L2PT packet becomes “Disabled”, and must subsequently be re-enabled using the clear error mac-rewrite command.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Layer 2 Protocol Tunneling Through a Network on page 263 • Understanding Layer 2 Protocol Tunneling on EX Series Switches

- *Configuring Layer 2 Protocol Tunneling on EX Series Switches with ELS Support (CLI Procedure)*
- [show mac-rewrite interface on page 370](#)
- [clear error mac-rewrite on page 358](#)

max-age


Syntax	<code>max-age seconds;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp)], [edit logical-systems <i>logical-system-name</i> protocols vstp vlan <i>vlan-id</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i>],</p> <p>[edit protocols mstp], [edit protocols rstp], [edit protocols stp], [edit protocols vstp vlan <i>vlan-id</i>]</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp)], [edit routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specifies the maximum expected arrival time of hello BPDUs.
Default	20 seconds
Options	<p><i>seconds</i>—(Optional) Number of seconds expected between hello BPDUs.</p> <p><i>seconds</i>—The maximum age of received protocol BPDUs.</p> <p>Range: 6 through 40</p> <p>Default: 20 seconds</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Maximum Age for Awaiting Arrival of Hello BPDUs on page 136 • Understanding STP on page 26 • Understanding MSTP on page 48 • Understanding VSTP on page 29 • Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195

- [Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217](#)
- [Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66](#)
- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)

max-hops

Syntax	<code>max-hops <i>hops</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols mstp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mstp], [edit protocols mstp], [edit routing-instances <i>routing-instance-name</i> protocols mstp]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for logical systems added in Junos OS Release 9.6. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	Configure the maximum number of hops a BPDU can be forwarded in the MSTP region.
Options	<p><i>hops</i>—(Optional) Number of hops the BPDU can be forwarded. Range: 1 through 255 Default: 19 hops20 hops</p>
Required Privilege Level	<p>routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding MSTP on page 48 • Configuring Multiple Spanning Tree Protocol on page 54 • Configuring MSTP on Switches on page 51 • Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195 • Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217 • Understanding MSTP on page 48 • show spanning-tree bridge on page 372 • show spanning-tree interface on page 377

mode

Syntax	<code>mode (p2p shared);</code>
Hierarchy Level	<pre>[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>], [edit protocols (mstp rstp vstp) interface <i>interface-name</i>], [edit protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>], [edit protocols mstp interface (all <i>interface-name</i>) arp-on-stp], [edit protocols mstpmsti <i>msti-id</i> interface <i>interface-name</i>) arp-on-stp], [edit protocols rstp interface (all <i>interface-name</i>) arp-on-stp], [edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>] [edit protocols stp interface (all (all <i>interface-name</i>))], [edit protocols stp interface (all <i>interface-name</i>) arp-on-stp], [edit protocols vstp vlan <i>vlan-id</i> interface (all <i>interface-name</i>) arp-on-stp]</pre>
Release Information	<p>Statement introduced in Junos OS Release 8.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), configures the link mode to identify point-to-point links.
Default	When the link is configured as full-duplex, the default link mode is p2p . When the link is configured half-duplex, the default link mode is shared .
<div>  NOTE: For EX4300 switches, the interfaces operate in full-duplex mode only. </div>	
Options	<p>p2p—The link is point to point.</p> <p>shared—The link is shared media.</p>

Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Spanning-Tree Instance Interface on page 33• Understanding Spanning-Tree Instance Interface Point-to-Point Link Mode on page 35• Understanding STP on page 26• Understanding VSTP on page 29• Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195• Example: Configuring Faster Convergence and Improved Network Stability on Switches with RSTP on page 66• Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217• Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84• show spanning-tree bridge on page 372• show spanning-tree interface on page 377

msti

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

Syntax `msti msti-id {
 vlan (vlan-id | vlan-name);
 interface interface-name {
 disable-timeout;
 cost cost;
 priority priority;
 }
}`

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

Release Information Statement introduced in Junos OS Release 8.4.
 Statement introduced in Junos OS Release 9.0 for EX Series switches.
 Support for logical systems added in Junos OS Release 9.6.
 Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
 Statement updated in Junos OS Release 15.1 for EX Series switches to support configuration of spanning tree parameters globally on all interfaces.



NOTE: You cannot disable spanning tree parameters globally on all interfaces.

Description Configures the Multiple Spanning Tree Instance (MSTI) identifier for Multiple Spanning Tree Protocol (MSTP). MSTI IDs are local to each region, so you can reuse the same MSTI ID in different regions.

Default MSTI is disabled.

Options *msti-id*—MSTI instance identifier.
Range: 1 through 64

Range: 1 through 4094. The Common Instance Spanning Tree (CIST) is always MSTI 0.

The remaining statements are explained separately. See [CLI Explorer](#).

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

- | | |
|------------------------------|---|
| Related Documentation | <ul style="list-style-type: none">• Understanding MSTP on page 48• Configuring Multiple Spanning Tree Protocol on page 54• Configuring MSTP on Switches on page 51• Configuring MSTP Instances on a Physical Interface on page 58• Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195• Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217• Understanding MSTP on page 48• show spanning-tree bridge on page 372• show spanning-tree interface on page 377 |
|------------------------------|---|

mstp

List of Syntax [MX Series on page 320](#)
 [EX Series on page 320](#)
 [QFX Series, EX Series on page 322](#)

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

EX Series `mstp {
 bpdu-block-on-edge;
 bridge-priority priority;
 configuration-name name;
 disable;
 forward-delay seconds;
 hello-time seconds;
 interface (all | interface-name){
 arp-on-stp;
 bpdu-timeout-action {`


```
    block;
    log;
}
cost cost;
disable;
edge;
mode mode;
no-root-port;
priority priority;
}
max-age seconds;
max-hops hops;
msti msti-id {
    vlan (vlan-id | vlan-name);
    interface interface-name {
        disable;
        cost cost;
        priority priority;
    }
}
revision-level revision-level;
traceoptions {
    file filename <files number > <size size > <no-stamp | world-readable |
    no-world-readable>;
    flag flag;
}
}
```

```

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

```

Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols], [edit protocols], [edit routing-instances <i>routing-instance-name</i> protocols]
Release Information	Statement introduced in Junos OS Release 8.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. bpdud-block-on-edge statement added in Junos OS Release 9.4. bpdud-timeout-action statement added in Junos OS Release 9.4. Support for logical systems added in Junos OS Release 9.6.
Description	Configures Multiple Spanning Tree Protocol (MSTP). MSTP is defined in the IEEE 802.1Q-2003 specification and is used to create a loop-free topology in networks with multiple spanning tree regions. The remaining statements are explained separately. See CLI Explorer .
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding MSTP on page 48• Configuring Multiple Spanning Tree Protocol on page 54• Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217• show spanning-tree bridge on page 372• show spanning-tree interface on page 377

no-root-port

Syntax	no-root-port;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>],</p> <p>[edit protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>],</p> <p>[edit protocols mstp interface (all <i>interface-name</i>) arp-on-stp],</p> <p>[edit protocols rstp interface (all <i>interface-name</i>) arp-on-stp],</p> <p>[edit protocols stp interface (all <i>interface-name</i>) arp-on-stp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>]</p> <p>[edit protocols vstp vlan <i>vlan-id</i> interface (all <i>interface-name</i>) arp-on-stp]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 17.1 for ACX Series routers.</p>
Description	<p>Configures an interface to be a spanning-tree designated port. If the bridge receives superior STP bridge protocol data units (BPDUs) on a root-protected interface, that interface transitions to a root-prevented STP state (inconsistency state) and the interface is blocked. This blocking prevents a bridge from being elected the root bridge. When the bridge stops receiving superior STP BPDUs on the root-protected interface, interface traffic is no longer blocked.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding VSTP on page 29 • Understanding Root Protection for Spanning-Tree Instance Interfaces in a Layer 2 Switched Network on page 247 • Enabling Root Protection for a Spanning-Tree Instance Interface on page 248 • Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on non-ELS EX Series Switches on page 251

- [Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217](#)
- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)

priority (Protocols STP)

Syntax	<code>priority interface-priority;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols mstp msti <i>msti-id</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mstp msti <i>msti-id</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>],</p> <p>[edit protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit protocols mstp msti <i>msti-id</i> interface <i>interface-name</i>],</p> <p>[edit protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>],</p> <p>[edit protocols mstp ;interface (all <i>interface-name</i>) arp-on-stp],</p> <p>[edit protocols mstpmsti <i>msti-id</i> interface <i>interface-name</i> arp-on-stp],</p> <p>[edit protocols rstp interface (all <i>interface-name</i>) arp-on-stp],</p> <p>[edit protocols stp interface (all <i>interface-name</i>) arp-on-stp],</p> <p>[edit protocols vstp vlan <i>vlan-id</i> interface (all <i>interface-name</i>) arp-on-stp]</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp) interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols mstp msti <i>msti-id</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vstp vlan <i>vlan-id</i> interface <i>interface-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specifies the interface priority to control which interface is elected as the root port. The interface priority must be set in increments of 16.
Default	The default value is 128.
Options	<p>priority—(Optional) Interface priority. The interface priority must be set in increments of 16.</p> <p>Range: 0 through 240</p>

Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Understanding Spanning-Tree Instance Interface on page 33 • Understanding Spanning-Tree Instance Interface Priority on page 34 • Understanding STP on page 26 • Understanding VSTP on page 29 • Configuring a Spanning-Tree Instance Interface as an Edge Port for Faster Convergence on page 42 • Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217 • Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84 • show spanning-tree bridge on page 372 • show spanning-tree interface on page 377

priority-hold-time

Syntax	<code>priority-hold-time <i>seconds</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp)], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp)], [edit protocols (mstp rstp)], [edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp)],
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Specify the number of seconds to hold before switching to the primary priority when the first core domain comes up.
Options	<i>seconds</i> —Number of seconds to hold before switching to primary priority. Range: 1 through 255 Default: 2 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Understanding VPLS Multihoming: Hold Time Before Switching to Primary Priority on page 243

protocol

List of Syntax	Syntax (MX Series Routers) on page 328 Syntax (EX2300 and EX3400 Switches) on page 328 Syntax (EX4300 and EX4600 Switches) on page 328 Syntax (EX9200 Switches) on page 328
Syntax (MX Series Routers)	<code>protocol (cdp pvstp stp vtp);</code>
Syntax (EX2300 and EX3400 Switches)	<code>protocol (cdp gvrp ieee8023ah lacp lldp mvrp stp vstp vtp);</code>
Syntax (EX4300 and EX4600 Switches)	<code>protocol (cdp elmi gvrp ieee8021x ieee8023ah lacp lldp mmrp mvrp stp udld vstp vtp);</code>
Syntax (EX9200 Switches)	<code>protocol (cdp elmi gvrp ieee8021x ieee8023ah lacp lldp mmrp mvrp pvstp stp udld vtp);</code>
Hierarchy Level	[edit logical-systems <i>name</i> protocols layer2-control mac-rewrite interface <i>interface-name</i>], [edit protocols layer2-control mac-rewrite interface <i>interface-name</i>]
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p> <p>Support for PVST/PVST+ introduced in Junos OS Release 13.3 for MX Series routers and EX9200 switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D10 for EX4300 switches</p> <p>Statement introduced in Junos OS Release 15.1X53-D55 for EX2300 and EX3400 switches.</p> <p>Support for E-LMI, IEEE 802.1X, MMRP, and UDLD introduced in Junos OS Release 17.3R1 for EX4300 switches.</p> <p>Support for E-LMI, GVRP, IEEE 802.1x, IEEE 802.3AH, LACP, LLDP, MMRP, MVRP, and UDLD introduced in Junos OS Release 17.3R1 for EX9200 switches.</p> <p>Statement introduced in Junos OS Release 17.4R1 for EX4600 switches.</p>
Description	<p>Configure the protocol to be tunneled on an interface for Layer 2 protocol tunneling (L2PT). To enable tunneling multiple protocols, include multiple protocol statements.</p> <p>Not all protocols listed in the Options section can be tunneled on all devices. The Syntax and Release Information sections list the available options for the protocols that can be tunneled by different devices as of a particular Junos OS release.</p> <p>When a control packet for a supported protocol is received on a service provider edge port configured for Layer 2 protocol tunneling (L2PT), the multicast destination MAC address is rewritten with the predefined multicast tunneling MAC address of 01:00:0c:cd:cd:d0. The packet is transported across the provider network transparently to the other end of the tunnel, and the original multicast destination MAC address is restored when the packet is transmitted.</p>

Options	<p>cdp—Tunnel the Cisco Discovery Protocol (CDP).</p> <p>elmi—Tunnel Ethernet Local Management Interface (E-LMI) packets.</p> <p>gvrp—Tunnel Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) packets.</p> <p>ieee8021x—Tunnel IEEE 802.1X authentication packets.</p> <p>ieee8023ah—Tunnel IEEE 802.3AH Operation, Administration, and Maintenance (OAM) link fault management (LFM) packets.</p> <p>lACP—Tunnel Link Aggregation Control Protocol (LACP) packets.</p> <p>lldp—Tunnel Link Layer Discovery Protocol (LLDP) packets.</p> <p>mmrp—Tunnel Multiple MAC Registration Protocol (MMRP) packets.</p> <p>mvrp—Tunnel Multiple VLAN Registration Protocol (MVRP) packets.</p> <p>pvstp—Tunnel VLAN Spanning Tree Protocol (VSTP), Per-VLAN Spanning Tree (PVST), and Per-VLAN Spanning Tree Plus (PVST+) Protocol packets.</p> <p>stp—Tunnel packets for all versions of Spanning-Tree Protocols.</p> <p>udld—Tunnel Unidirectional Link Detection (UDLD) packets.</p> <p>vstp—Tunnel VLAN Spanning Tree Protocol (VSTP) packets.</p> <p>vtp—Tunnel VLAN Trunking Protocol (VTP) packets.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding Layer 2 Protocol Tunneling Through a Network on page 263 • Understanding Layer 2 Protocol Tunneling Configuration Guidelines on page 265 • Configuring Layer 2 Protocol Tunneling on page 266 • <i>Understanding Layer 2 Protocol Tunneling on EX Series Switches</i> • <i>Configuring Layer 2 Protocol Tunneling on EX Series Switches with ELS Support (CLI Procedure)</i>

protocols (STP Type)

Syntax	<pre>protocols { mstp { ... } rstp { ... } vstp { ... } }</pre>
Hierarchy Level	[edit], [edit logical-systems <i>logical-system-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>], [edit routing-instances <i>routing-instance-name</i>]
Release Information	Statement introduced in Junos OS Release 8.4. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Support for logical systems added in Junos OS Release 9.6.
Description	Configure the Spanning Tree Protocol type as MSTP, RSTP, or VSTP.
Options	mstp —Configure the protocol as Multiple Spanning Tree. rstp —Configure the protocol as Rapid Spanning Tree. vstp —Configure the protocol as VLAN Spanning Tree.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RSTP on EX Series Switches (CLI Procedure) on page 65• Configuring MSTP on Switches on page 51• Configuring MSTP Instances on a Physical Interface on page 58• Configuring VLAN Spanning Tree Protocol on Switches on page 111• Configuring Rapid Spanning Tree Protocol on page 62• Configuring Multiple Spanning Tree Protocol on page 54• Configuring VLAN SpanningTree Protocol on page 106• Understanding MSTP on page 48

revision-level

Syntax	<code>revision-level <i>revision-level</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols mstp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mstp], [edit protocols mstp], [edit routing-instances <i>routing-instance-name</i> protocols mstp]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for logical systems added in Junos OS Release 9.6. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	For Multiple Spanning Tree Protocol (MSTP), set the revision number of the MSTP configuration.
Options	<p><i>revision-level</i>—Configure the revision number of the MSTP region configuration. Range: 0 through 65,535</p>
Required Privilege Level	<p>routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Understanding MSTP on page 48 • Configuring Multiple Spanning Tree Protocol on page 54 • Example: Configuring Network Regions for VLANs with MSTP on Switches on page 195 • Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217 • show spanning-tree bridge on page 372 • show spanning-tree interface on page 377

rstp

List of Syntax [MX Series on page 332](#)
 [EX Series on page 332](#)
 [ELS Versions: EX Series, QFX Series, NFX Series on page 333](#)

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

EX Series `rstp {`
 `bpdublockonedge;`
 `bridgepriority priority; priority;`
 `disable;`
 `forward-delay seconds;`
 `hellotime seconds;`
 `interface (all | interface-name) {`
 `arp-on-stp;`
 `bpdu-timeout-action {`
 `block;`
 `log;`
 `}`
 `cost cost;`
 `edge;`
 `mode mode;`
 `no-root-port;`
 `priority priority;`
 `}`
 `max-age seconds;`
 `traceoptions {`

```

    file filename <files number > <size size > <no-stamp | no-world-readable |
      world-readable>;
    flag flag;
  }
}

```

ELS Versions: EX Series, QFX Series, NFX Series

```

rstp {
  bpdu-block-on-edge;
  bpdu-destination-mac-address provider-bridge-group;
  bridge-priority priority;
  disable;
  extended-system-id;
  force-version stp;
  forward-delay seconds;
  hello-time seconds;
  max-age seconds;
  priority-hold-time seconds;
  traceoptions {
    file filename <files number > <size size > <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
}

```

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

Release Information Statement introduced in Junos OS Release 8.4.
 Statement introduced in Junos OS Release 9.0 for EX Series switches.
bpd~~u~~-block-on-edge statement added in Junos OS Release 9.4.
bpd~~u~~-timeout-action statement added in Junos OS Release 9.4.
 Support for logic systems added in Junos OS Release 9.6.
 Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
 Statement updated in Junos OS Release 15.1 for EX Series and QFX Series switches to support configuration of spanning tree parameters globally on all interfaces.



NOTE: You cannot disable spanning tree parameters globally on all interfaces.

Description Configure Rapid Spanning Tree Protocol (RSTP). RSTP is defined in the IEEE 802.1D-2004 specification and is used to prevent loops in Layer 2 networks, which results in shorter convergence times than those provided by basic Spanning Tree Protocol (STP).

VSTP and RSTP can be configured concurrently. You can selectively configure up to 253 VLANs using VSTP; the remaining VLANs will be configured using RSTP. VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on the switch. See [“Configuring VSTP on EX Series Switches \(CLI Procedure\)” on page 113](#) for more information on configuring VSTP and RSTP concurrently.



BEST PRACTICE: Configure RSTP when you configure VSTP. RSTP overhead is minimal and this configuration ensures that a spanning-tree protocol is running on all VLANs on your switch, even when your switch is supporting more than 253 VLANs.

The remaining statements are explained separately. See [CLI Explorer](#).

Default RSTP is enabled on all Ethernet switching interfaces.

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

Related Documentation

- [Configuring Rapid Spanning Tree Protocol on page 62](#)
- [Understanding RSTP on page 21](#)
- [Configuring RSTP on EX Series Switches \(CLI Procedure\) on page 65](#)
- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)


shutdown (BPDU Block)

Syntax	shutdown;
Hierarchy Level	[edit ethernet-switching-options bpdu-block interface (all [<i>interface-name</i>])]
Release Information	Statement introduced in Junos OS Release 12.2 for EX Series switches.
Description	Shut down all or specified interfaces to prevent spanning-tree protocol BPDUs (for STP, MSTP, RSTP, and VSTP) from entering the interfaces on which BPDU protection is configured.
Default	Not enabled
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133• Unblocking an Interface on non-ELS EX Series Switches That Receives BPDUs in Error (CLI Procedure) on page 147

stp

Syntax `stp {`
 `disable;`
 `bridge-priority` *priority*;
 `forward-delay` *seconds*;
 `hello-time` *seconds*;
 `interface` (all | *interface-name*) {
 `disable;`
 `bpdu-timeout-action` {
 `block;`
 `alarm;`
 }
 `cost` *cost*;
 `edge;`
 `mode` *mode*;
 `no-root-port;`
 `priority` *priority*;
 }
 `max-age` *seconds*;
 `traceoptions` {
 `file` *name* <replace> <size *size*> <files *number*> <no-stamp>
 <(world-readable | no-world-readable)>;
 `flag` *flag* <*flag-modifier*> <disable>;
 }
}

Syntax (EX Series) `stp {`
 `bpdu-block-on-edge` ;
 `bridge-priority` *priority*;
 `disable;`
 `forward-delay` *seconds*;
 `hello-time` *seconds*;
 `interface` (all | *interface-name*) {
 `arp-on-stp;`
 `bpdu-timeout-action` {
 `block;`
 `log;`
 }
 `cost` *cost*;
 `disable;`
 `mode` *mode*;
 `no-root-port;`
 `priority` *priority*;
 }
 `max-age` *seconds*;
 `traceoptions` {
 `file` *filename* <files *number* > <size *size*> <no-stamp | world-readable |
 no-world-readable>;
 `flag` *flag*;
 }
}

Hierarchy Level	[edit protocols], [edit protocols rstp force-version]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series.
Description	<p>When you explicitly configure STP, a switch uses the IEEE 802.1D 2004 specification, force version 0. This configuration runs a version of RSTP that is compatible with the classic, basic STP (defined in the IEEE 802.1D 1998 specification).</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
	<p> NOTE: Although the <code>edge</code> configuration statement appears in the CLI on the switch, this statement has no effect on the switch operation if you configure it.</p>
Default	STP is disabled; by default, RSTP is enabled on all Ethernet switching ports.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Overview of Spanning-Tree Protocols</i> • Understanding STP on page 26 • <i>Example: Configuring BPDU Protection on STP Interfaces to Prevent STP Miscalculations</i> • Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on non-ELS EX Series Switches on page 157 • Configuring STP on EX Series Switches (CLI Procedure) on page 45 • <i>Configuring STP</i> • show spanning-tree bridge on page 372 • show spanning-tree interface on page 377

system-id

Syntax	<code>system-id system-id-value { ip-address(es); }</code>
Hierarchy Level	<code>[edit logical-systems logical-system-name protocols (mstp rstp)],</code> <code>[edit logical-systems logical-system-name protocols vstp vlan vlan-id],</code> <code>[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (mstp rstp)],</code> <code>[edit logical-systems logical-system-name routing-instances routing-instance-name protocols vstp vlan vlan-id],</code> <code>[edit protocols (mstp rstp)],</code> <code>[edit protocols vstp vlan vlan-id],</code> <code>[edit routing-instances routing-instance-name protocols (mstp rstp)],</code> <code>[edit routing-instances routing-instance-name protocols vstp vlan vlan-id]</code>
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Determine the system identifier value for bridges in a VPLS multihomed Layer 2 ring with MPLS infrastructure.
Options	<p>system-id-value—System identifier in the format <code>nnnnnn:nnnnnn</code>, where <i>n</i> = any digit from 0 through 9.</p> <p>Range: Any valid value</p> <p>Default: None</p> <p>ip-address(es)—Valid IP host addresses in the format <code>ip-address/32</code>.</p> <p>Range: Any valid IP address</p> <p>Default: None</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure on page 240• Understanding VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 241• Understanding VPLS Multihoming: System Identifier for Bridges in the Ring on page 244

traceoptions (Spanning Tree)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i> <flag-modifier> <disable>; } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols (mstp rstp vstp)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp)],</p> <p>[edit protocols (mstp rstp vstp vstp vlan <i>vlan-id</i>)],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols (mstp rstp vstp)]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.</p> <p>Support for logical systems added in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	Sets protocol-level tracing options for for spanning-tree protocols MPLS, MVRP, STP, RSTP, MSTP, and VSTP.
Default	The default STP protocol-level trace options are inherited from the global traceoptions statement. Traceoptions is disabled.
Options	<p>disable—(Optional) Disable the tracing operation. One use of this option is to disable a single operation when you have defined a broad group of tracing operations, such as all.</p> <p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks. We recommend that you place STP tracing output in the file /var/log/stp-log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option.</p> <p>Range: 2 through 1000 files</p> <p>Default: 1 trace file only</p> <p>flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. The following are the STP-specific tracing options:</p> <ul style="list-style-type: none"> all—Trace all operations.

- **all-failures**—Trace all failure conditions.
- **bpdu**—Trace BPDU reception and transmission.
- **bridge-detection-state-machine**—Trace the bridge detection state machine.
- **error**—Trace all failure conditions.
- **events**—Trace events of the protocol state machine.
- **pdu**—Trace PDUs that were received and sent.
- **port-information-state-machine**—Trace the port information state machine.
- **port-migration-state-machine**—Trace the port migration state machine.
- **port-receive-state-machine**—Trace the port receive state machine.
- **port-role-transit-state-machine**—Trace the port role transit state machine.
- **port-role-select-state-machine**—Trace the port role selection state machine.
- **port-state-transit-state-machine**—Trace the port state transit state machine.
- **port-transmit-state-machine**—Trace the port transmit state machine.
- **ppmd**—Trace the state and events for the ppm process.
- **socket**—Trace socket activity.
- **state-machine**—Trace state machine information.
- **state-machine-variables**—Trace when the state machine variables change.
- **timers**—Trace protocol timers.
- **topology-change-state-machine**—Trace the topology change state machine.

The following are the global tracing options:

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

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

- **parse**—Trace configuration parsing.
- **policy**—Trace policy operations and actions.
- **regex-parse**—Trace regular-expression parsing.
- **route**—Trace routing table changes.
- **state**—Trace state transitions.
- **task**—Trace protocol task processing.
- **timer**—Trace protocol task timer processing.

no-world-readable—(Optional) Prevent any user from reading the log file.

replace—(Optional) Replace an existing trace file if there is one.

Default: If you do not include this option, tracing output is appended to an existing trace file.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you must also specify a maximum number of trace files with the **files** option.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through the maximum file size supported on your system

Default: 1 MB

world-readable—(Optional) Allow any user to read the log file.

Required Privilege	routing—To view this statement in the configuration.
Level	routing-control—To add this statement to the configuration.

**Related
Documentation**

- [Understanding RSTP on page 21](#)
- [Understanding STP on page 26](#)
- [Understanding VSTP on page 29](#)
- [Understanding Multiple VLAN Registration Protocol \(MVRP\)](#)
- [Understanding Spanning-Tree Protocol Trace Options on page 31](#)
- [Configuring Tracing Spanning-Tree Operations on page 274](#)
- [Understanding MSTP on page 48](#)
- [Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217](#)
- [Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 84](#)
- [Example: Tracing Spanning-Tree Protocol Operations on page 276](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)

vlan (MSTP)

Syntax `vlan vlan-id;`

EX Series `vlan (all | vlan-id | vlan-name) {`
 `bridge-priority priority;`
 `forward-delay seconds;`
 `hello-time seconds;`
 `interface interface-name {`
 `bpdu-timeout-action {`
 `block;`
 `log;`
 `}`
 `cost cost;`
 `disable;`
 `edge;`
 `mode mode;`
 `no-root-port;`
 `priority priority;`
 `}`
 `max-age seconds;`
 `traceoptions {`
 `file filename <files number > <size size > <no-stamp | world-readable |`
 `no-world-readable>;`
 `flag flag;`
 `}`
 `}`

Hierarchy Level [edit logical-systems *logical-system-name* protocols `mstp msti msti-id`],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 protocols `mstp msti msti-id`],
 [edit protocols `mstp msti msti-id`],
 [edit protocols `mstpmsti msti-id`]
 [edit protocols `vstp`]
 [edit routing-instances *routing-instance-name* protocols `mstp msti msti-id`]

Release Information Statement introduced in Junos OS Release 8.4.
 Statement introduced in Junos OS Release 9.0 for EX Series switches.
 Statement updated with enhanced ? (CLI completion feature) functionality in Junos OS
 Release 9.5 for EX Series switches.
 Support for logical systems added in Junos OS Release 9.6.
 Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure the VLANs for a Multiple Spanning Tree Instance (MSTI) or VSTP instance.



NOTE: When you configure VSTP with the `set protocol vstp vlan all` command, `vlan-id 1` is excluded to be compatible with Cisco PVST+. If you

want vlan-id 1 to be included in VSTP, you must set it separately with the `set protocol vstp vlan 1` command.



TIP: To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type `?` after `vlan` or `vlan`s in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.

Options *vlan-name*—Name of the VLAN.

vlan-id—The VLAN identifier associated with the MSTI.

vlan-id-range—Range of VLAN identifiers associated with the MSTI in the form *minimum-vlan-id-maximum-vlan-id*. VLAN identifier ranges are not supported for VSTP.

Range: 1 through 4096

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- [Understanding MSTP on page 48](#)
- [Understanding VSTP on page 29](#)
- [Configuring Multiple Spanning Tree Protocol on page 54](#)
- [Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217](#)

vlan (VSTP)

Syntax	<pre> vlan <i>vlan-id</i> { bridge-priority <i>priority</i>; forward-delay <i>seconds</i>; hello-time <i>seconds</i>; max-age <i>seconds</i>; interface <i>interface-name</i> { cost <i>cost</i>; edge; mode (p2p shared); no-root-port; priority <i>interface-priority</i>; } } </pre>
EX Series	<pre> vlan (all <i>vlan-id</i> <i>vlan-name</i>) { bridge-priority <i>priority</i>; forward-delay <i>seconds</i>; hello-time <i>seconds</i>; interface (all <i>interface-name</i>) { bpdu-timeout-action { block; log; } cost <i>cost</i>; disable; edge; mode <i>mode</i>; no-root-port; priority <i>priority</i>; } max-age <i>seconds</i>; traceoptions { file <i>filename</i> <files <i>number</i> > <size <i>size</i> > <no-stamp world-readable no-world-readable>; flag <i>flag</i>; } } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols vstp], [edit protocols vstp]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.0. Statement introduced in Junos OS Release 9.4 for EX Series switches. Support for logical systems added in Junos OS Release 9.6. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	<p>Configure VSTP VLAN parameters.</p>



TIP: To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type ? after vlan or vlans in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.

Options **all**—All VLANs.

vlan-id—Numeric VLAN identifier.

vlan-range—Name of the VLAN range.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level routing—To view this statement in the configuration.
 routing-control—To add this statement to the configuration.

Related Documentation • [Understanding VSTP on page 29](#)
 • [Configuring VLAN SpanningTree Protocol on page 106](#)

vlan-group

Syntax `vlan-group group group-name {
 vlan (vlan-id |vlan-group |all) {
 }`

Hierarchy Level `[edit protocols vstp]`

Release Information Statement introduced in Junos OS Release 15.1 for EX Series switches.

Description Configure VLAN group for Spanning Tree Protocol (VSTP). VSTP is used to prevent loops in Layer 2 networks on a per-VLAN basis.



BEST PRACTICE: Configure RSTP when you configure VSTP. RSTP overhead is minimal and this configuration ensures that a spanning-tree protocol is running on all VLANs on your switch, even when your switch is supporting more than the maximum number of allowed VSTP VLANs.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level routing—To view this statement in the configuration.
 routing-control—To add this statement to the configuration.

Related Documentation

- [vstp on page 349](#)
- [show spanning-tree bridge on page 372](#)
- [show spanning-tree interface on page 377](#)
- [Configuring VLAN Spanning Tree Protocol on Switches on page 111](#)
- [Understanding VSTP on page 29](#)

vppls-flush-on-topology-change

Syntax	<code>vppls-flush-on-topology-change;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> protocols (<i>mstp</i> <i>rstp</i>)],</code> <code>[edit logical-systems <i>logical-system-name</i> protocols <i>vstp</i> <i>vlan</i> <i>vlan-id</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols</code> <code> (<i>mstp</i> <i>rstp</i>)],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols</code> <code> <i>vstp</i> <i>vlan</i> <i>vlan-id</i>],</code> <code>[edit protocols (<i>mstp</i> <i>rstp</i>)],</code> <code>[edit protocols <i>vstp</i> <i>vlan</i> <i>vlan-id</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols (<i>mstp</i> <i>rstp</i>)],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols <i>vstp</i> <i>vlan</i> <i>vlan-id</i>]</code>
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Determine the action the bridge should take when the topology of a multihomed Layer 2 ring with MPLS infrastructure changes: flush the media access control (MAC) cache or not. By default, the bridge does not flush the cache when the topology changes.
Required Privilege Level	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding VPLS Multihoming: Bridge Flush of MAC Cache on Topology Change on page 245

vstp

List of Syntax [MX Series on page 349](#)
 [EX Series, QFX Series, QFabric on page 349](#)
 [ELS versions: EX Series, QFX Series, NFX Series on page 351](#)

MX Series `vstp {`
 `bpdu-block-on-edge;`
 `force-version stp;`
 `interface interface-name {`
 `bpdu-timeout-action {`
 `alarm;`
 `block;`
 `}`
 `cost cost;`
 `edge;`
 `mode (p2p | shared);`
 `no-root-port;`
 `priority interface-priority;`
 `}`
 `priority-hold-time seconds;`
 `vlan vlan-id {`
 `bridge-priority priority;`
 `forward-delay seconds;`
 `hello-time seconds;`
 `max-age seconds;`
 `interface interface-name {`
 `access-trunk`
 `bpdu-timeout-action {`
 `alarm;`
 `block;`
 `}`
 `cost cost;`
 `edge;`
 `mode (p2p | shared);`
 `no-root-port;`
 `priority interface-priority;`
 `}`
 `}`
 `traceoptions {`
 `file filename <files number> <size size> <world-readable | no-world-readable>;`
 `flag flag <flag-modifier> <disable>;`
 `}`
 `}`

EX Series, QFX Series, QFabric `vstp {`
 `bpdu-block-on-edge;`
 `disable;`
 `force-version stp;`
 `vlan (all | vlan-id | vlan-name) {`
 `bridge-priority priority;`
 `forward-delay seconds;`
 `hello-time seconds;`
 `}`

```
interface (all | interface-name) {
  arp-on-stp;
  bpdu-timeout-action {
    block;
    log;
  }
  cost cost;
  disable;
  edge;
  mode mode;
  no-root-port;
  priority priority;
}
max-age seconds;
traceoptions {
  file filename <files number > <size size> <no-stamp | no-world-readable |
    world-readable>;
  flag flag;
}
}
```

```

ELS versions: EX vstp {
Series, QFX Series, NFX
Series
    bpdublock-on-edge;
    disable;
    force-version stp;
    interface (interface-name disable | interface-range-name | all ){
        bpdubtimeout-action {
            alarm;
            block;
        }
        cost cost;
        edge;
        mode (p2p | shared);
        no-root-port;
        priority interface-priority;
    }
    priority-hold-time seconds;
    vlan (vlan-id | all){
        bridge-priority priority;
        forward-delay seconds;
        hello-time seconds;
        max-age seconds;
        interface (interface-name disable | interface-range-name | all ){
            bpdubtimeout-action {
                alarm;
                block;
            }
            cost cost;
            edge;
            mode (p2p | shared);
            no-root-port;
            priority interface-priority;
        }
    }
    traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable>;
        flag flag <flag-modifier> <disable>;
    }
    vlan-group group group-name {
        vlansvlan-name (vlan-id |vlan-range | open-set-of-values) {
            interface all;
            interface interface-name {
                disable;
            }
        }
    }
}

```

Hierarchy Level [edit protocols]

[edit logical-systems *logical-system-name* protocols],

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols],

[edit protocols],

[edit routing-instances *routing-instance-name* protocols]

Release Information Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 9.4 for EX Series switches.
bpdudrop-on-edge statement added in Junos OS Release 9.4.
bpdudrop-timeout-action statement added in Junos OS Release 9.4.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement updated in Junos OS Release 15.1 for EX Series switches to support configuration of spanning tree parameters globally on all interfaces.



NOTE: You cannot disable spanning tree parameters globally on all interfaces.

Description Configures VLAN Spanning Tree Protocol (VSTP). VSTP is used to prevent loops in Layer 2 networks on a per-VLAN basis.

You can have a maximum of 253 VSTP VLANs per switch.

If the number of VLANs on your switch exceeds the VSTP VLAN limit, you must use the **vlan** statement to specify which VLANs or VLAN groups use VSTP. You also cannot use the **vlan all** option to configure VSTP when your switch has more than the maximum allowed VSTP VLANs. To ensure all VLANs are running a spanning-tree protocol, run RSTP for networks with large numbers of VLANs.



NOTE: When you configure VSTP with the **set protocol vstp vlan all** command, VLAN ID 1 is not set; it is excluded so that the configuration is compatible with Cisco PVST+. If you want VLAN ID 1 to be included in the VSTP configuration on your switch, you must set it separately with the **set protocol vstp vlan 1** command.



NOTE: Option **vlan all** is not supported in Junos OS Release 13.2X50.



BEST PRACTICE: Configure RSTP when you configure VSTP. RSTP overhead is minimal and this configuration ensures that some spanning tree protocol is running on all VLANs on your switch, even when your switch has more than the maximum number of allowed VSTP VLANs.

The remaining statements are explained separately. See [CLI Explorer](#).

Default VSTP is not enabled by default.

Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding VSTP on page 29• Configuring VLAN SpanningTree Protocol on page 106• Configuring VSTP on EX Series Switches (CLI Procedure) on page 113• Configuring VSTP (CLI Procedure)• Example: Configuring VSTP on QFX Series Switches and EX4600 Switches• show spanning-tree bridge on page 372• show spanning-tree interface on page 377

CHAPTER 14

Operational Mode Commands for Spanning-Tree Configuration

- `clear bpdu-error`
- `clear error bpdu interface`
- `clear error mac-rewrite`
- `clear spanning-tree protocol-migration`
- `clear spanning-tree statistics`
- `clear spanning-tree statistics bridge`
- `clear spanning-tree stp-buffer`
- `show bridge mac-table`
- `show mac-rewrite interface`
- `show spanning-tree bridge`
- `show spanning-tree interface`
- `show spanning-tree mstp configuration`
- `show spanning-tree statistics`
- `show spanning-tree statistics bridge`
- `show spanning-tree statistics interface`
- `show spanning-tree statistics message-queues`
- `show spanning-tree stp-buffer see-all`

clear bpdv-error

Syntax	<code>clear bpdv-error interface <i>interface-name</i></code>
Release Information	Command introduced in Junos OS Release 9.1 for EX Series switches. Command updated in Junos OS Release 11.1 for EX Series switches—a BPDU error shuts down the interface and this command brings the interface back up. Command introduced in Junos OS Release 11.1 for the QFX Series.
Description	Clear bridge protocol data unit (BPDU) errors from an interface and bring up the interface.
Options	<i>interface-name</i> —Clear BPDU errors on the specified interface.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 133• <i>Understanding BPDU Protection for STP, RSTP, and MSTP</i>• show spanning-tree interface on page 377
List of Sample Output	clear bpdv-error interface on page 356

Sample Output

clear bpdv-error interface

```
user@switch> clear bpdv-error interface xe-0/0/1.0
```

clear error bpdu interface

List of Syntax	MX Series on page 357 QFX Series, EX Series, NFX Series on page 357
MX Series	<code>clear error bpdu interface <i>interface-name</i></code>
QFX Series, EX Series, NFX Series	<code>clear error bpdu interface (all <i>interface-name</i>)</code>
Release Information	Command introduced in Junos OS Release 9.4. Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches. Command supports all option in Junos OS Release 15.1 for EX Series switches.
Description	Clear a bridge protocol data unit (BPDU) error condition caused by the detection of a possible bridging loop from Spanning Tree Protocol (STP) operation.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • Configuring BPDU Protection for Spanning-Tree Instance Interfaces on page 137 • Configuring BPDU Protection on All Edge Ports on page 145 • Unblocking a Switch Interface That Receives BPDUs in Error (CLI Procedure) on page 146
List of Sample Output	clear error bpdu interface on page 357
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear error bpdu interface

```
user@host> clear error bpdu interface ge-1/1/1
```

clear error mac-rewrite

Syntax	clear error mac-rewrite <interface <i>interface-name</i>>
Release Information	Command introduced in Junos OS Release 9.1.
Description	<p>Clear a MAC rewrite error condition caused by the reception of tunneled protocol packets on an interface with Layer 2 protocol tunneling enabled.</p> <p>On interfaces with L2PT configured, customer-facing ports should not receive packets with the L2PT MAC address as the destination address unless there is a network topology or configuration error. Any such interface receiving an L2PT packet becomes “Disabled”, and must subsequently be re-enabled by clearing the error with this command.</p>
Options	interface <i>interface-name</i> —(Optional) Clear the MAC rewrite error condition for the specified interface.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• Understanding Layer 2 Protocol Tunneling Through a Network on page 263• Configuring Layer 2 Protocol Tunneling on EX Series Switches with ELS Support (CLI Procedure)• Clearing a MAC Rewrite Error on an Interface with Layer 2 Protocol Tunneling• show mac-rewrite interface on page 370
List of Sample Output	clear error mac-rewrite interface on page 358
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear error mac-rewrite interface

```
user@host> clear error mac-rewrite interface ge-1/0/1
```

clear spanning-tree protocol-migration


Syntax	<code>clear spanning-tree protocol-migration</code> <code><interface <i>interface-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Release 9.0.
Description	Revert from the original IEEE 802.1D Spanning Tree Protocol (STP) back to the Rapid Spanning Tree Protocol after the force-version statement has been removed from the configuration.
Options	none —Reset the STP protocol for all interfaces and all routing instances. interface <i>interface-name</i> —(Optional) Reset the STP protocol for the specified interface only. routing-instance <i>routing-instance-name</i> —(Optional) Reset the STP protocol for a particular routing instance.
Additional Information	For information about the force-version statement, see the <i>Junos Routing Protocols Configuration Guide</i> .
Required Privilege Level	clear

Sample Output

clear spanning-tree protocol-migration

```
user@host> clear spanning-tree protocol-migration
```

clear spanning-tree statistics

List of Syntax	Syntax on page 360 Syntax (EX Series Switches and the QFX Series) on page 360
Syntax	clear spanning-tree statistics <interface <i>interface-name</i> > <logical-system <i>logical-system-name</i> >
Syntax (EX Series Switches and the QFX Series)	clear spanning-tree statistics <interface <i>interface-name</i> >
Release Information	Command introduced in Junos OS Release 8.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series.
Description	Clear Spanning Tree Protocol statistics for all interfaces or a specified interface.
Options	none —Reset STP counters for all interfaces for all routing instances. interface <i>interface-name</i> —(Optional) Clear STP statistics for the specified interface only. logical-system <i>logical-system-name</i> —(Optional) Clear STP statistics on a particular logical system.
<div> NOTE: The logical-system option is not available on QFabric systems.</div>	
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• Understanding STP on page 26• show spanning-tree statistics on page 389• show spanning-tree bridge on page 372• show spanning-tree interface on page 377
List of Sample Output	clear spanning-tree statistics on page 361
Output Fields	This command produces no output.

Sample Output

clear spanning-tree statistics

```
user@switch> clear spanning-tree statistics
```

clear spanning-tree statistics bridge

Syntax clear spanning-tree statistics bridge

Release Information Command introduced in Junos OS Release 14.1.

Description Clear the statistics of the bridge.

Required Privilege Level clear

List of Sample Output [clear spanning-tree statistics bridge \(MX Series\) on page 362](#)

Sample Output

clear spanning-tree statistics bridge (MX Series)

```
user@host> clear spanning-tree statistics bridge
```

clear spanning-tree stp-buffer

Syntax clear spanning-tree stp-buffer

Release Information Command introduced in Junos OS Release 14.1.

Description Clear the stp-buffer.

Required Privilege Level clear

List of Sample Output [clear spanning-tree stp-buffer \(MX Series\) on page 363](#)

Sample Output

clear spanning-tree stp-buffer (MX Series)

```
user@host> clear spanning-tree stp-buffer
```

show bridge mac-table

Syntax	<pre>show bridge mac-table <age> <brief count detail extensive> <bridge-domain (all <i>bridge-domain-name</i>)> <global-count> <instance <i>instance-name</i>> <interface <i>interface-name</i>> <mac-address> <instance <i>instance-name</i>> <vlan-id (all-vlan <i>vlan-id</i>)></pre>
Release Information	Command introduced in Junos OS Release 8.4. Command introduced in Junos OS Release 15.1 Support for PBB-EVPN instance added in Junos OS Release 16.1 MAC Flag P to indicate a MAC Pinned interface introduced in Junos OS 16.2
Description	(MX Series routers only) Display Layer 2 MAC address information.
Options	<p>none—Display all learned Layer 2 MAC address information.</p> <p>age— (Optional) Display age of a single mac-address.</p> <p>brief count detail extensive—(Optional) Display the specified level of output.</p> <p>bridge-domain (all <i>bridge-domain-name</i>)—(Optional) Display learned Layer 2 MAC addresses for all bridging domains or for the specified bridging domain.</p> <p>global-count—(Optional) Display the total number of learned Layer 2 MAC addresses on the system.</p> <p>instance <i>instance-name</i>—(Optional) Display learned Layer 2 MAC addresses for the specified routing instance.</p> <p>interface <i>interface-name</i>—(Optional) Display learned Layer 2 MAC addresses for the specified interface.</p> <p>mac-address—(Optional) Display the specified learned Layer 2 MAC address information.</p> <p>vlan-id (all-vlan <i>vlan-id</i>)—(Optional) Display learned Layer 2 MAC addresses for all VLANs or for the specified VLAN.</p>
Additional Information	When Layer 2 protocol tunneling is enabled, the tunneling MAC address 01:00:0c:cd:cd:d0 is installed in the MAC table. When the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunk Protocol (VTP) is configured for Layer 2 protocol tunneling on an interface, the corresponding protocol MAC address is installed in the MAC table.

Required Privilege Level view

List of Sample Output [show bridge mac-table on page 366](#)
[show bridge mac-table \(with Layer 2 Services over GRE Interfaces\) on page 366](#)
[show bridge mac-table \(with VXLAN enabled\) on page 367](#)
[show bridge mac-table age \(for GE interface\) on page 367](#)
[show bridge mac-table age \(for AE interface\) on page 367](#)
[show bridge mac-table count on page 367](#)
[show bridge mac-table detail on page 368](#)
[show bridge mac-table instance pbb-evpn on page 368](#)
[show bridge mac-table on page 368](#)

Output Fields [Table 24 on page 365](#) describes the output fields for the **show bridge mac-table** command. Output fields are listed in the approximate order in which they appear.

Table 24: show bridge mac-table Output Fields

Field Name	Field Description
Age	Age of a single mac-address.
Routing instance	Name of the routing instance.
Bridging domain	Name of the bridging domain.
MAC address	MAC address or addresses learned on a logical interface.
MAC flags	Status of MAC address learning properties for each interface: <ul style="list-style-type: none"> • S—Static MAC address is configured. • D—Dynamic MAC address is configured. • L—Locally learned MAC address is configured. • C—Control MAC address is configured. • SE—MAC accounting is enabled. • NM—Non-configured MAC. • R—Remote PE MAC address is configured. • P—MAC Pinned interface is configured
Logical interface	Name of the logical interface.
MAC count	Number of MAC addresses learned on the specific routing instance or interface.
Learning interface	Name of the logical interface on which the MAC address was learned.
Learning VLAN	VLAN ID of the routing instance or bridge domain in which the MAC address was learned.
VXLAN ID/VXLAN	VXLAN Network Identifier (VNI).

Table 24: show bridge mac-table Output Fields (*continued*)

Field Name	Field Description
Layer 2 flags	Debugging flags signifying that the MAC address is present in various lists.
Epoch	Spanning Tree Protocol epoch number identifying when the MAC address was learned. Used for debugging.
Sequence number	Sequence number assigned to this MAC address. Used for debugging.
Learning mask	Mask of the Packet Forwarding Engines where this MAC address was learned. Used for debugging.
IPC generation	Creation time of the logical interface when this MAC address was learned. Used for debugging.

Sample Output

show bridge mac-table

```

user@host> show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
          SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : default-switch
Bridging domain : test1, VLAN : 1
  MAC          MAC      Logical      NH      RTR
  address      flags    interface  Index   ID
01:00:0c:cc:cc:cc S,NM    NULL
01:00:0c:cc:cc:cd S,NM    NULL
01:00:0c:cd:cd:d0 S,NM    NULL
64:87:88:6a:17:d0 D        ae0.1
64:87:88:6a:17:f0 D        ae0.1

```

show bridge mac-table (with Layer 2 Services over GRE Interfaces)

```

user@host> show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned
          SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : default-switch
Bridging domain : vlan-1, VLAN : 1
  MAC          MAC      Logical
  address      flags    interface
00:01:01:00:01:f7 D,SE    gr-1/2/10.0
00:03:00:32:01:f7 D,SE    gr-1/2/10.0
00:00:21:11:11:10 DL      ge-1/0/0.0
00:00:21:11:11:11 DL      ge-1/1/0.0

Routing instance : default-switch
Bridging domain : vlan-2, VLAN : 2
  MAC          MAC      Logical
  address      flags    interface
00:02:01:33:01:f7 D,SE    gr-1/2/10.1

```

```
00:00:21:11:21:10 DL ge-1/0/0.1
00:00:21:11:21:11 DL ge-1/1/0.1
```

show bridge mac-table (with VXLAN enabled)

```
user@host> show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned
          SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)
```

```
Routing instance : default-switch
Bridging domain : vlan-1, VLAN : 1
VXLAN: Id : 100, Multicast group: 233.252.0.1
MAC          MAC          Logical
address      flags      interface
00:01:01:00:01:f7 D,SE    vtep.1052010
00:03:00:32:01:f7 D,SE    vtep.1052011
00:00:21:11:11:10 DL      ge-1/0/0.0
00:00:21:11:11:11 DL      ge-1/1/0.0
```

```
Routing instance : default-switch
Bridging domain : vlan-2, VLAN : 2, VXLAN : 200
VXLAN: Id : 200, Multicast group: 233.252.0.2
MAC          MAC          Logical
address      flags      interface
00:02:01:33:01:f7 D,SE    vtep.1052010
00:04:00:14:01:f7 D,SE    vtep.1052011
00:00:21:11:21:10 DL      ge-1/0/0.1
00:00:21:11:21:11 DL      ge-1/1/0.1
```

show bridge mac-table age (for GE interface)

```
user@host> show vpls mac-table age 00:02:03:aa:bb:1a instance vpls_instance_1
MAC Entry Age information
Current Age: 4 seconds
```

show bridge mac-table age (for AE interface)

```
user@host> show vpls mac-table age 00:02:03:aa:bb:1a instance vpls_instance_1
MAC Entry Age information
Current Age on FPC1: 102 seconds
Current Age on FPC2: 94 seconds
```

show bridge mac-table count

```
user@host> show bridge mac-table count
2 MAC address learned in routing instance vs1 bridge domain vlan100
```

```
MAC address count per interface within routing instance:
Logical interface      MAC count
ge-11/0/3.0            1
ge-11/1/4.100          0
ge-11/1/1.100          0
ge-11/1/0.100          0
xe-10/2/0.100          1
xe-10/0/0.100          0
```

```
MAC address count per learn VLAN within routing instance:
Learn VLAN ID          MAC count
```

```

0                                2

0 MAC address learned in routing instance vs1 bridge domain vlan200

MAC address count per interface within routing instance:
Logical interface      MAC count
ge-11/1/0.200          0
ge-11/1/1.200          0
ge-11/1/4.200          0
xe-10/0/0.200          0
xe-10/2/0.200          0

MAC address count per learn VLAN within routing instance:
Learn VLAN ID          MAC count
0                        0

```

show bridge mac-table detail

```

user@host> show bridge mac-table detail
MAC address: 00:00:00:19:1c:db
Routing instance: vs1
Bridging domain: vlan100
Learning interface: ge-11/0/3.0   Learning VLAN: 0
Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
Epoch: 4                          Sequence number: 0
Learning mask: 0x800               IPC generation: 0

MAC address: 00:00:00:59:3a:2f
Routing instance: vs1
Bridging domain: vlan100
Learning interface: xe-10/2/0.100 Learning VLAN: 0
Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
Epoch: 7                          Sequence number: 0
Learning mask: 0x400               IPC generation: 0

```

show bridge mac-table instance pbb-evpn

```

user@host> show bridge mac-table instance pbb-evpn
Routing instance : pbb-evpn
Bridging domain : isid-bd10000, ISID : 10000
MAC          MAC      Logical      NH      RTR
address      flags     interface  Index   ID
00:19:e2:b0:76:eb  D      cbp.1000
aa:bb:cc:dd:ee:f2  DC
aa:bb:cc:dd:ee:f3  DC      1048576 1048576
1048575 1048575

```

show bridge mac-table

```

user@host>run show bridge mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned, C -Control MAC
O -OVSDB MAC, SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC,
P -Pinned MAC)

Routing instance : VS-541
Bridging domain : 541, VLAN : 541
MAC MAC Logical NH RTR
address flags interface Index ID
00:00:01:00:00:01 DPRC xe-0/0/3.0
00:00:02:00:00:01 DP  xe-0/0/3.0

```


show mac-rewrite interface

Syntax	show mac-rewrite interface <brief detail> <interface-name>
Release Information	Command introduced in Junos OS Release 9.1. Command introduced in Junos OS Release 14.1X53-D10 for EX4300 switches. Command introduced in Junos OS Release 15.1X53-D55 for EX2300 and EX3400 switches. Command introduced in Junos OS Release 17.4R1 for EX4600 switches.
Description	Display Layer 2 protocol tunneling (L2PT) information.
Options	brief detail —(Optional) Display the specified level of output. interface interface-name —(Optional) Display L2PT information for the specified interface.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • layer2-control on page 309 • mac-rewrite on page 311 • protocol on page 328 • Understanding Layer 2 Protocol Tunneling Through a Network on page 263 • Understanding Layer 2 Protocol Tunneling Configuration Guidelines on page 265 • Configuring Layer 2 Protocol Tunneling on page 266 • Understanding Layer 2 Protocol Tunneling on EX Series Switches • Configuring Layer 2 Protocol Tunneling on EX Series Switches with ELS Support (CLI Procedure)
List of Sample Output	show mac-rewrite interface on page 371 show mac-rewrite interface (EX Series Switches) on page 371
Output Fields	Table 25 on page 370 lists the output fields for the show mac-rewrite interface command. Output fields are listed in the approximate order in which they appear.

Table 25: show mac-rewrite interface Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface on which L2PT is configured.	brief detail

Table 25: show mac-rewrite interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
Protocols	<p>Layer 2 protocols being tunneled on this interface.</p> <p>All devices that support L2PT can tunnel the following protocols: Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunk Protocol (VTP).</p> <p>The following Layer 2 protocols can also be tunneled on some devices that support L2PT: E-LMI, GVRP, IEEE 802.1X, IEEE 802.3AH, LACP, LLDP, MMRP, MVRP, PVSTP+, UDLD, or VSTP. See protocol for more information on the supported protocols for tunneling on different devices.</p>	brief detail

Sample Output

show mac-rewrite interface

```

user@host> show mac-rewrite interface
Interface      Protocols
ge-1/0/5      STP VTP CDP PVSTP+

```

show mac-rewrite interface (EX Series Switches)

```

user@switch> show mac-rewrite interface
Interface      Protocols
ge-0/0/1      802.3AH LLDP STP

```

show spanning-tree bridge

List of Syntax [Syntax on page 372](#)
 [Syntax \(QFX Series and EX Series\) on page 372](#)

Syntax show spanning-tree bridge
 <brief | detail>
 <msti *msti-id*>
 <routing-instance *routing-instance-name*>
 <vlan-id *vlan-id*>

Syntax (QFX Series and EX Series) show spanning-tree bridge
 <brief | detail>
 <msti *msti-id*>
 <vlan-id *vlan-id*>

Release Information Command introduced in Junos OS Release 8.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.
 Command introduced in Junos OS Release 11.1 for the QFX Series.

Description Displays the configured or calculated spanning-tree protocol (can be either STP, RSTP, MSTP, or VSTP) parameters.

Options **none**—(Optional) Display brief STP bridge information for all multiple spanning-tree instances (MSTIs).

brief | detail—(Optional) Display the specified level of output.

msti *msti-id*—(Optional) Display spanning-tree protocol bridge information for the specified MSTI or Common and Internal Spanning Tree (CIST). Specify **0** for CIST. Specify a value from **1** through **4094** for an MSTI.

routing-instance *routing-instance-name*—(Optional) Display STP bridge information for the specified routing instance.

vlan-id *vlan-id*—(Optional) Display spanning-tree protocol bridge information for the specified VLAN. Specify a VLAN tag identifier from **1** through **4094**.

Required Privilege Level view

Related Documentation

- [Understanding STP on page 26](#)
- [Understanding RSTP on page 21](#)
- [Understanding VSTP on page 29](#)
- [Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217](#)

- [show spanning-tree interface on page 377](#)

List of Sample Output [show spanning-tree bridge routing-instance on page 374](#)
[show spanning-tree bridge msti on page 375](#)
[show spanning-tree bridge vlan-id \(MSTP\) on page 375](#)
[show spanning-tree bridge \(RSTP\) on page 376](#)
[show spanning-tree bridge vlan-id \(RSTP\) on page 376](#)

Output Fields [Table 26 on page 373](#) lists the output fields for the **show spanning-tree bridge** command. Output fields are listed in the approximate order in which they appear.

Table 26: show spanning-tree bridge Output Fields

Field Name	Field Description
Routing instance name	Name of the routing instance under which the bridge is configured.
Enabled protocol	Spanning Tree Protocol type enabled.
Root ID	Bridge ID of the elected spanning-tree root bridge. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.
Root cost	Calculated cost to reach the root bridge from the bridge where the command is entered.
Root port	Interface that is the current elected root port for this bridge.
CIST regional root	Bridge ID of the elected MSTP regional root bridge.
CIST internal root cost	Calculated cost to reach the regional root bridge from the bridge where the command is entered.
Hello time	Configured number of seconds between transmissions of configuration BPDUs.
Maximum age	Configured maximum expected arrival time of hello bridge protocol data units (BPDUs).
Forward delay	How long an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hop count	Configured maximum number of hops a BPDU can be forwarded in the MSTP region.
Message age	Number of elapsed seconds since the most recent BPDU was received.
Number of topology changes	Total number of STP topology changes detected since the routing device last booted.

Table 26: show spanning-tree bridge Output Fields (*continued*)

Field Name	Field Description
Time since last topology change	Number of elapsed seconds since the most recent topology change.
Bridge ID (Local)	Locally configured bridge ID. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.
Extended system ID	System identifier.
MSTI regional root	Bridge ID of the elected MSTP regional root bridge.

Sample Output

show spanning-tree bridge routing-instance

```

user@host> show spanning-tree bridge routing-instance vs1 detail
STP bridge parameters
Routing instance name           : vs1
Enabled protocol                : MSTP

STP bridge parameters for CIST
Root ID                        : 32768.00:13:c3:9e:c8:80
Root cost                      : 0
Root port                     : ge-10/2/0
CIST regional root             : 32768.00:13:c3:9e:c8:80
CIST internal root cost       : 22000
Hello time                     : 2 seconds
Maximum age                   : 20 seconds
Forward delay                  : 15 seconds
Hop count                     : 18
Message age                   : 0
Number of topology changes    : 1
Time since last topology change : 1191 seconds
Local parameters
  Bridge ID                   : 32768.00:90:69:0b:7f:d1
  Extended system ID          : 1

STP bridge parameters for MSTI 1
MSTI regional root            : 32769.00:13:c3:9e:c8:80
Root cost                     : 22000
Root port                     : ge-10/2/0
Hello time                    : 2 seconds
Maximum age                   : 20 seconds
Forward delay                  : 15 seconds
Hop count                     : 18
Number of topology changes    : 1
Time since last topology change : 1191 seconds
Local parameters
  Bridge ID                   : 32769.00:90:69:0b:7f:d1
  Extended system ID          : 1

STP bridge parameters for MSTI 2
MSTI regional root            : 32770.00:13:c3:9e:c8:80
Root cost                     : 22000
Root port                     : ge-10/2/0

```

```

Hello time                : 2 seconds
Maximum age                : 20 seconds
Forward delay              : 15 seconds
Hop count                  : 18
Number of topology changes : 1
Time since last topology change : 1191 seconds
Local parameters
  Bridge ID                : 32770.00:90:69:0b:7f:d1
  Extended system ID       : 1

```

show spanning-tree bridge msti

```

user@host> show spanning-tree bridge msti 1 routing-instance vs1 detail
STP bridge parameters
Routing instance name      : vs1
Enabled protocol           : MSTP

STP bridge parameters for MSTI 1
MSTI regional root        : 32769.00:13:c3:9e:c8:80
Root cost                  : 22000
Root port                  : xe-10/2/0
Hello time                 : 2 seconds
Maximum age                : 20 seconds
Forward delay              : 15 seconds
Hop count                  : 18
Number of topology changes : 1
Time since last topology change : 1191 seconds
Local parameters
  Bridge ID                : 32769.00:90:69:0b:7f:d1
  Extended system ID       : 1

```

show spanning-tree bridge vlan-id (MSTP)

```

user@host> show spanning-tree bridge vlan-id 1 101 routing-instance vs1 detail
STP bridge parameters
Routing instance name      : vs1
Enabled protocol           : MSTP

STP bridge parameters for CIST
Root ID                    : 32768.00:13:c3:9e:c8:80
Root cost                  : 0
Root port                  : xe-10/2/0
CIST regional root        : 32768.00:13:c3:9e:c8:80
CIST internal root cost   : 22000
Hello time                 : 2 seconds
Maximum age                : 20 seconds
Forward delay              : 15 seconds
Hop count                  : 18
Message age                : 0
Number of topology changes : 0
Local parameters
  Bridge ID                : 32768.00:90:69:0b:7f:d1
  Extended system ID       : 1
  Hello time               : 2 seconds
  Maximum age              : 20 seconds
  Forward delay            : 15 seconds
  Path cost method         : 32 bit
  Maximum hop count        : 20

```

show spanning-tree bridge (RSTP)

```
user@host> show spanning-tree bridge
STP bridge parameters
Routing instance name      : GLOBAL
Enabled protocol           : RSTP
Root ID                    : 28672.00:90:69:0b:3f:d0
Hello time                  : 2 seconds
Maximum age                 : 20 seconds
Forward delay               : 15 seconds
Message age                 : 0
Number of topology changes  : 58
Time since last topology change : 14127 seconds
Local parameters
  Bridge ID                 : 28672.00:90:69:0b:3f:d0
  Extended system ID        : 0

STP bridge parameters for bridge VLAN 10
Root ID                    : 28672.00:90:69:0b:3f:d0
Hello time                  : 2 seconds
Maximum age                 : 20 seconds
Forward delay               : 15 seconds
Message age                 : 0
Number of topology changes  : 58
Time since last topology change : 14127 seconds
Local parameters
  Bridge ID                 : 28672.00:90:69:0b:3f:d0
  Extended system ID        : 0

STP bridge parameters for bridge VLAN 20
Root ID                    : 28672.00:90:69:0b:3f:d0
Hello time                  : 2 seconds
Maximum age                 : 20 seconds
Forward delay               : 15 seconds
Message age                 : 0
Number of topology changes  : 58
Time since last topology change : 14127 seconds
Local parameters
  Bridge ID                 : 28672.00:90:69:0b:3f:d0
  Extended system ID        : 0
```

show spanning-tree bridge vlan-id (RSTP)

```
user@host> show spanning-tree bridge vlan-id 10
STP bridge parameters
Routing instance name      : GLOBAL
Enabled protocol           : RSTP

STP bridge parameters for VLAN 10
Root ID                    : 28672.00:90:69:0b:3f:d0
Hello time                  : 2 seconds
Maximum age                 : 20 seconds
Forward delay               : 15 seconds
Message age                 : 0
Number of topology changes  : 58
Time since last topology change : 14127 seconds
Local parameters
  Bridge ID                 : 28672.00:90:69:0b:3f:d0
  Extended system ID        : 0
```


show spanning-tree interface

List of Syntax	Syntax on page 377 Syntax (EX Series Switches and QFX Series Switches) on page 377 Syntax (EX Series Switches) on page 377
Syntax	<pre>show spanning-tree interface <brief detail> <msti <i>msti-id</i>> <routing-instance <i>routing-instance-name</i>> <vlan-id <i>vlan-id</i>></pre>
Syntax (EX Series Switches and QFX Series Switches)	<pre>show spanning-tree interface <brief detail> <msti <i>msti-id</i>> <vlan-id <i>vlan-id</i>></pre>
Syntax (EX Series Switches)	<pre>show spanning-tree interface <brief detail> <interface-name <i>interface-name</i>> <msti <i>msti-id</i>> <vlan-id <i>vlan-id</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 8.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for the QFX Series.</p>
Description	<p>Display the configured or calculated interface-level spanning-tree protocol (can be either STP, RSTP, or MSTP) parameters. In brief mode, will not display interfaces that are administratively disabled or do not have a physical link.</p>
Options	<p>none—Display brief STP interface information.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>interface-name <i>interface-name</i>—(Optional) Name of an interface.</p> <p>msti <i>msti-id</i>—(Optional) Display STP interface information for the specified MST instance.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display STP interface information for the specified routing instance.</p> <p>vlan-id <i>vlan-id</i>—(Optional) Display STP interface information for the specified VLAN.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show spanning-tree bridge on page 372

- [Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217](#)
- [Understanding STP on page 26](#)
- [Understanding RSTP on page 21](#)
- [Understanding MSTP on page 48](#)
- [Understanding VSTP on page 29](#)

List of Sample Output

[show spanning-tree interface on page 379](#)
[show spanning-tree interface \(QFX Series\) on page 379](#)
[show spanning-tree interface \(EX Series\) on page 380](#)
[show spanning-tree interface detail on page 381](#)
[show spanning-tree interface detail \(EX Series\) on page 382](#)
[show spanning-tree interface msti on page 384](#)
[show spanning-tree interface vlan-id on page 384](#)
[show spanning-tree interface \(VSTP\) on page 384](#)
[show spanning-tree interface vlan-id \(VSTP\) on page 384](#)
[show spanning-tree interface brief \(EX Series\) on page 385](#)
[show spanning-tree interface ge-1/0/0 \(EX Series\) on page 385](#)

Output Fields

[Table 27 on page 378](#) lists the output fields for the **show spanning-tree interface** command. Output fields are listed in the approximate order in which they appear.

Table 27: show spanning-tree Interface Output Fields

Field Name	Field Description
Interface name	Interface configured to participate in the STP, RSTP, VSTP, or MSTP instance.
Port ID	Logical interface identifier configured to participate in the MSTP or VSTP instance.
Designated port ID	Port ID of the designated port for the LAN segment to which this interface is attached.
Designated bridge ID	Bridge ID of the designated bridge for the LAN segment to which this interface is attached.
Port Cost	Configured cost for the interface.
Port State	STP port state: forwarding (FWD), blocking (BLK), listening, learning, or disabled.
Port Role	MSTP, VSTP, or RSTP port role: designated (DESG), backup (BKUP), alternate (ALT), (ROOT), or Root Prevented (Root-Prev).
Link type	MSTP, VSTP, or RSTP link type. Shared or point-to-point (pt-pt) and edge or nonedge.

Table 27: show spanning-tree Interface Output Fields (*continued*)

Field Name	Field Description
Alternate	Identifies the interface as an MSTP, VSTP, or RSTP alternate root port (Yes) or nonalternate root port (No).
Boundary Port	Identifies the interface as an MSTP regional boundary port (Yes) or nonboundary port (No).
Edge delay while expiry count	Number of times the edge delay timer expired on that interface.
Rcvd info while expiry count	Number of times the rcvd info timer expired on that interface.

Sample Output

show spanning-tree interface

```
user@host> show spanning-tree interface routing-instance vs1 detail
Spanning tree interface parameters for instance 0
```

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ae1	128:1	128:1	32768.0090690b47d1	1000	FWD	DESG
ge-2/1/2	128:2	128:2	32768.0090690b47d1	20000	FWD	DESG
ge-2/1/5	128:3	128:3	32768.0090690b47d1	29999	FWD	DESG
ge-2/2/1	128:4	128:26	32768.0013c39ec880	20000	FWD	ROOT
xe-9/2/0	128:5	128:5	32768.0090690b47d1	2000	FWD	DESG
xe-9/3/0	128:6	128:6	32768.0090690b47d1	2000	FWD	DESG

```
Spanning tree interface parameters for instance 1
```

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ae1	128:1	128:1	32769.0090690b47d1	1000	FWD	DESG
ge-2/1/2	128:2	128:2	32769.0090690b47d1	20000	FWD	DESG
ge-2/1/5	128:3	128:3	32769.0090690b47d1	29999	FWD	DESG
ge-2/2/1	128:4	128:26	32769.0013c39ec880	20000	FWD	ROOT
xe-9/2/0	128:5	128:5	32769.0090690b47d1	2000	FWD	DESG
xe-9/3/0	128:6	128:6	32769.0090690b47d1	2000	FWD	DESG

```
Spanning tree interface parameters for instance 2
```

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ae1	128:1	128:1	32770.0090690b47d1	1000	FWD	DESG
ge-2/1/2	128:2	128:2	32770.0090690b47d1	20000	FWD	DESG
ge-2/1/5	128:3	128:3	32770.0090690b47d1	29999	FWD	DESG
ge-2/2/1	128:4	128:26	32770.0013c39ec880	20000	FWD	ROOT
xe-9/2/0	128:5	128:5	32770.0090690b47d1	2000	FWD	DESG
xe-9/3/0	128:6	128:6	32770.0090690b47d1	2000	FWD	DESG

show spanning-tree interface (QFX Series)

```
user@host> show spanning-tree interface routing-instance vs1 detail
```

Spanning tree interface parameters for instance 0

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ae1	128:1	128:1	32768.0090690b47d1	1000	FWD	DESG
ge-2/1/2	128:2	128:2	32768.0090690b47d1	20000	FWD	DESG
ge-2/1/5	128:3	128:3	32768.0090690b47d1	29999	FWD	DESG
ge-2/2/1	128:4	128:26	32768.0013c39ec880	20000	FWD	ROOT
xe-9/2/0	128:5	128:5	32768.0090690b47d1	2000	FWD	DESG
xe-9/3/0	128:6	128:6	32768.0090690b47d1	2000	FWD	DESG

Spanning tree interface parameters for instance 1

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ae1	128:1	128:1	32769.0090690b47d1	1000	FWD	DESG
ge-2/1/2	128:2	128:2	32769.0090690b47d1	20000	FWD	DESG
ge-2/1/5	128:3	128:3	32769.0090690b47d1	29999	FWD	DESG
ge-2/2/1	128:4	128:26	32769.0013c39ec880	20000	FWD	ROOT
xe-9/2/0	128:5	128:5	32769.0090690b47d1	2000	FWD	DESG
xe-9/3/0	128:6	128:6	32769.0090690b47d1	2000	FWD	DESG

Spanning tree interface parameters for instance 2

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ae1	128:1	128:1	32770.0090690b47d1	1000	FWD	DESG
ge-2/1/2	128:2	128:2	32770.0090690b47d1	20000	FWD	DESG
ge-2/1/5	128:3	128:3	32770.0090690b47d1	29999	FWD	DESG
ge-2/2/1	128:4	128:26	32770.0013c39ec880	20000	FWD	ROOT
xe-9/2/0	128:5	128:5	32770.0090690b47d1	2000	FWD	DESG
xe-9/3/0	128:6	128:6	32770.0090690b47d1	2000	FWD	DESG

show spanning-tree interface (EX Series)

```
user@switch> show spanning-tree interface
```

Spanning tree interface parameters for instance 0

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/0.0	128:513	128:513	8192.0019e2500340	1000	FWD	DESG
ge-0/0/2.0	128:515	128:515	8192.0019e2500340	1000	BLK	DIS
ge-0/0/4.0	128:517	128:517	8192.0019e2500340	1000	FWD	DESG
ge-0/0/23.0	128:536	128:536	8192.0019e2500340	1000	FWD	DESG

Spanning tree interface parameters for instance 1

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/0.0	128:513	128:513	8193.0019e2500340	1000	FWD	DESG
ge-0/0/2.0	128:515	128:515	8193.0019e2500340	1000	BLK	DIS
ge-0/0/4.0	128:517	128:517	8193.0019e2500340	1000	FWD	DESG
ge-0/0/23.0	128:536	128:536	8193.0019e2500340	1000	FWD	DESG

Spanning tree interface parameters for instance 2

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-0/0/0.0	128:513	128:1	8194.001b549fd000	1000	FWD	ROOT

```

ge-0/0/2.0 128:515 128:515 32770.0019e2500340 4000 BLK DIS
ge-0/0/4.0 128:517 128:1 16386.001b54013080 1000 BLK ALT
ge-0/0/23.0 128:536 128:536 32770.0019e2500340 1000 FWD DESG

```

show spanning-tree interface detail

```

user@host> show spanning-tree interface routing-instance vs1 detail
Spanning tree interface parameters for instance 0

```

```

Interface name           : ae1
Port identifier          : 128.1
Designated port ID      : 128.1
Port cost                : 1000
Port state               : Forwarding
Designated bridge ID     : 32768.00:90:69:0b:47:d1
Port role                : Designated
Link type                : Pt-Pt/NONEDGE
Boundary port            : No

```

```

Interface name           : ge-2/1/2
Port identifier          : 128.2
Designated port ID      : 128.2
Port cost                : 20000
Port state               : Forwarding
Designated bridge ID     : 32768.00:90:69:0b:47:d1
Port role                : Designated
Link type                : Pt-Pt/NONEDGE
Boundary port            : No

```

```

Interface name           : ge-2/1/5
Port identifier          : 128.3
Designated port ID      : 128.3
Port cost                : 29999
Port state               : Forwarding
Designated bridge ID     : 32768.00:90:69:0b:47:d1
Port role                : Designated
Link type                : Pt-Pt/NONEDGE
Boundary port            : No

```

```

Interface name           : ge-2/2/1
Port identifier          : 128.4
Designated port ID      : 128.26
Port cost                : 20000
Port state               : Forwarding
Designated bridge ID     : 32768.00:13:c3:9e:c8:80
Port role                : Root
Link type                : Pt-Pt/NONEDGE
Boundary port            : No

```

```

Interface name           : xe-9/2/0
Port identifier          : 128.5
Designated port ID      : 128.5
Port cost                : 2000
Port state               : Forwarding
Designated bridge ID     : 32768.00:90:69:0b:47:d1
Port role                : Designated
Link type                : Pt-Pt/NONEDGE
Boundary port            : No

```

```

Interface name           : xe-9/3/0

```

```
Port identifier           : 128.6
Designated port ID       : 128.6
Port cost                 : 2000
Port state                : Forwarding
Designated bridge ID     : 32768.00:90:69:0b:47:d1
Port role                 : Designated
Link type                 : Pt-Pt/NONEDGE
Boundary port            : No
```

Spanning tree interface parameters for instance 1

```
Interface name           : ae1
Port identifier           : 128.1
Designated port ID       : 128.1
Port cost                 : 1000
Port state                : Forwarding
Designated bridge ID     : 32768.00:90:69:0b:47:d1
Port role                 : Designated
Link type                 : Pt-Pt/NONEDGE
Boundary port            : No
```

```
Interface name           : ge-2/1/2
Port identifier           : 128.2
Designated port ID       : 128.2
Port cost                 : 20000
Port state                : Forwarding
Designated bridge ID     : 32768.00:90:69:0b:47:d1
Port role                 : Designated
Link type                 : Pt-Pt/NONEDGE
Boundary port            : No
```

```
Interface name           : ge-2/1/5
Port identifier           : 128.3
Designated port ID       : 128.3
Port cost                 : 29999
Port state                : Forwarding
Designated bridge ID     : 32768.00:90:69:0b:47:d1
Port role                 : Designated
Link type                 : Pt-Pt/NONEDGE
Boundary port            : No
```

```
Interface name           : ge-2/2/1
Port identifier           : 128.4
Designated port ID       : 128.26
Port cost                 : 20000
Port state                : Forwarding
Designated bridge ID     : 32768.00:13:c3:9e:c8:80
Port role                 : Root
Link type                 : Pt-Pt/NONEDGE
Boundary port            : No
```

...

show spanning-tree interface detail (EX Series)

```
user@switch> show spanning-tree interface detail
Spanning tree interface parameters for instance 0
```

```
Interface name           : ge-1/0/0.0
Port identifier           : 128.625
```

```
Designated port ID      : 128.625
Port cost                : 20000
Port state               : Blocking
Designated bridge ID    : 32768.00:19:e2:50:95:a0
Port role                : Disabled
Link type                : Pt-Pt/EDGE
Boundary port           : NA
Edge delay while expiry count : 0
Rcvd info while expiry count : 0

Interface name          : ge-1/0/1.0
Port identifier         : 128.626
Designated port ID      : 128.626
Port cost                : 20000
Port state               : Blocking
Designated bridge ID    : 32768.00:19:e2:50:95:a0
Port role                : Disabled
Link type                : Pt-Pt/NONEDGE
Boundary port           : NA
Edge delay while expiry count : 0
Rcvd info while expiry count : 0

Interface name          : ge-1/0/2.0
Port identifier         : 128.627
Designated port ID      : 128.627
Port cost                : 20000
Port state               : Blocking
Designated bridge ID    : 32768.00:19:e2:50:95:a0
Port role                : Disabled
Link type                : Pt-Pt/NONEDGE
Boundary port           : NA
Edge delay while expiry count : 0
Rcvd info while expiry count : 0

Interface name          : ge-1/0/10.0
Port identifier         : 128.635
Designated port ID      : 128.635
Port cost                : 20000
Port state               : Blocking
Designated bridge ID    : 32768.00:19:e2:50:95:a0
Port role                : Disabled
Link type                : Pt-Pt/NONEDGE
Boundary port           : NA
Edge delay while expiry count : 0
Rcvd info while expiry count : 0

Interface name          : ge-1/0/20.0
Port identifier         : 128.645
Designated port ID      : 128.645
Port cost                : 20000
Port state               : Blocking
Designated bridge ID    : 32768.00:19:e2:50:95:a0
Port role                : Disabled
Link type                : Pt-Pt/NONEDGE
Boundary port           : NA
Edge delay while expiry count : 0
Rcvd info while expiry count : 0
[output truncated]
```

show spanning-tree interface msti

```
user@host> show spanning-tree interface msti 1 routing-instance vs1 detail
Spanning tree interface parameters for instance 1
```

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
xe-7/0/0	128:1	128:1	32769.0090690b4fd1	2000	FWD	DESG
ge-5/1/0	128:2	128:2	32769.0090690b4fd1	20000	FWD	DESG
ge-5/1/1	128:3	128:3	32769.0090690b4fd1	20000	FWD	DESG
ae1	128:4	128:1	32769.0090690b47d1	10000	BLK	ALT
ge-5/1/4	128:5	128:3	32769.0090690b47d1	20000	BLK	ALT
xe-7/2/0	128:6	128:6	32769.0090690b47d1	2000	FWD	ROOT

show spanning-tree interface vlan-id

```
user@host> show spanning-tree interface vlan-id 101 routing-instance vs1 detail
Spanning tree interface parameters for instance 0
```

Interface	Port ID	Designated port ID	Designated bridge ID	Port Cost	State	Role
ge-11/0/5	128:1	128:1	32768.0090690b7fd1	20000	FWD	DESG
ge-11/0/6	128:2	128:1	32768.0090690b7fd1	20000	BLK	BKUP
ge-11/1/0	128:3	128:2	32768.0090690b4fd1	20000	BLK	ALT
ge-11/1/1	128:4	128:3	32768.0090690b4fd1	20000	BLK	ALT
ge-11/1/4	128:5	128:1	32768.0090690b47d1	20000	BLK	ALT
xe-10/0/0	128:6	128:5	32768.0090690b4fd1	2000	BLK	ALT
xe-10/2/0	128:7	128:4	32768.0090690b47d1	2000	FWD	ROOT

show spanning-tree interface (VSTP)

```
user@host> show spanning-tree interface
Spanning tree interface parameters for instance 0
```

Interface	Port ID	Designated port ID	Designated bridge ID	Cost	State	Role
ge-1/0/1	128:1	128:1	28672.0090690b3fe0	20000	FWD	DESG
ge-1/0/2	128:2	128:2	28672.0090690b3fe0	20000	FWD	DESG

```
Spanning tree interface parameters for VLAN 10
```

Interface	Port ID	Designated port ID	Designated bridge ID	Cost	State	Role
ge-1/0/1	128:1	128:1	28672.0090690b3fe0	20000	FWD	DESG
ge-1/0/2	128:2	128:2	28672.0090690b3fe0	20000	FWD	DESG

```
Spanning tree interface parameters for VLAN 20
```

Interface	Port ID	Designated port ID	Designated bridge ID	Cost	State	Role
ge-1/0/1	128:1	128:1	28672.0090690b3fe0	20000	FWD	DESG
ge-1/0/2	128:2	128:2	28672.0090690b3fe0	20000	FWD	DESG

show spanning-tree interface vlan-id (VSTP)

```
user@host> show spanning-tree interface vlan-id 10
Spanning tree interface parameters for VLAN 10
```

Interface	Port ID	Designated port ID	Designated bridge ID	Cost	State	Role
-----------	---------	-----------------------	-------------------------	------	-------	------

ge-1/0/1	128:1	128:1	28672.0090690b3fe0	20000	FWD	DESG
ge-1/0/2	128:2	128:2	28672.0090690b3fe0	20000	FWD	DESG

show spanning-tree interface brief (EX Series)

```
user@switch> show spanning-tree interface brief
Spanning tree interface parameters for instance 0
```

Interface	Port ID	Designated	Designated	Port	State	Role
port ID	bridge ID	Cost				
ge-1/0/0.0	128:625	128:625	32768.0019e25095a0	20000	BLK	DIS
ge-1/0/1.0	128:626	128:626	32768.0019e25095a0	20000	BLK	DIS
ge-1/0/2.0	128:627	128:627	32768.0019e25095a0	20000	BLK	DIS
ge-1/0/10.0	128:635	128:635	32768.0019e25095a0	20000	BLK	DIS
ge-1/0/20.0	128:645	128:645	32768.0019e25095a0	20000	BLK	DIS
ge-1/0/30.0	128:655	128:655	32768.0019e25095a0	20000	BLK	DIS

show spanning-tree interface ge-1/0/0 (EX Series)

```
user@switch> show spanning-tree interface ge-1/0/0
```

Interface	Port ID	Designated	Designated	Port	State	Role
port ID	bridge ID	Cost				
ge-1/0/0.0	128:625	128:625	32768.0019e25095a0	20000	BLK	DIS

show spanning-tree mstp configuration

List of Syntax	Syntax on page 386 Syntax (EX Series Switch and the QFX Series) on page 386
Syntax	<code>show spanning-tree mstp configuration</code> <code><brief detail></code> <code><routing-instance <i>routing-instance-name</i>></code>
Syntax (EX Series Switch and the QFX Series)	<code>show spanning-tree mstp configuration</code> <code><brief detail></code>
Release Information	Command introduced in Junos OS Release 8.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series.
Description	Display the MSTP configuration.
Options	none —Display MSTP configuration information. brief detail —(Optional) Display the specified level of output. routing-instance <i>routing-instance-name</i> —(Optional) Display MSTP configuration information for the specified routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Understanding MSTP on page 48• Example: Configuring Network Regions for VLANs with MSTP on non-ELS EX Series Switches on page 217• show spanning-tree bridge on page 372• show spanning-tree statistics on page 389• mstp on page 320
List of Sample Output	show spanning-tree mstp configuration detail on page 387 show spanning-tree mstp configuration detail (QFX Series) on page 387 show spanning-tree mstp configuration (EX Series) on page 387
Output Fields	Table 28 on page 387 lists the output fields for the show spanning-tree mstp configuration command. Output fields are listed in the approximate order in which they appear.

Table 28: show spanning-tree mstp configuration Output Fields

Field Name	Field Description
Context id	Internally generated identifier.
Region name	MSTP region name carried in the MSTP BPDUs.
Revision	Revision number of the MSTP configuration.
Configuration digest	Numerical value derived from the VLAN-to-instance mapping table.
MSTI	MST instance identifier.
Member VLANs	VLAN identifiers associated with the MSTI.

Sample Output

show spanning-tree mstp configuration detail

```

user@host> show spanning-tree mstp configuration routing-instance vs1 detail
MSTP configuration information
Context identifier      : 1
Region name            : henry
Revision                : 3
Configuration digest    : 0x6da4b5c4fd587757eef35675365e1

MSTI      Member VLANs
0 0-99,101-199,201-4094
1 100
2 200

```

show spanning-tree mstp configuration detail (QFX Series)

```

user@1f0> show spanning-tree mstp configuration routing-instance vs1 detail
MSTP configuration information
Context identifier      : 1
Region name            : henry
Revision                : 3
Configuration digest    : 0x6da4b5c4fd587757eef35675365e1

MSTI      Member VLANs
0 0-99,101-199,201-4094
1 100
2 200

```

show spanning-tree mstp configuration (EX Series)

```

user@host> show spanning-tree mstp configuration
MSTP configuration information
Context identifier      : 0
Region name            : region1
Revision                : 0
Configuration digest    : 0xc92e7af9febb44d8df928b87f16b

```

MSTI	Member VLANs
0	0-100,105-4094
1	101-102
2	103-104

show spanning-tree statistics

List of Syntax	Syntax on page 389 Syntax (EX Series and QFX Series) on page 389 Syntax (EX Series) on page 389
Syntax	<pre>show spanning-tree statistics <brief detail> <interface <i>interface-name</i>> <routing-instance <i>routing-instance-name</i>></pre>
Syntax (EX Series and QFX Series)	<pre>show spanning-tree statistics <brief detail> <interface <i>interface-name</i> vlan <i>vlan-id</i>></pre>
Syntax (EX Series)	<pre>show spanning-tree statistics interface <i>interface-name</i> vlan <i>vlan-id</i> <brief detail></pre>
Release Information	<p>Command introduced in Junos OS Release 8.4.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Command introduced in Junos OS Release 11.1 for QFX Series switches.</p>
Description	Display STP statistics.
Options	<p>none—Display brief STP statistics.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>interface <i>interface-name</i>—(Optional) Display STP statistics for the specified interface.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display STP statistics for the specified routing instance.</p>
Required Privilege Level	view
List of Sample Output	show spanning-tree statistics routing-instance on page 390 show spanning-tree statistics interface routing-instance detail on page 390
Output Fields	<p>Table 29 on page 389 lists the output fields for the show spanning-tree statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 29: show spanning-tree statistics Output Fields

Field Name	Field Description
Message type	Type of message being counted.

Table 29: show spanning-tree statistics Output Fields (*continued*)

Field Name	Field Description
BPDUs sent	Total number of BPDUs sent.
BPDUs received	Total number of BPDUs received.
BPDUs sent in last interval	Number of BPDUs sent within a specified interval.
BPDUs received in last interval	Number of BPDUs received within a specified interval.
Interface	Interface for which the statistics are being displayed.
Next BPDU transmission	Number of seconds until the next BPDU is scheduled to be sent.

Sample Output

show spanning-tree statistics routing-instance

```

user@host> show spanning-tree statistics routing-instance vs1 detail
Routing instance level STP statistics
Message type           : bpdus
BPDUs sent              : 1396
BPDUs received          : 1027
BPDUs sent in last interval : 5      (duration: 4 sec)
BPDUs received in last interval: 4    (duration: 4 sec)

```

show spanning-tree statistics interface routing-instance detail

```

user@host> show spanning-tree statistics interface ge-11/1/4 routing-instance vs1 detail
Interface  BPDUs sent  BPDUs received  Next BPDU
                                     transmission
ge-11/1/4      7           190           0

```

show spanning-tree statistics bridge

Syntax	show spanning-tree statistics bridge
Release Information	Command introduced in Junos OS Release 14.1.
Description	Display the STP statistics of the bridge.
Required Privilege Level	view
List of Sample Output	show spanning-tree statistics bridge (MX Series) on page 391
Output Fields	Table 30 on page 391 describes the output fields for the show spanning-tree statistics bridge command. Output fields are listed in the approximate order in which they appear.

Table 30: show spanning-tree statistics bridge Output Fields

Field Name	Field Description
STP Context	Context of STP instances saved for each routing instance. All STP instances in the same routing instances have same context.
STP Instance	Instance number that uniquely identifies each STP session per routing instance.
Number of Root Bridge Changes	Counts the number of Root Bridge change events.
Number of Root Port Changes	Counts the number of Root Port change events.
Recent TC Received	Details about the last topology change received.

Sample Output

show spanning-tree statistics bridge (MX Series)

```

user@host> show spanning-tree statistics bridge
STP Context : default
STP Instance : 0
Number of Root Bridge Changes: 1      Last Changed: Wed Oct 23 07:10:05
2013
Number of Root Port Changes: 2      Last Changed: Wed Oct 23 07:10:05
2013
Recent TC Received: ge-3/1/4.32767    Received : Wed Oct 23 07:10:07
2013

```

show spanning-tree statistics interface

Syntax	show spanning-tree statistics interface
Release Information	Command introduced in Junos OS Release 14.1.
Description	Display the STP statistics related to the interface.
Required Privilege Level	view
List of Sample Output	show spanning-tree statistics interface (MX Series) on page 392
Output Fields	Table 31 on page 392 describes the output fields for the show spanning-tree statistics interface command. Output fields are listed in the approximate order in which they appear.

Table 31: show spanning-tree statistics interface Output Fields

Field Name	Field Description
Interface	Interface name.
BPDUs sent	Total number of BPDUs sent from the bridge on the interface.
BPDUs received	Total number of BPDUs received by the bridge on the interface.
Next BPDU Transmission	Time after which the next BPDU is sent by the bridge on the interface.
TC Tx/Rx	Total number of Topology Change BPDUs sent or received on the interface.
Proposal Tx/Rx	Total number of Proposal BPDUs sent or received on the interface.
Agreement Tx/Rx	Total number of Agreement BPDUs sent or received on the interface.

Sample Output

show spanning-tree statistics interface (MX Series)

```
user@host> show spanning-tree statistics interface
```

Interface	BPDUs Sent	BPDUs Received	Next BPDU Transmission	TCs Tx/Rx	Proposal Tx/Rx	Agreement Tx/Rx
xe-0/0/0	49	3	1	5/2	0/2	1/0
ge-1/0/0	48	1	1	5/1	0/1	1/1

show spanning-tree statistics message-queues

Syntax	show spanning-tree statistics message-queues
Release Information	Command introduced in Junos OS Release 14.1.
Description	Display the STP message queues-related statistics.
Required Privilege Level	view
List of Sample Output	show spanning-tree statistics message-queues (MX Series) on page 393
Output Fields	Table 32 on page 393 describes the output fields for the show spanning-tree statistics message-queues command. Output fields are listed in the approximate order in which they appear.

Table 32: show spanning-tree statistics message-queues Output Fields

Field Name	Field Description
Queue	PPMD name.
Current size	Number of packets currently present in the queue.
High-watermark	Maximum number of packets present in the queue at any time.
max/avg wait time	Maximum or average time packet waiting to be consumed.

Sample Output

show spanning-tree statistics message-queues (MX Series)

```
user@host> show spanning-tree statistics message-queues
```

Queue	Current size	High-watermark	max/avg wait time
PPMD-TX	15	142	17636884/17636884
PPMD-RX	18	83	18866272/18866272

show spanning-tree stp-buffer see-all

Syntax	<pre>show spanning-tree stp-buffer see-all <stp-instance stp-instance-id routing-instance instance-name> <vlan vlan-id routing-instance instance-name></pre>
Release Information	Command introduced in Junos OS Release 14.1.
Description	Display the configured STP (RSTP, MSTP, VSTP) interface parameters.
Options	<p>none— Display STP (RSTP, MSTP, VSTP) interface role/state changes that are logged into internal memory called the buffer. Entries in the buffer depend on the user configuration.</p> <p>stp-instance <i>stp-instance-id</i> routing-instance <i>instance-name</i>— (Optional) Display the STP buffer for the specified stp-instance and routing instance.</p> <p>vlan <i>vlan-id</i> routing-instance <i>instance-name</i>— (Optional) Display the STP buffer for the specified vlan id and routing instance.</p>
Required Privilege Level	view
List of Sample Output	<p>show spanning-tree stp-buffer see-all (MX Series) on page 395</p> <p>show spanning-tree stp-buffer see-all stp-instance stp-instance-id routing-instance instance-name (MX Series) on page 396</p> <p>show spanning-tree stp buffer see-all vlan vlan-id routing-instance instance-name (MX Series) on page 397</p>
Output Fields	Table 33 on page 394 describes the output fields for the show spanning-tree stp-buffer see-all command. Output fields are listed in the approximate order in which they appear.

Table 33: show spanning-tree stp-buffer see-all Output Fields

Field Name	Field Description	Level of Output
Global Events	<p>Displays events when PPMD RX/TX queues reach 70 % of their maximum queue size. The following indicates received queue status:</p> <ul style="list-style-type: none"> GT — Greater than 70 % of their maximum queue size. LT — Less than 70 % of their maximum queue size. 	none, stp-instance , vlan
Per STP instance Information	Information about every STP instance.	none, stp-instance , vlan
Routing Inst	Routing instance to which the STP instance belongs.	none, stp-instance , vlan

Table 33: show spanning-tree stp-buffer see-all Output Fields (*continued*)

Field Name	Field Description	Level of Output
STP Instance	Instance number that uniquely identifies each STP session per routing-instance.	none, stp-instance
Root Bridge	Bridge priority and bridge ID of ROOT bridge in the topology.	none, vlan
Root Port	Information about ROOT port, if any, on the local bridge at the displayed timestamp.	none, vlan
TC Received	Time at which topology change was received and on which port.	none, stp-instance, vlan
TC Generated	Time at which topology change occurred and on which port.	none, stp-instance, vlan
Port	The interface where the event is occurring.	none, stp-instance, vlan
State	STP state of the port. The following are the types of state: <ul style="list-style-type: none"> Forwarding — Port forwards the traffic and is included in active topology and learns MAC addresses. Blocking — Port does not forward traffic and is not included in active topology. Does not learn MAC addresses. 	none, vlan
Role	Role of the port. The following are the types of ports: <ul style="list-style-type: none"> Root — Port closest to the Root bridge. Designated — Port sends the best BPDU on the connected segment. Alternate — Port blocked for receiving more useful BPDUs from another bridge. Disabled — Port is disabled. Cannot send or receive BPDUs. 	none, stp-instance, vlan

Sample Output

show spanning-tree stp-buffer see-all (MX Series)

```

user@host> show spanning-tree stp-buffer see-all
1. Global Events:
Time at which different Queue's reached 70% of the Maximum Q-size
Mar 18 13:18:04 RCV_Q GT
Mar 18 13:18:57 RCV_Q LT

```

Mar 18 13:19:33 XMIT_Q GT

2. Per STP Instance Information :

Routing Inst : default
 STP Instance : 02
 Root Bridge : 12288.00:23:9c:f0:17:d0 Mar 18 13:18:04
 STP Instance : 03
 Root Port : ge-0/1/2 Mar 18 13:18:38
 STP Instance : 03
 TC Received : ge-0/0/2 Mar 18 15:12:12
 STP Instance : 03
 TC Generated: ge-0/2/2 Mar 18 15:13:27

3. This section will print the time stamp for per Instance - port event changes.

STP Instance : 02
 Port : ge-1/0/0 Mar 22 13:35:02
 State : FWD S
 Role : DESG

STP Instance : 00
 Port : ge-0/0/3 Mar 22 14:03:46
 State : BLK
 Role : ALT R
 STP Instance : 00
 Port : ge-1/0/0 Mar 28 02:03:49
 State : BLK S
 Role : ALT

show spanning-tree stp-buffer see-all stp-instance-id routing-instance instance-name (MX Series)

user@host> show spanning-tree stp-buffer see-all stp-instance 0 routing-instance mstp_inst

1. Global Events:

Time at which different Queue's reached 70% of the Maximum Q-size
 No Entry So far

2. Per STP Instance Information :

Routing Inst : mstp_inst

STP Instance : 0
 TC Generated : ge-3/0/5.32767 Tue Dec 17 06:00:50 2013
 STP Instance : 0
 TC Generated : ge-3/1/1.32767 Tue Dec 17 06:00:50 2013
 STP Instance : 0
 TC Received : ge-3/0/5.32767 Tue Dec 17 06:00:50 2013
 STP Instance : 0
 TC Received : ge-3/0/5.32767 Tue Dec 17 06:00:50 2013
 STP Instance : 0
 TC Received : ge-3/0/5.32767 Tue Dec 17 06:00:51 2013
 STP Instance : 0
 TC Received : ge-3/0/5.32767 Tue Dec 17 06:00:53 2013

3. This section will print the time stamp for per Instance, Port Event changes.

STP Instance : 0
 Port : ge-3/0/5.32767 Tue Dec 17 06:00:49 2013

```

State      : BLK S
Role       : DIS

STP Instance : 0
Port       : ge-3/0/5.32767 Tue Dec 17 06:00:49 2013
State      : BLK
Role       : DESG R

STP Instance : 0
Port       : ge-3/1/1.32767 Tue Dec 17 06:00:49 2013
State      : BLK S
Role       : DIS

STP Instance : 0
Port       : ge-3/1/1.32767 Tue Dec 17 06:00:49 2013
State      : BLK
Role       : DESG R

STP Instance : 0
Port       : ge-3/0/5.32767 Tue Dec 17 06:00:50 2013
State      : FWD S
Role       : DESG

STP Instance : 0
Port       : ge-3/1/1.32767 Tue Dec 17 06:00:50 2013
State      : FWD S
Role       : DESG

```

show spanning-tree stp buffer see-all vlan vlan-id routing-instance instance-name (MX Series)

```

user@host> show spanning-tree stp-buffer see-all vlan 10 routing-instance vstp_inst
1. Global Events:
Time at which different Queue's reached 70% of the Maximum Q-size
Mar 18 13:18:04 RCV_Q GT
Mar 18 13:18:57 RCV_Q LT
Mar 18 13:19:33 XMIT_Q GT

2. Per STP Instance Information :
Routing Inst   : default
VLAN ID       : 02
Root Bridge    : 12288.00:23:9c:f0:17:d0 Mar 18 13:18:04
VLAN ID       : 03
Root Port      : ge-0/1/2 Mar 18 13:18:38
VLAN ID       : 03
TC Received    : ge-0/0/2 Mar 18 15:12:12
VLAN ID       : 03
TC Generated   : ge-0/2/2 Mar 18 15:13:27

3. This section will print the time stamp for per Instance - port event changes.
VLAN ID : 02
Port     : ge-1/0/0 Mar 22 13:35:02
State    : FWD S
Role     : DESG

VLAN ID : 00
Port     : ge-0/0/3 Mar 22 14:03:46
State    : BLK
Role     : ALT R
VLAN ID : 00
Port     : ge-1/0/0 Mar 28 02:03:49

```

State : BLK S
Role : ALT