JUNIPER NETWORKS

Junos® OS

Spanning-Tree Protocol Options Feature Guide for Routing Devices

Release
13.2

Published: 2013-07-22

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS Spanning-Tree Protocol Options Feature Guide for Routing Devices
13.2

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 http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Supported Platforms

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

- MX Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

Table 1 on page xi 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.

Table 2 on page xi 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`

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

Convention	Description	Examples
Italic text like this	• Introduces or emphasizes important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

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

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (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 send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/

- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Spanning-Tree Protocol Options

Loop Protection for Spanning-Tree Instance Interfaces Overview

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.

You can configure spanning-tree protocol loop protection to improve the stability of Layer 2 networks.

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

- Loop Protection for a Spanning-Tree Instance Interface on page 13
- Configuring Loop Protection for a Spanning-Tree Instance Interface on page 21
- Example: Enabling Loop Protection for Spanning-Tree Protocols on page 35

Root Protection for Spanning-Tree Instance Interfaces Overview

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.

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

- Root Protect for a Spanning-Tree Instance Interface on page 14
- Enabling Root Protect for a Spanning-Tree Instance Interface on page 20

BPDU Protection for Spanning-Tree Instance Interfaces Overview

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

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

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

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

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

- **vlan-vpls**
- **extended-vlan-vpls**

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

Related Documentation

- Configuring BPDU Protection on Individual Interfaces on page 23
- Configuring BPDU Protection on All Edge Ports on page 24
- *Spanning-Tree Protocols Supported on MX Series Routers*
- Root Protection for Spanning-Tree Instance Interfaces Overview on page 4
- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview on page 5

VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview

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*.

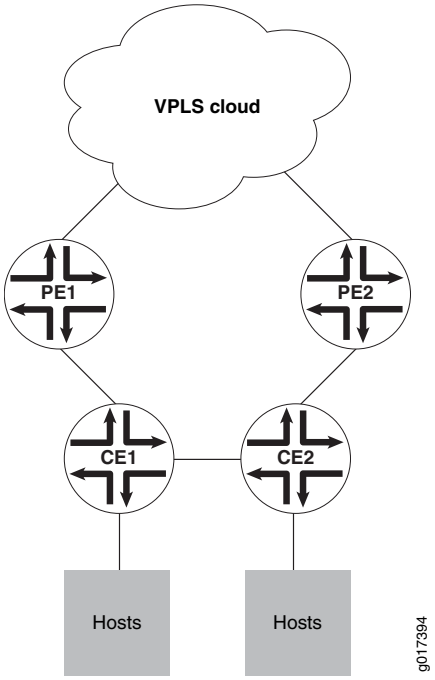
Related Documentation

- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 6
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning Tree Behavior on page 24
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning Tree Behavior on page 26
- Example: Configuring VPLS Root Topology Change Actions on page 35

VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology

Figure 1 on page 6 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 1: 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

- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview on page 5
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning Tree Behavior on page 24
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning Tree Behavior on page 26
- Example: Configuring VPLS Root Topology Change Actions on page 35

Layer 2 Protocol Tunneling Through a Network Overview

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

Layer 2 protocol tunneling is supported on MX Series routers with Enhanced (Dense Port Concentrators) DPCs and Enhanced Queuing (DPCs), see Table 4 on page 8 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 3 on page 8 shows the MPCs and Enhanced DPCs supported when configuring Layer 2 protocol tunneling and VPLS.

Table 3: 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 4 on page 8 lists the DPCs that support the Layer 2 tunneling protocol.

Table 4: DPCs Supported for Layer 2 Protocol Tunneling

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

Table 4: DPCs Supported for Layer 2 Protocol Tunneling *(continued)*

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

NOTE: When an MX Series router 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 33
- *Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface*
- *Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface*

PART 2

Configuration

CHAPTER 2

Configuration Guidelines for Spanning-Tree Protocol Options

Loop Protection for a Spanning-Tree Instance Interface

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.**

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.

Related Documentation

- Loop Protection for Spanning-Tree Instance Interfaces Overview on page 3
- Configuring Loop Protection for a Spanning-Tree Instance Interface on page 21
- Example: Enabling Loop Protection for Spanning-Tree Protocols on page 35
- **bpdu-timeout-action on page 42**
- *interface (Spanning Tree)*

Root Protect for a Spanning-Tree Instance Interface

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.

Related Documentation

- Root Protection for Spanning-Tree Instance Interfaces Overview on page 4
- Enabling Root Protect for a Spanning-Tree Instance Interface on page 20
- *interface (Spanning Tree)*
- **no-root-port on page 43**

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

- Root Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection for Spanning-Tree Instance Interfaces Overview on page 4
- Configuring BPDU Protection on Individual Interfaces on page 23

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

- Root Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection for Spanning-Tree Instance Interfaces Overview on page 4
- Configuring BPDU Protection on All Edge Ports on page 24

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

- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview on page 5
- VPLS Multihoming: Hold Time Before Switching to Primary Priority on page 16
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning Tree Behavior on page 24
- Example: Configuring VPLS Root Topology Change Actions on page 35

VPLS Multihoming: Hold Time Before Switching to Primary Priority

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 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

- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview on page 5
- VPLS Multihoming: Priority of the Backup Bridge on page 15
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning Tree Behavior on page 24
- Example: Configuring VPLS Root Topology Change Actions on page 35

VPLS Multihoming: System Identifier for Bridges in the Ring

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 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

- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview on page 5
- VPLS Multihoming: Priority of the Backup Bridge on page 15
- VPLS Multihoming: Hold Time Before Switching to Primary Priority on page 16
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning Tree Behavior on page 24
- Example: Configuring VPLS Root Topology Change Actions on page 35

VPLS Multihoming: Bridge Flush of MAC Cache on Topology Change

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.

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

- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview on page 5
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning Tree Behavior on page 24
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning Tree Behavior on page 26

- Example: Configuring VPLS Root Topology Change Actions on page 35

CHAPTER 3

Configuration Tasks for Spanning-Tree Protocol Options

Loop Protection for a Spanning-Tree Instance Interface

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.

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.

Related Documentation

- Loop Protection for Spanning-Tree Instance Interfaces Overview on page 3
- Configuring Loop Protection for a Spanning-Tree Instance Interface on page 21
- Example: Enabling Loop Protection for Spanning-Tree Protocols on page 35
- **bpdu-timeout-action on page 42**
- *interface (Spanning Tree)*

Enabling Root Protect 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

- Root Protection for Spanning-Tree Instance Interfaces Overview on page 4
- Root Protect for a Spanning-Tree Instance Interface on page 14

Configuring Loop Protection for a Spanning-Tree Instance Interface

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

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

To configure enhanced loop protection:

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

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

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

   - For all MSTP instances on a physical interface:

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

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

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

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

Related Documentation

- Loop Protection for Spanning-Tree Instance Interfaces Overview on page 3
- Loop Protection for a Spanning-Tree Instance Interface on page 13
- Example: Enabling Loop Protection for Spanning-Tree Protocols on page 35

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

- Root Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection for Spanning-Tree Instance Interfaces Overview on page 4
- Configuring BPDU Protection on Individual Interfaces on page 23

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

- Root Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection for Spanning-Tree Instance Interfaces Overview on page 4
- Configuring BPDU Protection on All Edge Ports on page 24

Configuring BPDU Protection on Individual Interfaces

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

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

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

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

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

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

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

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

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

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

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

Related Documentation

- Root Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 14

Configuring BPDU Protection on All Edge Ports

On MX Series routers, 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

- Root Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection on All Edge Ports of the Bridge on page 14

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# setvpls-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

- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview on page 5
- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 6
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning Tree Behavior on page 26
- Example: Configuring VPLS Root Topology Change Actions on page 35

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Related Documentation

- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview on page 5
- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 6
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning Tree Behavior on page 24
- Example: Configuring VPLS Root Topology Change Actions on page 35

CHAPTER 4

Configuration Guidelines for Layer 2 Protocol Tunneling

MAC Address Rewriting Enabled for Layer 2 Protocol Tunneling

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

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 7
- Layer 2 Protocol Tunnel Interface on page 29
- Layer 2 Protocol to be Tunneled on page 30
- Configuring Layer 2 Protocol Tunneling on page 33

Layer 2 Protocol Tunnel Interface

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

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

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

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 7
- MAC Address Rewriting Enabled for Layer 2 Protocol Tunneling on page 29
- Layer 2 Protocol to be Tunneled on page 30
- Configuring Layer 2 Protocol Tunneling on page 33

Layer 2 Protocol to be Tunneled

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.

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 7
- MAC Address Rewriting Enabled for Layer 2 Protocol Tunneling on page 29
- Layer 2 Protocol Tunnel Interface on page 29

- Configuring Layer 2 Protocol Tunneling on page 33

CHAPTER 5

Configuration Task for Layer 2 Protocol Tunneling

Configuring Layer 2 Protocol Tunneling

To configure Layer 2 protocol tunneling:

1. Enable MAC address rewriting for Layer 2 protocol tunneling:

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

2. Configure the Layer 2 protocol tunnel interface:

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

4. Verify the configuration:

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

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 7
- *Checking for a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface*
- *Clearing a MAC Rewrite Error Condition Blocking a Spanning-Tree Instance Interface*

CHAPTER 6

Spanning-Tree Protocol Options and Tunneling Examples

Example: Enabling Loop Protection for Spanning-Tree Protocols

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

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

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

Related Documentation

- Loop Protection for a Spanning-Tree Instance Interface on page 13
- Loop Protection for Spanning-Tree Instance Interfaces Overview on page 3

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

- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview on page 5
- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 6
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning Tree Behavior on page 24
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning Tree Behavior on page 26

CHAPTER 7

Configuration Statements for Spanning-Tree Protocols

[edit protocols mstp] Hierarchy Level

The following statement hierarchy can also be included at the **[edit logical-systems *logical-system-name*]** hierarchy level.

```
protocols {
    mstp {
        disable;
        backup-bridge-priority priority;
        bpdu-block-on-edge;
        bpdu-destination-mac-address provider-bridge-group;
        bridge-priority priority;
        configuration-name configuration-name;
        forward-delay seconds;
        hello-time seconds;
        interface interface-name {
            bpdu-timeout-action {
                alarm;
                block;
            }
            cost cost;
            edge;
            mode (point-to-point | shared);
            no-root-port;
            priority interface-priority;
        }
        max-age seconds;
        max-hops hops;
        msti identifier {
            backup-bridge-priority priority;
            bridge-priority priority;
            interface interface-name {
```

```
            cost cost;
            priority interface-priority;
          }
          vlan [ vlan-ids ];
        }
        priority-hold-time seconds;
        revision-level revision-level;
        system-id mac-address {
          ip-address ip-address</prefix-length>;
        }
        traceoptions {
          file filename <files number> <size maximum-file-size> <world-readable |
            no-world-readable>;
          flag flag <disable>;
        }
        vpls-flush-on-topology-change;
      }
    }
```

Related Documentation

- *Notational Conventions Used in Junos OS Configuration Hierarchies*
- *[edit protocols] Hierarchy Level*

[edit protocols rstp] Hierarchy Level

The following statement hierarchy can also be included at the **[edit logical-systems *logical-system-name*]** hierarchy level.

```
protocols {
  rstp {
    disable;
    backup-bridge-priority priority;
    bpdu-block-on-edge;
    bpdu-destination-mac-address provider-bridge-group;
    bridge-priority priority;
    extended-system-id id;
    force-version stp;
    forward-delay seconds;
    hello-time seconds;
    interface interface-name {
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost cost;
      edge;
      mode (point-to-point | shared);
      no-root-port;
      priority interface-priority;
    }
    max-age seconds;
    priority-hold-time seconds;
    system-id mac-address {
      ip-address ip-address</prefix-length>;
    }
```

```
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
    vpls-flush-on-topology-change;
  }
}
```

Related Documentation

- *Notational Conventions Used in Junos OS Configuration Hierarchies*
- *[edit protocols] Hierarchy Level*

[edit protocols vstp] Hierarchy Level

The following statement hierarchy can also be included at the **[edit logical-systems *logical-system-name*]** hierarchy level.

```
protocols {
  vstp {
    disable;
    bpdu-block-on-edge;
    force-version stp;
    interface interface-name {
        access-trunk
        bpdu-timeout-action {
      alarm;
        block;
      }
      cost cost;
      edge;
      mode (point-to-point | shared);
      no-root-port;
      priority interface-priority;
    }
    priority-hold-time seconds;
    system-id mac-address {
      ip-address ip-address</prefix-length>;
    }
    vlan vlan-id {
      ... the vlan subhierarchy appears after the main [edit protocols vstp] hierarchy level ...
    }
    vpls-flush-on-topology-change;
  }

  vstp {
    vlan vlan-id {
      backup-bridge-priority priority;
      bridge-priority priority;
      forward-delay seconds;
      hello-time seconds;
      interface interface-name {
        ... same statements as at the [edit protocols vstp interface interface-name] hierarchy
          level ...
      }
```

```
            max-age seconds;
            traceoptions {
              file filename <files number> <size maximum-file-size> <world-readable |
                no-world-readable>;
              flag flag <disable>;
            }
          }
        }
      }
```

Related Documentation

- *Notational Conventions Used in Junos OS Configuration Hierarchies*
- *[edit protocols] Hierarchy Level*

backup-bridge-priority

Syntax backup-bridge-priority *priority*;

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

Release Information Statement introduced in Junos OS Release 10.0.

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

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

Range: 0 through 61,440

Default: 32,768

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

Related Documentation

- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview on page 5
- Configuring VPLS Root Protection Topology Change Actions to Control VLAN Spanning Tree Behavior on page 26
- Configuring VPLS Root Protection Topology Change Actions to Control Global Spanning Tree Behavior on page 24
- VPLS Multihoming: Priority of the Backup Bridge on page 15

bpdu-block-on-edge

Syntax bpdu-block-on-edge;

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

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

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

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

Related Documentation

- BPDU Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection on All Edge Ports of the Bridge on page 14
- Configuring BPDU Protection on All Edge Ports on page 24

bpdu-timeout-action

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

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

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

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

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

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

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

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

Related Documentation
- Loop Protection for Spanning-Tree Instance Interfaces Overview on page 3
- Configuring Loop Protection for a Spanning-Tree Instance Interface on page 21
- Example: Enabling Loop Protection for Spanning-Tree Protocols on page 35

no-root-port

Syntax no-root-port;

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

Release Information Statement introduced in Junos OS Release 9.1.
Support for logical systems added in Junos OS Release 9.6.

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

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

Related Documentation
- Root Protection for Spanning-Tree Instance Interfaces Overview on page 4
- Root Protect for a Spanning-Tree Instance Interface on page 14
- Enabling Root Protect for a Spanning-Tree Instance Interface on page 20

priority-hold-time

Syntax priority-hold-time *seconds*;

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

Release Information Statement introduced in Junos OS Release 10.0.

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

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

Range: 1 through 255

Default: 2 seconds

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

Related Documentation
- VPLS Multihoming: Hold Time Before Switching to Primary Priority on page 16

system-id

Syntax

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

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 10.0.

Description

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

Options

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

Range: Any valid value

Default: None

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

Range: Any valid IP address

Default: None

Required Privilege Level

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

Related Documentation

- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Overview on page 5
- VPLS Multihomed Layer 2 Ring and MPLS Infrastructure Topology on page 6
- VPLS Multihoming: System Identifier for Bridges in the Ring on page 16

vpls-flush-on-topology-change

Syntax vpls-flush-on-topology-change;

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

Release Information Statement introduced in Junos OS Release 10.0.

Description Determine the action the bridge should take when the topology of a multihomed Layer 2 ring with MPLS infrastructure changes: flush the media access control (MAC) cache or not. By default, the bridge does not flush the cache when the topology changes.

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

Related Documentation
- VPLS Multihoming: Bridge Flush of MAC Cache on Topology Change on page 17

[edit protocols layer2-control] Hierarchy Level

The following statement hierarchy can also be included at the **[edit logical-systems *logical-system-name*]** hierarchy level.

```
protocols {
    layer2-control {
        bpdu-block {
            disable-timeout seconds;
            interface [ interface-names ];
        }
        mac-rewrite {
            interface interface-name {
                protocol {
                    cdp;
                    stp;
                    vtp;
                }
            }
        }
        nonstop-bridging;
        traceoptions {
            file filename <files number> <size maximum-file-size> <world-readable |
                no-world-readable>;
            flag flag <disable>;
        }
```

```
    }
  }
```

Related Documentation

- *Notational Conventions Used in Junos OS Configuration Hierarchies*
- *[edit protocols] Hierarchy Level*

bpdu-block

Syntax

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

Hierarchy Level [edit protocols layer2-control]

Release Information Statement introduced in Junos OS Release 9.4.

Description Enable BPDU blocking on an interface.

The remaining statements are described separately.

Required Privilege Level

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

Related Documentation

- BPDU Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 14
- Configuring BPDU Protection on Individual Interfaces on page 23

disable-timeout

Syntax disable-timeout *seconds*;

Hierarchy Level [edit protocols layer2-control bpdu-block]

Release Information Statement introduced in Junos OS Release 9.4.

Description Configure the timeout value to periodically check to see if an interface is still disabled with BPDU blocking. If this option is not configured, the interface is not periodically checked and remains disabled.

Options ***seconds***—Disable timeout value.

Range: 10 through 3600

Default: If this option is not configured, the interface is not periodically checked and remains disabled.

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

Related Documentation

- BPDU Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 14

interface (BPDU Blocking)

Syntax interface *interface-name*;

Hierarchy Level [edit protocols layer2-control bpdu-block]

Release Information Statement introduced in Junos OS Release 9.4.

Description Configure the interface to participate in BPDU blocking.

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

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

Related Documentation

- BPDU Protection for Spanning-Tree Instance Interfaces Overview on page 4
- BPDU Protection for Individual Spanning-Tree Instance Interfaces on page 14
- Configuring BPDU Protection on Individual Interfaces on page 23

interface (Layer 2 Protocol Tunneling)

Syntax

```
interface interface-name {
  protocol (cdp | stp | vtp);
}
```

Hierarchy Level [edit protocols layer2-control mac-rewrite]

Release Information Statement introduced in Junos OS Release 9.1.

Description Configure an interface for Layer 2 protocol tunneling.

The remaining statement is described separately.

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

Related Documentation

- Layer 2 Protocol Tunneling Through a Network Overview on page 7

PART 3

Administration

CHAPTER 8

Operational Mode Commands for Layer 2 Protocol Tunneling

clear error bpdu

Syntax **clear error bpdu**
<interface *interface-name*>

Release Information Command introduced in Junos OS Release 9.4.

Description (MX Series routers only) Clear a bridge protocol data unit (BPDU) error condition caused by the detection of a possible bridging loop from Spanning Tree Protocol (STP) operation.

Options **interface *interface-name***—(Optional) Clear the BPDU error condition for the specified interface.

Required Privilege Level clear

List of Sample Output clear error bpdu interface on page 54

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear error bpdu interface

```
user@host> clear error bpdu interface ge-1/1/1
```

clear error mac-rewrite

Syntax clear error mac-rewrite
<interface *interface-name*>

Release Information Command introduced in Junos OS Release 9.1.

Description (MX Series routers only) Clear a MAC rewrite error condition caused by the reception of tunneled Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunk Protocol (VTP) packets on an interface with Layer 2 protocol tunneling enabled.

Options interface *interface-name*—(Optional) Clear the MAC rewrite error condition for the specified interface.

Required Privilege Level clear

List of Sample Output clear error mac-rewrite interface on page 55

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear error mac-rewrite interface

```
user@host> clear error mac-rewrite interface ge-1/0/1
```

show bridge mac-table

Syntax

show bridge mac-table
<brief | count | detail | extensive>
<bridge-domain (all | *bridge-domain-name*)>
<global-count>
<interface *interface-name*>
<*mac-address*>
<vlan-id (all-vlan | *vlan-id*)>

Release Information

Command introduced in Junos OS Release 8.4.

Description

(MX Series routers only) Display Layer 2 MAC address information.

Options

none—Display all learned Layer 2 MAC address information.

brief | count | detail | extensive—(Optional) Display the specified level of output.

bridge-domain (all | *bridge-domain-name*)—(Optional) Display learned Layer 2 MAC addresses for all bridging domains or for the specified bridging domain.

global-count—(Optional) Display the total number of learned Layer 2 MAC addresses on the system.

instance *instance-name*—(Optional) Display learned Layer 2 MAC addresses for the specified routing instance.

interface *interface-name*—(Optional) Display learned Layer 2 MAC addresses for the specified interface.

mac-address—(Optional) Display the specified learned Layer 2 MAC address information.

vlan-id (all-vlan | *vlan-id*)—(Optional) Display learned Layer 2 MAC addresses for all VLANs or for the specified VLAN.

Additional Information

When Layer 2 protocol tunneling is enabled, the tunneling MAC address 01:00:0c:cd:cd:d0 is installed in the MAC table. When the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunk Protocol (VTP) is configured for Layer 2 protocol tunneling on an interface, the corresponding protocol MAC address is installed in the MAC table.

Required Privilege Level

view

List of Sample Output

show bridge mac-table on page 58
show bridge mac-table brief on page 58
show brief mac-table count on page 58
show bridge mac-table detail on page 58

Output Fields

Table 5 on page 57 describes the output fields for the **show bridge mac-table** command. Output fields are listed in the approximate order in which they appear.

Table 5: show bridge mac-table Output fields

Field Name	Field Description
Routing instance	Name of the routing instance.
Bridging domain	Name of the bridging domain.
MAC address	MAC address or addresses learned on a logical interface.
MAC flags	Status of MAC address learning properties for each interface: • **S**—Static MAC address is configured. • **D**—Dynamic MAC address is configured. • **SE**—MAC accounting is enabled. • **NM**—Non-configured MAC.
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.
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,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vs1
 Bridging domain : vlan100, VLAN : 100
   Learning  MAC                MAC      Logical
   VLAN      address            flags    interface
             00:00:00:19:1c:db  D        ge-11/0/3.0
             00:00:00:59:3a:2f  D        xe-10/2/0.100
```

show bridge mac-table brief

```
user@host> show bridge mac-table brief
MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vs1
 Bridging domain : vlan100, VLAN : 100
   Learning  MAC                MAC      Logical
   VLAN      address            flags    interface
             00:00:00:19:1c:db  D        ge-11/0/3.0
             00:00:00:59:3a:2f  D        xe-10/2/0.100
```

show brief 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 mac-rewrite interface

Syntax **show mac-rewrite interface**
<brief | detail>
<interface-name>

Release Information Command introduced in Junos OS Release 9.1.

Description (MX Series routers only) Display Layer 2 protocol tunneling information.

Options **brief | detail**—(Optional) Display the specified level of output.

interface *interface-name*—(Optional) Display Layer 2 protocol tunneling information for the specified interface.

Required Privilege Level view

List of Sample Output show mac-rewrite interface on page 60

Output Fields Table 6 on page 60 lists the output fields for the **show mac-rewrite interface** command. Output fields are listed in the approximate order in which they appear.

Table 6: show mac-rewrite interface Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface that has Layer 2 protocol tunneling configured on it.	**brief detail**
Protocols	Layer 2 protocols being tunneled on this interface: Cisco Discovery Protocol (**CDP**), Spanning Tree Protocol (**STP**), or VLAN Trunk Protocol (**VTP**)	**brief detail**

Sample Output

show mac-rewrite interface

```
user@host> show mac-rewrite interface
Interface       Protocols

 ge-1/0/1       STP VTP CDP
```


PART 4

Index

Index

Symbols

B

C

D

F

I

L