AOS-CX 10.14 High Availability Guide

All Switch Series

Hewlett Packard Enterprise

Published: October 2024
Version: 1

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Optane™, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

All third-party marks are property of their respective owners.

Contents

About this document 7
Applicable products 7
Latest version available online 7
Command syntax notation conventions 7
About the examples 8
Identifying switch ports and interfaces 9
Identifying modular switch components 10

High Availability 12
High Availability Overview 12
High Availability switchover behaviors 13
Management Module Failover Overview 14
High Availability switchover behaviors 15
AAA on Switches with Multiple Management Modules 16
High Availability Commands 16
redundancy switchover 16

BFD 18
BFD Features 18
Configuring BFD for an IPv4 Static Route 19
Configuring BFD for BGP 20
Configuring BFD For OSPFv2 22
Configuring BFD For OSPFv3 23
Configuring BFD for PIM Over IPv4 25
Configuring BFD for PIM Over IPv6 26
Configuring BFD for VRRP 28
BFD Commands 29
bfd 29
bfd <IPV4-ADDR> 29
bfd all-interfaces (OSPF) 30
bfd detect-multiplier 31
bfd disable 32
bfd enable (Context: config-hsc) 33
bfd disable (Context: config-hsc) 34
bfd echo disable 34
bfd echo-src-ip-address 36
bfd min-echo-receive-interval 37
bfd min-receive-interval 38
bfd min-transmit-interval 39
clear bfd statistics 40
ip ospf bfd 41
ip ospf bfd disable 42
ip route bfd 42
ipv6 ospfv3 bfd 44
ipv6 ospfv3 bfd disable 45
neighbor fall-over bfd (context: config-router) 45
show bfd 46
show bfd interface 50
show hsc 51

ERPS **53**
Limitations, Conflicts, or Exclusions 54
ERPS Commands 55
clear erps ring <RINGID> instance <ID> 55
clear erps statistics 56
erps ring 57
erps ring <RINGID> <port0|port1> interface 58
erps ring <RINGID> description 59
erps ring <RINGID> guard-interval 60
erps ring <RINGID> hold-off-interval 61
erps ring <RINGID> instance 62
erps ring <RINGID> instance <ID> control-vlan 63
erps ring <RINGID> instance <ID> description 64
erps ring <RINGID> instance <ID> enable 65
erps ring <RINGID> instance <ID> protected-vlans 66
erps ring <RINGID> instance <ID> protection-switch {{manual|force} <PORT0>|<PORT1>} 67
erps ring <RINGID> instance <ID> revertive 69
erps ring <RINGID> instance <ID> role 70
erps ring <RINGID> instance <ID> rpl 71
erps ring <RINGID> meg-level 72
erps ring <RINGID> parent-ring 73
erps ring <RINGID> sub-ring 74
erps ring <RINGID> tcn-propogation 75
erps ring <RINGID> transmission-interval 76
erps ring <RINGID> wtr-interval 77
show erps statistics 78
show erps status 80
show erps summary 82

Support and Other Resources **84**
Accessing Aruba Support 84
Accessing Updates 85
Aruba Support Portal 85
My Networking 85
Warranty Information 85
Regulatory Information 85
Documentation Feedback 86

Chapter 1
About this document

This document describes features of the AOS-CX network operating system. It is intended for administrators responsible for installing, configuring, and managing Aruba switches on a network.

Applicable products

This document applies to the following products:

- Aruba 4100i Switch Series (JL817A, JL818A)
- Aruba 6000 Switch Series (R8N85A, R8N86A, R8N87A, R8N88A, R8N89A, R9Y03A)
- Aruba 6100 Switch Series (JL675A, JL676A, JL677A, JL678A, JL679A)
- Aruba 6200 Switch Series (JL724A, JL725A, JL726A, JL727A, JL728A, R8Q67A, R8Q68A, R8Q69A, R8Q70A, R8Q71A, R8V08A, R8V09A, R8V10A, R8V11A, R8V12A, R8Q72A, JL724B, JL725B, JL726B, JL727B, JL728B, S0M81A, S0M82A, S0M83A, S0M84A, S0M85A, S0M86A, S0M87A, S0M88A, S0M89A, S0M90A, S0G13A, S0G14A, S0G15A, S0G16A, S0G17A)
- Aruba 6300 Switch Series (JL658A, JL659A, JL660A, JL661A, JL662A, JL663A, JL664A, JL665A, JL666A, JL667A, JL668A, JL762A, R8S89A, R8S90A, R8S91A, R8S92A)
- Aruba 6400 Switch Series (R0X31A, R0X38B, R0X38C, R0X39B, R0X39C, R0X40B, R0X40C, R0X41A, R0X41C, R0X42A, R0X42C, R0X43A, R0X43C, R0X44A, R0X44C, R0X45A, R0X45C, R0X26A, R0X27A, JL741A)
- Aruba 8100 Switch Series (R9W94A, R9W95A, R9W96A, R9W97A)
- Aruba 8320 Switch Series (JL479A, JL579A, JL581A)
- Aruba 8325 Switch Series (JL624A, JL625A, JL626A, JL627A)
- Aruba 8360 Switch Series (JL700A, JL701A, JL702A, JL703A, JL706A, JL707A, JL708A, JL709A, JL710A, JL711A, JL700C, JL701C, JL702C, JL703C, JL706C, JL707C, JL708C, JL709C, JL710C, JL711C, JL704C, JL705C, JL719C, JL718C, JL717C, JL720C, JL722C, JL721C)
- Aruba 8400 Switch Series (JL366A, JL363A, JL687A)
- Aruba 9300 Switch Series (R9A29A, R9A30A, R8Z96A)
- Aruba 10000 Switch Series (R8P13A, R8P14A)

Latest version available online

Updates to this document can occur after initial publication. For the latest versions of product documentation, see the links provided in Support and Other Resources.

Command syntax notation conventions

Convention	Usage
`example-text`	Identifies commands and their options and operands, code examples,

Convention	Usage
	filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets (**[ ]**).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: ■ *<example-text>* ■ <example-text> ■ *example-text* ■ *example-text*	Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: ■ For output formats where italic text cannot be displayed, variables are enclosed in angle brackets (**< >**). Substitute the text—including the enclosing angle brackets—with an actual value. ■ For output formats where italic text can be displayed, variables might or might not be enclosed in angle brackets. Substitute the text including the enclosing angle brackets, if any, with an actual value.
|	Vertical bar. A logical **OR** that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.
{ }	Braces. Indicates that at least one of the enclosed items is required.
[ ]	Brackets. Indicates that the enclosed item or items are optional.
... or . . .	Ellipsis: ■ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ■ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

About the examples

Examples in this document are representative and might not match your particular switch or environment.

The slot and port numbers in this document are for illustration only and might be unavailable on your switch.

Understanding the CLI prompts

When illustrating the prompts in the command line interface (CLI), this document uses the generic term **switch**, instead of the host name of the switch. For example:

```
switch>
```

The CLI prompt indicates the current command context. For example:

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

switch(*CONTEXT-NAME*)#

Indicates the configuration context for a feature. For example:

```
switch(config-if)#
```

Identifies the **interface** context.

Variable information in CLI prompts

In certain configuration contexts, the prompt may include variable information. For example, when in the VLAN configuration context, a VLAN number appears in the prompt:

```
switch(config-vlan-100)#
```

When referring to this context, this document uses the syntax:

```
switch(config-vlan-<VLAN-ID>)#
```

Where <*VLAN-ID*> is a variable representing the VLAN number.

Identifying switch ports and interfaces

Physical ports on the switch and their corresponding logical software interfaces are identified using the format:

member/slot/port

On the 4100i Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 on the switch.

On the 6000 and 6100 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 on the switch.

On the 6200 Switch Series

- *member*: Member number of the switch in a Virtual Switching Framework (VSF) stack. Range: 1 to 8. The primary switch is always member 1. If the switch is not a member of a VSF stack, then member is 1.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 in slot 1 on member 1.

On the 6300 Switch Series

- *member*: Member number of the switch in a Virtual Switching Framework (VSF) stack. Range: 1 to 10. The primary switch is always member 1. If the switch is not a member of a VSF stack, then member is 1.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 on member 1.

On the 6400 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Specifies physical location of a module in the switch chassis.
  - Management modules are on the front of the switch in slots 1/1 and 1/2.
  - Line modules are on the front of the switch starting in slot 1/3.
- *port*: Physical number of a port on a line module.

For example, the logical interface **1/3/4** in software is associated with physical port 4 in slot 3 on member 1.

On the 83xx, 9300, and 10000 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 on the switch.

If using breakout cables, the port designation changes to x:y, where x is the physical port and y is the lane when split to 4 x 10G or 4 x 25G. For example, the logical interface 1/1/4:2 in software is associated with lane 2 on physical port 4 in slot 1 on member 1.

On the 8400 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Specifies physical location of a module in the switch chassis.
  - Management modules are on the front of the switch in slots 1/5 and 1/6.
  - Line modules are on the front of the switch in slots 1/1 through 1/4, and 1/7 through 1/10.
- *port*: Physical number of a port on a line module

For example, the logical interface **1/1/4** in software is associated with physical port 4 in slot 1 on member 1.

Identifying modular switch components

- Power supplies are on the front of the switch behind the bezel above the management modules. Power supplies are labeled in software in the format: *member/power supply*:
  - *member*: 1.
  - *power supply*: 1 to 4.
- Fans are on the rear of the switch and are labeled in software as: *member/tray/fan*:
  - *member*: 1.
  - *tray*: 1 to 4.
  - *fan*: 1 to 4.
- Fabric modules are not labeled on the switch but are labeled in software in the format: *member/module*:

- *member*: 1.
- *member*: 1 or 2.

- The display module on the rear of the switch is not labeled with a member or slot number.

Chapter 2
High Availability

The High Availability (HA) feature has three components:

- Redundant Management
- OVSDB synchronization
- Filesystem replication

High Availability Overview

Key goals of HA include:

- Achieve five-nines (99.999%) availability of switching traffic through minimization of unplanned network outages.
- Fault tolerant: No single active component failure will cause an outage.
- Live replacement of hardware with minimal or no disruption.

Terminology:

- **MM**: Abbreviation for management module
- **MM to MM link**: Refers to the 10GbE-KR Ethernet link between two MMs
- **OVSDB**: Abbreviation for Open vSwitch Database
- **Active MM**: Management module that has control of the chassis
- **Standby MM**: Backup management module for the active management module
- **JSON-RPC**: Remote procedure call protocol encoded in JSON

Key parts of the HA feature include:

Network redundancy: Protocols and redundant network paths provide redundancy in the network, enabling traffic to continue flowing if a network link or network switch fails.

Hardware redundancy: Redundant hardware components (power supplies, fabric cards, management modules) allow continued switching traffic or system management in the event of a hardware failure or hardware maintenance. This functionality is supported through:

- Fast failover (management failover)
- Hot insert and removal (all field-replaceable hardware components)

Redundancy of specific, field-replaceable hardware components includes:

- Redundancy management (management modules), which is in charge of:
  - HA infrastructure
  - File synchronization
  - OVSDB synchronization
  - MM failover

- Standby MM configuration
- Software version update

The Active MM controls infrastructure, files, and the database. If the Active MM is removed, all management passes to the Standby MM.

- Fabric redundancy (fabric cards)
- Network interface redundancy (line cards)
- Power management (power supplies)

- **Software redundancy**: Software (including daemons) provides redundancy in software by supporting one or more of the following methods:
  - Nonstop switching restart:
    - The daemon reads its last known state or the current hardware state from OVSDB.
    - The daemon adjusts its internal state to match the last known state.
    - There is no traffic interruption and no moment in time where the last known configuration is not in effect.
    - The daemon restarts fast enough to respond to protocols that require peer communication without timing out.
    - Examples include LACP, ACLS, TCAM entries, and MSTP.
  - Graceful restart:
    - Current state is still read from OVSDB. Traffic follows the rules of this state until the protocol has fully recovered.
    - Connections to other switches are re-established.
    - Current state is republished to peers, which can then respond back with adjustments.
    - Examples include routing protocols.
  - Full state reset:
    - Any non-default runtime state the daemon has in hardware or OVSDB is forced back to the default state.
    - Any connections are closed and have to be manually restarted.
    - This is primarily for user-facing daemons and features for which the default state does not have a large impact on traffic.
    - Examples include SSH, web server, TFTP, and CLI.

High Availability switchover behaviors

The following behaviors are expected during an HA switchover event.

- The count of console login attempts is cleared (reset to 0).
- The count of login attempts for the **aaa authentication limit-login-attempts** feature is cleared (reset to 0).
- The output of the command **show authentication locked-out-userslist** is cleared of users locked out via the console.
- The output of the command **show authentication locked-out-users list** is cleared of users locked out via SSH, TELNET, or REST (as verified on an SSH channel.)

Management Module Failover Overview

There are two types of Management Module (MM) failover:

- **Controlled failover**: The user triggers this type of failover by rebooting the Active MM or running the `redundancy switchover` command.
- **Uncontrolled failover**: This type of failover is triggered by unexpected events like a crash on the Active MM or hot removal of the Active MM.

In a dual MM chassis, the Standby MM detects failover events in one of the following ways:

- A mailbox interrupt is received from the Active MM to indicate takeover. This interrupt can come for controlled or uncontrolled failover (except for a hot removal).
- Active MM hot removal detection.
- Heartbeat loss detected on the Standby MM for more than 10 seconds.

If the Active MM is not responding and is still not detected by the first two methods, it will be caught by this method.

Failover requirements:

- The Standby MM must be present to trigger a failover. An Unassigned MM will never trigger a failover.
- The Redundant Management Daemon (`hpe-rdntmgmtd`) is responsible for triggering failover from the Standby MM.
- When a failover is triggered, the Standby MM becomes the Active MM while the previously Active MM is rebooted.

Standby recovery requirements:

- The Active MM must be present to trigger a recovery.
- The Redundant Management Daemon (`hpe-rdntmgmtd`) is responsible for triggering recover from the Active MM.
- When a recovery is triggered, the Active MM reboots the nonresponsive Standby MM. This action occurs for any of the following conditions:

Condition: Heartbeat lost from Active MM:

- The failover monitor thread on the Standby MM will increment the heartbeat failed count.
- The `hpe-rdntmgmtd` daemon on the Standby MM will:
  - Detect the failover condition due to heartbeat fail count increasing past the maximum of 10 and triggering failover
  - Initiate reboot of the Active MM.
- Active MM will join as a standby after reboot.

Condition: Heartbeat lost from Standby MM:

- The recover monitor thread on the Active MM will increment the heartbeat failed count.
- The `hpe-rdntmgmtd` daemon on the Active MM will:

- Detect the recover condition due to heartbeat fail count increasing past the maximum of 7 and triggering recover.
- Initiate reboot of Standby MM.

- Standby MM will join as a standby after reboot.

Condition: Planned reboot of Active MM:

- A planned reboot on the Active MM will send a failover command to the Standby MM.
- The `hpe-rdntmgmtd` daemon on the Standby MM will:
  - Process this command and perform a failover immediately instead of waiting for the failover monitor to detect it using heartbeats.
  - Initiate reboot of the Active MM.
- Active MM will join as a standby after reboot.

Condition: Removal of Active MM:

- Removal of the Active MM from Slot 1 triggers the `hpe-rdntmgmtd` daemon on the Standby MM to initiate failover immediately instead of waiting for the failover monitor to detect it using heartbeats.
- Active MM will join as a standby after reboot.

Condition: Crash on Active MM:

- A crash on the Active MM is handled by the crash handler, which sends a failover command to the Standby MM.
- The `hpe-rdntmgmtd` daemon on the Standby MM will:
  - Process this command and perform failover immediately instead of waiting for the failover monitor to detect it using heartbeats.
  - Initiate reboot of the Active MM.
- Active MM will join as a standby after reboot.

Condition: `redundancy switchover` command:

- User executes the `redundancy switchover` command on the Active MM.
- This action will send a takeover signal to the Standby MM and reboot the Active MM.
- The `hpe-rdntmgmtd` daemon on Standby MM will process this takeover signal and perform failover immediately.
- Active MM will join as a standby after reboot.

Why did my second MM not take over after Active failed?

This action will happen if the second MM is not Standby-Ready.

The second MM must be elected as Standby and in a ready state before failover. If not, a double fault occurs and the second MM will not take over.

High Availability switchover behaviors

The following behaviors are expected during an HA switchover event:

- The count of console login attempts is cleared (reset to 0).
- The count of login attempts for the **aaa authentication limit-login-attempts** feature is cleared (reset to 0).
- The output of the command **show authentication locked-out-users list** is cleared of users locked out via the console.
- The output of the command **show authentication locked-out-users list** is cleared of users locked out via SSH, TELNET, or REST (as verified on an SSH channel.)

AAA on Switches with Multiple Management Modules

Consider the following when working with local authentication, authorization, and accounting (AAA) on switchers with multiple management modules:

- Local authentication:
  - The user database is synchronized between the Active and Standby management modules.
  - Only local users belonging to the `administrators` group and using local password authentication are permitted to log in to the Standby management module. Alternatively, the Standby management module can be accessed from the Active management module by providing a logged in admin user password.
- Local authorization:
  - A few nonconfiguration commands are available on the Standby management module.
  - For expert users, the bash shell is available on the Standby management module.
- Local accounting:
  - The audit logs used for local accounting are available only on the Active Management Module.

High Availability Commands

redundancy switchover

`redundancy switchover`

Description

Causes the switch to immediately switch over to the Standby Management Module. This command must be executed from the Active Management Module and will fail if the Standby Management Module is in a failed state or not present.

Examples

This example shows the redundancy switchover command on an active management module with a standby management module that is present.

```
switch#redundancy switchover
This command causes the switch to immediately switchover to the Standby Management
Module.
Do you want to continue [y/n]?
```

This example shows the redundancy switchover command on an active management module with a standby management module that is absent.

```
switch#redundancy switchover
Standby Management Module not found, switchover request ignored.
```

This example shows the redundancy switchover command on a standby management module.

```
switch#redundancy switchover
Redundancy switchover must be performed from the Active Management Module,
switchover request ignored.
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	Manager (#)	Administrators or local user group members with execution rights for this command.

Chapter 3
BFD

The BFD feature and thus this entire chapter is not applicable to the 6200 Switch Series.

Bidirectional Forwarding Detection (BFD) provides a general-purpose, standard, medium- and protocol-independent fast failure detection mechanism. It can detect and monitor the connectivity of links in IP to detect communication failures quickly. BFD operates independently of media, data protocols, and routing protocols.

BFD establishes a session between two network devices to detect failures on the bidirectional forwarding paths between the devices and provide services for upper-layer protocols. BFD provides no neighbor discovery mechanism. Protocols that BFD services notify BFD of devices to which it needs to establish sessions. After a session is established, if no BFD control packet is received from the peer within the negotiated BFD interval, BFD notifies a failure to the protocol, which then takes appropriate measures.

BFD operates in two modes:

- Asynchronous mode: In this mode, an operating device periodically sends BFD control packets to another device. If the other device does not receive BFD control packet from the peer within the specified interval, it tears down the BFD session.
- Demand mode: in this mode, it is assumed that an operating device has an independent way of verifying that it has connectivity to the peer. Once a BFD session is established, one device may request that the other device stops sending BFD control packets, except when the connection must be explicitly validated, in which case a short sequence of BFD control packets is exchanged. Demand mode may operate independently in each direction, or simultaneously.

BFD also has an echo function. When echo is active, an operating device periodically sends BFD echo packets. The peer device returns the received BFD echo packets back without processing them (it loops them through its forwarding path). If the sending device does not receive BFD echo packets from the peer within a specified interval, the session is considered down. Since the echo function is handling the task of detection, the rate of periodic transmission of control packets may be reduced in asynchronous mode, and eliminated in demand mode.

BFD Features

BGP, OSPFv2, OSPFv3, PIMv4 and PIMv6, static routes, and VRRP are clients of BFD.

Supported:

- BFD v1
- Asynchronous mode + echo
- IPv6 (6300, 6400, 8100, 8320, 8325, 8360, 8400, 9300, and 9300P switches only)
- Asynchronous mode on IPv6 tunnel interfaces (8400 switches only)
- Asynchronous mode for VxLAN tunnels (8325, 8360, and 8400, and 9300 switches only)
- Single hop

- IPv4
- RoP, SVI, and LAG interfaces
- VSX synchronization. For more information, see the *Virtual Switching Extension (VSX) Guide* for your switch and software version.
- Loopbacks are supported for VxLAN sessions (8325, 8360 and 8400 switches only), and static routes (6300, 6400 and 8400 switches only). Same IP version restrictions apply.

Not supported:

- MIB support
- Demand mode
- Micro-BFD
- Authentication
- Echo function on tunnel interfaces
- BFD sessions are not supported on tunnel interfaces (6300, 6400, and 8320 switches only)
- Echo function for IPv6
- Asynchronous mode on tunnel interfaces (832x and 9300 switches only)
- Multi-hop configurations. BFD works only for directly connected neighbors. BFD neighbors must be no more than one IP hop away.
- Passive and virtual link interfaces. Loopbacks are not supported on the 8320, 8325, and 8360, and 9300 switches with the exception of VXLAN sessions on 8325 and 8360 switches.
- Exceeding a maximum of 20 BFD sessions with interval values of 300ms. Spurious sessions flaps will occur when the limit of sessions is exceeded.
- Minimum intervals of 300ms are only compatible with the async_vxlan mode (BFD sessions across VxLAN) and is not user configurable.
- Setting minimum transmit time interval between 500 ms and 1000 ms, and `bfd detect-multiplier` less than 3 might result in spurious flaps.

Configuring BFD for an IPv4 Static Route

Procedure

1. Enable BFD support with the command `bfd`.
2. Enable BFD on an IPv4 static route with the command `ip route bfd`.
3. For most deployments, the default values for the following features do not need to be changed. If your deployment requires different settings, change the default values with the indicated command:

BFD setting	Default value	Command to change it
Sets the BFD detection multiplier on an interface.	5	`bfd detect-multiplier`
Sets the minimum time interval between received BFD echo packets.	500 milliseconds	`bfd min-echo-receive-interval`
Sets the minimum time	3000 milliseconds	`bfd min-transmit-interval`

BFD setting	Default value	Command to change it
interval between transmitted BFD control packets on an interface.		

Configuring the timers to be too aggressive (for example, detect-multiplier of 1) can sometimes lead to BFD session flaps depending upon traffic conditions.

4. Review BFD configuration settings with the commands `show bfd`.

Example

Enabling BFD on a static IPv4 route.

```
switch# config
switch(config)# bfd
switch# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# ip address 192.168.1.1/24
switch(config-if)# exit
switch(config)# ip route 10.0.2.0/24 20.0.0.2 bfd
```

Configuring BFD for BGP

Procedure

1. Enable BFD support with the command `bfd`.
2. Create a BGP peer and initiate a connection to it with the command `neighbor remote-as`.
3. Enable BFD on a BGP interface with the command `neighbor fall-over bfd`.
4. Define an address family and activate it with the commands `address-family` and `neighbor activate`.
5. For most deployments, the default values for the following features do not need to be changed. If your deployment requires different settings, change the default values with the indicated command:

BFD setting	Default value	Command to change it
Sets the BFD detection multiplier on an interface.	5	`bfd detect-multiplier`
Sets the minimum time interval between received BFD echo packets.	500 milliseconds	`bfd min-echo-receive-interval`
Sets the minimum time interval between transmitted BFD control packets on an interface.	3000 milliseconds	`bfd min-transmit-interval`

Configuring the timers to be too aggressive (for example, detect-multiplier of 1) can sometimes lead to BFD session flaps depending upon traffic conditions.

6. Review BFD configuration settings with the commands `show bfd`.

Example

Enabling BFD on a BGP interface.

```
switch# config
switch(config)# bfd
switch(config)# router bgp 100
switch(config-router)# neighbor 10.1.231.2 remote-as 100
switch(config-router)# neighbor 10.1.231.2 fall-over bfd
switch(config-router)# address-family ipv4-unicast
switch(config-router-ipv4-uc)# neighbor 10.1.231.2 activate
switch(config-router-ipv4-uc)# exit
switch(config-router)# exit
switch(config)# exit
switch# show ip bgp neighbors
Codes: ^ Inherited from peer-group

VRF : default
BGP Neighbor 9.0.0.1 (External)
    Description          :
    Peer-group           :

    Remote Router Id     : 0.0.0.0            Local Router Id     : (null)
    Remote AS            : 100                Local AS            : 100
    Remote Port          : 0                  Local Port          : 0
    State                : Idle               Admin Status        : Up
    Conn. Established    : 0                  Conn. Dropped       : 0
    Passive              : No                 Update-Source       :
    Cfg. Hold Time       : 180                Cfg. Keep Alive     : 60
    Neg. Hold Time       : 0                  Neg. Keep Alive     : 0
    Up/Down Time         : 00h:00m:00s        Alt. Local-AS       : 0
    Local-AS Prepend     : No
    Fall-over            : No                 BFD                 : Enabled
    Password             :
    Last Err Sent        : No Error
    Last SubErr Sent     : No Error
    Last Err Rcvd        : No Error
    Last SubErr Rcvd     : No Error

    Graceful-Restart     : Enabled            Rt. Reflect. Client: No
    Gr. Restart Time     : 120                Gr. Stalepath Time : 150
    Max. Prefix          : 0                  Send Community     :
    Allow-AS in          : 0                  Remove Private-AS  : No
    Advt. Interval       : 30                 TTL                : 255
    Soft Reconfig In     :                    Local Cluster-ID   :
    Nexthop-Self         :                    Default-Originate  :
    Weight               : 0
    TTL Security Hops    : 0

    Routemap In          :
    Routemap Out         :

  Message statistics:
                        Sent     Rcvd
                        -----    ------
    Open                   0         0
    Notification           0         0
    Updates                0         0
    Keepalives             0         0
    Route Refresh          0         0
    Total                  0         0

    Capability         Advertised      Received
```

```
-------------------------------------------
Route Refresh        No               No
Graceful Restart     No               No
Four Octet ASN       No               No
```

Configuring BFD For OSPFv2

Prerequisites

- OSPFv2 must be enabled.
- ICMP must be disabled.

Procedure

1. Enable BFD support with the command `bfd`.
2. Enable BFD on all OSPF interfaces with the command `bfd all-interfaces`, or enable BFD on a specific interface with the command `ip ospf bfd`.
3. For most deployments, the default values for the following features do not need to be changed. If your deployment requires different settings, change the default values with the indicated command:

BFD setting	Default value	Command to change it
Sets the BFD detection multiplier on an interface.	5	`bfd detect-multiplier`
Sets the minimum time interval between received BFD echo packets.	500 milliseconds	`bfd min-echo-receive-interval`
Sets the minimum time interval between transmitted BFD control packets on an interface.	3000 milliseconds	`bfd min-transmit-interval`

   Configuring the timers to be too aggressive (for example, setting a detection multiplier of 1) can sometimes lead to BFD session flaps depending upon traffic conditions.
4. Review BFD configuration settings with the commands `show bfd`.

Examples

This example shows how to enable BFD on all OSPFv2 interfaces.

```
switch# config
switch(config)# bfd
switch(config)# router ospf 1
switch(config-ospf-1)# area 1
switch(config-ospf-1)# bfd all-interfaces
switch(config-ospf-1)# exit
switch(config) router ospf 2
switch(config-ospf-2)# area 2
switch(config-ospf-2)# bfd all-interfaces
switch(config-ospf-2)# exit
```

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# ip address 192.168.1.1/24
switch(config-if)# ip ospf 1 area 1
switch(config-if)# exit
switch(config)# interface 1/1/2
switch(config-if)# no shutdown
switch(config-if)# ip address 192.168.1.2/24
switch(config-if)# ip ospf 2 area 2
switch(config-if)# exit
switch(config)# exit
switch# show bfd
Admin status : Enabled
Echo source IP : 2.2.2.2
Statistics:
Total Number of Control Packets Transmitted : 42
Total Number of Control Packets Received : 42
Total Number of Control Packets Dropped : 0
Session Interface Source IP       Destination IP  Echo     State      Application
------- --------- --------------- --------------- -------- ---------- -----------
1       1/1/1     192.168.1.1     100.100.100.101 Enabled  Up         OSPF
2       1/2/2     192.168.1.2     10.1.5.6        Enabled  Up         OSPF
```

This example shows how to enable BFD on a specific OSPFv2 interface.

```
switch# config
switch(config)# bfd
switch(config)# router ospf 1
switch(config-ospf-1)# area 1
switch(config-ospf-1)# exit
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# ip address 192.168.1.1/24
switch(config-if)# ip ospf 1 area 1
switch(config-if)# ip ospf bfd
switch(config-if)# exit
switch(config)# exit
switch# show bfd session 1
BFD Session Information - Session 1
Min Tx Interval (sec) : 10
Min Rx Interval (sec) : 10
Min Echo Rx Interval (msec) : 700
Detect Multiplier : 3
Application : OSPF
Local Discriminator : 1
Remote Discriminator : 1
Echo : Enabled
Local Diagnostic : N/A
Remote Diagnostic: N/A
Flap count: 0
Internal state: Up
Interface Source IP       Destination IP  State      Pkt In   Pkt Out  Pkt Drop
--------- --------------- --------------- ---------- -------- -------- --------
1/1/1     192.168.1.1     100.100.100.101 Up         100      101      0
```

Configuring BFD For OSPFv3

Prerequisites

- OSPFv3 must be enabled.
- ICMP must be disabled.

Procedure

1. Enable BFD support with the command `bfd`.
2. Enable BFD on all OSPF interfaces with the command `bfd all-interfaces`, or enable BFD on a specific interface with the command `ipv6 ospfv3 bfd`.
3. For most deployments, the default values for the following features do not need to be changed. If your deployment requires different settings, change the default values with the indicated command:

BFD setting	Default value	Command to change it
Sets the BFD detection multiplier on an interface.	5	`bfd detect-multiplier`
Sets the minimum time interval between received BFD echo packets.	500 milliseconds	`bfd min-echo-receive-interval`
Sets the minimum time interval between transmitted BFD control packets on an interface.	3000 milliseconds	`bfd min-transmit-interval`

   Configuring the timers to be too aggressive (for example, detect-multiplier of 1) can sometimes lead to BFD session flaps depending upon traffic conditions.
4. Review BFD configuration settings with the commands `show bfd`.

Examples

This example shows how to enable BFD on an all OSPFv3 interfaces.

```
switch# config
switch(config)# bfd
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1
switch(config-ospfv3-1)# router-id 1.1.1.1
switch(config-ospfv3-1)# bfd all-interfaces
switch(config-ospfv3-1)# exit
switch(config) router ospfv3 2
switch(config-ospfv3-2)# area 2
switch(config-ospfv3-2)# router-id 1.1.1.2
switch(config-ospfv3-2)# bfd all-interfaces
switch(config-ospfv3-2)# exit
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# ipv6 address  100::1/64
switch(config-if)# ipv6 ospfv3 1 area 1
switch(config-if)# exit
switch(config)# interface 1/1/2
switch(config-if)# no shutdown
switch(config-if)# ipv6 address  100::2/64
switch(config-if)# ipv6 ospfv3 2 area 2
switch(config-if)# exit
switch(config)# exit
```

```
switch# show bfd

Admin status: enabled
Echo source IP: 100.100.100.1
Statistics:
Total number of control packets transmitted: 20
Total number of control packets received: 17
Total number of control packets dropped: 0

Session Interface VRF     Source IP               Destination IP           Echo
 State        Application
------- --------- ------- ---------------         ---------------          -------
- ------------ ------------
1       tunnel1   default fe80::94f1:28a0:1ef:700 fe80::94f1:28a0:1ef:a100 enabled
 up           ospfv3
2       tunnel1   default fe80::94e2:37b1:1ef:111 fe80::94e2:37b1:1ef:555  enabled
 up           ospfv3
```

This example shows how to enable BFD on a specific OSPFv3 interface.

```
switch# config
switch(config)# bfd
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1
switch(config-ospfv3-1)# router-id 1.1.1.1
switch(config-ospfv3-1)# exit
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# ipv6 address  100::1/64
switch(config-if)# ipv6 ospfv3 1 area 1
switch(config-if)# ipv6 ospfv3 bfd
switch(config-if)# exit
switch(config)# exit
switch# show bfd interface 1/1/1

Admin status: enabled
Echo source IP: 100.100.100.1
Statistics:
Total number of control packets transmitted: 20
Total number of control packets received: 17
Total number of control packets dropped: 0

Session Interface VRF       Source IP               Destination IP           Echo
   State        Application
------- --------- --------- ---------------         ---------------          -----
--- ------------ ------------
1       tunnel1   default   fe80::94f1:28a0:1ef:700 fe80::94f1:28a0:1ef:a100
enabled  up           ospfv3
```

Configuring BFD for PIM Over IPv4

Prerequisites

PIM must be enabled globally and on the specific interface that will support BFD.

Procedure

1. Enable BFD support with the command `bfd`.
2. For most deployments, the default values for the following features do not need to be changed. If your deployment requires different settings, change the default values with the indicated command:

BFD setting	Default value	Command to change it
Sets the BFD detection multiplier on an interface.	5	`bfd detect-multiplier`
Sets the minimum time interval between received BFD echo packets.	500 milliseconds	`bfd min-echo-receive-interval`
Sets the minimum time interval between transmitted BFD control packets on an interface.	3000 milliseconds	`bfd min-transmit-interval`

   Configuring the timers to be too aggressive (for example, detect-multiplier of 1) can sometimes lead to BFD session flaps depending upon traffic conditions.
3. Switch to the interface on which you want to enable BFD with the command `interface`.
4. Enable BFD support with the command `ip pim-sparse bfd`.
5. Review BFD configuration settings with the commands `show bfd`.

Examples

This example shows how to configure PIM and enable BFD on interface **1/1/2**.

```
switch# config
switch(config)# bfd
switch(config)# router pim
switch(config-pim)# enable
switch(config-pim)# exit
switch(config)# interface 1/1/2
switch(config-if)# no shutdown
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)# ip pim-sparse enable
switch(config-if)# ip pim-sparse bfd
switch(config-if)# exit
switch(config)# exit
switch# show bfd
Admin status: enabled
Statistics:
Total number of control packets transmitted: 7
Total number of control packets received: 8
Total number of control packets dropped: 0
Session Interface VRF       Source IP           Destination IP         Echo
State        Application
------- --------- --------- ------------------- ---------------------- -------- --
---------- ------------
1       1/1/2     default   N/A                 10.1.1.2               enabled  up
          pim
```

Configuring BFD for PIM Over IPv6

Prerequisites

PIM must be enabled globally and on the specific interface that will support BFD.

Procedure

1. Enable BFD support with the command `bfd`.
2. For most deployments, the default values for the following features do not need to be changed. If your deployment requires different settings, change the default values with the indicated command:

BFD setting	Default value	Command to change it
Sets the BFD detection multiplier on an interface.	5	`bfd detect-multiplier`
Sets the minimum time interval between received BFD echo packets.	500 milliseconds	`bfd min-echo-receive-interval`
Sets the minimum time interval between transmitted BFD control packets on an interface.	3000 milliseconds	`bfd min-transmit-interval`

   Configuring the timers to be too aggressive (for example, detect-multiplier of 1) can sometimes lead to BFD session flaps depending upon traffic conditions.
3. Switch to the interface on which you want to enable BFD with the command `interface`.
4. Enable BFD support with the command `ip pim-sparse bfd`.
5. Review BFD configuration settings with the commands `show bfd`.

Examples

This example shows how to configure PIM and enable BFD on interface **1/1/2**.

```
switch# config
switch(config)# bfd
switch(config)# router pim6
switch(config-pim)# enable
switch(config-pim)# exit
switch(config)# interface 1/1/2
switch(config-if)# no shutdown
switch(config-if)# ipv6 address 2130::1/64
switch(config-if)# ipv6 mld enable
switch(config-if)# ip pim-sparse enable
switch(config-if)# ip pim-sparse bfd
switch(config-if)# exit
switch(config)# exit
switch# show bfd
Admin status: enabled
Echo source IP: <none>
Statistics:
Total number of control packets transmitted: 8
Total number of control packets received: 8
Total number of control packets dropped: 0
Session Interface VRF       Source IP           Destination IP                Echo
    State        Application
------- --------- --------- ------------------- ----------------------------- ----
```

```
---- ------------ ------------
1       1/1/2     default   N/A                 fe80::94f1:2821:2ef:6300
enabled  up           pimv6
```

Configuring BFD for VRRP

Procedure

1. Enable BFD support with the command `bfd`.
2. Enable BFD on a VRRP interface with the command `bfd`<*IPV4-ADDR*>.
3. For most deployments, the default values for the following features do not need to be changed. If your deployment requires different settings, change the default values with the indicated command:

BFD setting	Default value	Command to change it
Sets the BFD detection multiplier on an interface.	5	`bfd detect-multiplier`
Sets the minimum time interval between received BFD echo packets.	500 milliseconds	`bfd min-echo-receive-interval`
Sets the minimum time interval between transmitted BFD control packets on an interface.	3000 milliseconds	`bfd min-transmit-interval`

   Configuring the timers to be too aggressive (for example, detect-multiplier of 1) can sometimes lead to BFD session flaps depending upon traffic conditions.
4. Review BFD configuration settings with the commands `show bfd`.

Example

Enabling BFD on a VRRP interface.

```
switch# config
switch(config)# bfd
switch# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# ip address 192.168.1.1/24
switch(config-if)# vrrp 1 address-family ipv4
switch(config-if-vrrp)# bfd 192.158.1.2
switch(config-if-vrrp)# exit
switch# show vrrp

VRRP is enabled

Interface 1/1/1 - Group 1 - Address-Family IPv4
  State is ACTIVE
  State duration 56 mins 57.826 secs
  Virtual IP address is 10.0.0.1
  Virtual MAC address is 00:00:5e:00:01:01
  Advertisement interval is 1000 msec
```

```
Preemption enabled
Priority is 100
Active Router is 10.0.0.2 (local), priority is 100
Active Advertisement interval is 1000 msec
Active Down interval is unknown
Tracked object ID is 1, and state Down
```

BFD Commands

bfd

```
bfd
no bfd
```

Description

Enables BFD support on the switch. BFD is disabled by default.

The **no** form of this command disables BFD and removes all related configuration settings. To disable BFD, but retain configuration settings, use the command bfd disable.

Examples

Enabling BFD support:

```
switch(config)# bfd
```

Disabling BFD support and removing all configuration settings:

```
switch(config)# no bfd
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	config	Administrators or local user group members with execution rights for this command.

bfd *<IPV4-ADDR>*

```
bfd <IPV4-ADDR>
no bfd <IPV4-ADDR>
```

Description

Enables BFD under VRRP for the specified IP address. BFD is asynchronous and echo mode is supported.

The **no** form of this command disables BFD under VRRP for the specified IP address.

Parameter	Description
<IPV4-ADDR>	Specifies the address on which to enable BFD in IPv4 format (**x.x.x.x**), where **x** is a decimal number from 0 to 255.

Examples

On the 6400 Switch Series, interface identification differs.

Enabling BFD on the address **10.0.0.1** on VRRP **1**:

```
switch(config)# interface 1/1/1
switch(config-if)# routing
switch(config-if)# vrrp 1 address-family ipv4
switch(config-if-vrrp)# bfd 10.0.0.1
```

Disabling BFD on the address **10.0.0.1** on VRRP **1**:

```
switch(config)# interface 1/1/1
switch(config-if)# routing
switch(config-if)# vrrp 1 address-family ipv4
switch(config-if-vrrp)# no bfd 10.0.0.1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	config-if-vrrp	Administrators or local user group members with execution rights for this command.

bfd all-interfaces (OSPF)

```
bfd all-interfaces
```

```
no bfd all-interfaces
```

Description

Enables BFD on all OSPFv2 or OSPFv3 interfaces.

The **no** form of this command disables BFD on all active OSPFv2/OSPFv3 or IPv4/IPv6 interfaces, excluding those on which BFD was enabled at the interface level with the commands `ip ospf bfd` and `ipv6 ospfv3 bfd`.

Examples

Enabling BFD on all OSPFv2 interfaces:

```
switch(config)# router ospf 1
switch(config-ospf-1)# bfd all-interfaces
```

Disabling BFD on all OSPFv2 interfaces:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no bfd all-interfaces
```

Enabling BFD on all OSPFv3 interfaces:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# bfd all-interfaces
```

Disabling BFD on all OSPFv3 interfaces:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no bfd all-interfaces
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-ospf-<INSTANCE-TAG>` `config-ospfv3-<INSTANCE-TAG>`	Administrators or local user group members with execution rights for this command.

bfd detect-multiplier

```
bfd detect-multiplier <MULTIPLIER>
no bfd detect-multiplier <MULTIPLIER>
```

Description

Sets BFD detection multiplier on an interface.

The **no** form of this command removes the configured BFD detection multiplier.

Parameter	Description
<MULTIPLIER>	Specifies the BFD detection multiplier. Range: 1 to 5. Default: 5.

Examples

Setting the BFD detection multiplier to **3**:

```
switch(config-if)# bfd detect-multiplier 3
```

Removing the BFD detection multiplier:

```
switch(config-if)# no bfd detect-multiplier 3
```

Setting the BFD detection multiplier to the default value:

```
switch(config-if)# no bfd detect-multiplier
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	config-if	Administrators or local user group members with execution rights for this command.

bfd disable

```
bfd disable
```

Description

Disables BFD on the switch, but retains all configuration settings.

Examples

Disabling BFD:

```
switch(config)# bfd disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	config	Administrators or local user group members with execution rights for this command.

bfd enable (Context: config-hsc)

```
switch(config-hsc)# bfd enable
switch(config-hsc)# no bfd enable
```

Description

Enables or disables BFD for HSC feature.

Usage

BFD must be enabled globally to work for HSC.

Examples

Enabling BFD support for HSC:

```
switch(config)# hsc
switch(config-hsc)# bfd enable
```

Disabling BFD support for HSC:

```
switch(config)# hsc
switch(config-hsc)# no bfd enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	`config`	Administrators or local user group members with execution rights for this command.

bfd disable (Context: config-hsc)

```
switch(config-hsc)# bfd disable
```

Description

Disables BFD for HSC feature.

Example

Disabling BFD support for HSC:

```
switch(config)# hsc
switch(config-hsc)# bfd disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	`config`	Administrators or local user group members with execution rights for this command.

bfd echo disable

```
bfd echo disable
```

```
no bfd echo disable
```

Description

Disables support for BFD echo packets. Echo packet support is enabled by default.

The **no** form of this command enables support for BFD echo packets.

Toggling this feature on 8100, 8325, 8360 or 9300 switches may cause route flapping.

BFD IPv6 Echo is not supported.

Authority

Examples

On the 6400 Switch Series, interface identification differs.

Enabling BFD echo packet support on all interfaces:

```
switch(config)# no bfd echo disable
```

Disabling BFD echo packet support on all interfaces:

```
switch(config)# bfd echo disable
```

Enabling BFD echo packet support on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# bfd echo disable
```

Disabling BFD echo packet support on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no bfd echo disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325	`config` `config-if`	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8360 8400 9300 10000		

bfd echo-src-ip-address

```
bfd echo-src-ip-address <IPV4-ADDR>
no bfd echo-src-ip-address <IPV4-ADDR>
```

Description

Sets the source IPv4 address for BFD echo packets. This address is used in all echo sessions.

The source IP address must not be on the same network segment as any switch interface, otherwise a large number of ICMP redirect packets may be sent by the remote device, causing network congestion.

The **no** form of this command removes the source IPv4 address for BFD echo packets, which causes the switch to stop sending echo packets. When a valid value is set, all sessions with a peer that is capable of receiving echo packets, will start transmitting echo packets. BFD control sessions continue to run concurrently with echo packets.

Parameter	Description
<IPV4-ADDR>	Specifies an IP address in IPv4 format (**x.x.x.x**), where **x** is a decimal number from 0 to 255.

Examples

Setting the source IP address to **198.51.100.1**:

```
switch(config)# bfd echo-src-ip-address 198.51.100.1
```

Removing the source IP address **198.51.100.1**:

```
switch(config)# no bfd echo-src-ip-address 198.51.100.1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	config	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8100 8360 8400		

bfd min-echo-receive-interval

```
bfd min-echo-receive-interval <INTERVAL>
no bfd min-echo-receive-interval <INTERVAL>
```

Description

Sets the minimum time interval between received BFD echo packets.

The **no** form of this command removes the configured BFD echo packets interval. If the interval is not set, the default interval is used.

BFD IPv6 Echo is not supported.

Parameter	Description
<INTERVAL>	Specifies the minimum reception interval in milliseconds. A value of 0 means that the switch does not support reception of BFD echo packets. Range: 0, 50 to 1000. Default: 500.

Examples

Setting the minimum reception interval to **1000** milliseconds:

```
switch(config)# bfd min-echo-receive-interval 1000
```

Removing the minimum reception interval:

```
switch(config)# no bfd min-echo-receive-interval 1000
```

Setting the minimum reception interval to the default value:

```
switch(config)# no bfd min-echo-receive-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300	`config`	Administrators or local user group members with execution

Platforms	Command context	Authority
6400 8100 8320 8325 8360 8400 9300 10000		rights for this command.

bfd min-receive-interval

```
bfd min-receive-interval <INTERVAL>
no bfd min-receive-interval <INTERVAL>
```

Description

Sets the minimum time interval between received BFD control packets on an interface.

The **no** form of this command removes the configured BFD minimum interval on an interface. If the interval is not set, the default interval is used.

Parameter	Description
<INTERVAL>	Specifies the minimum receive interval in milliseconds. A value of 0 means that the switch does not support reception of BFD control packets. Range: 500 to 20000100 to 20000. Default: 3000.

Examples

Setting the minimum receive interval to **1000** milliseconds:

```
switch(config-if)# bfd min-receive-interval 1000
```

Removing the minimum receive interval:

```
switch(config-if)# no bfd min-receive-interval 1000
```

Setting the minimum receive interval to the default value:

```
switch(config-if)# no bfd min-receive-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-if`	Administrators or local user group members with execution rights for this command.

bfd min-transmit-interval

```
bfd min-transmit-interval <INTERVAL>
no bfd min-transmit-interval <INTERVAL>
```

Description

Sets the minimum time interval between transmitted BFD control packets on an interface.

The **no** form of this command removes the configured BFD minimum transmitted interval on an interface. If the interval is not set, the default interval is used.

Parameter	Description
<INTERVAL>	Specifies the minimum transmit interval in milliseconds. Range: 500 to 20000 50 to 20000 Default: 3000.

Usage

- If the minimum time interval is set between 500 ms and 1000 ms, then `bfd detect-multiplier` must be set to at least 3.
- If **bfd detect-multiplier** is set to 1, then the minimum transmit interval must be set to at least 3000 ms.
- Whenever the minimum time interval is set to a value less than 1000 ms, BFD automatically adjusts the transmission interval to 1000 ms if any of the following conditions apply:
  - The session is operating in asynchronous mode and echo is enabled.
  - The session state is in any other state than `up`.

As described in RFC 5880, this behavior occurs because BFD echo provides quick detection which allows the BFD asynchronous session to lower its traffic/resource requirements.

BFD IPv6 Echo is not supported.

Examples

Setting the minimum transmit interval to **500** ms:

```
switch(config-if)# bfd min-transmit-interval 500
```

Removing the minimum transmit interval:

```
switch(config-if)# no bfd min-transmit-interval 500
```

Setting the minimum transmit interval to the default value:

```
switch(config-if)# no bfd min-transmit-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	config-if	Administrators or local user group members with execution rights for this command.

clear bfd statistics

`clear bfd statistics [session <ID>]`

Description

Clears statistics for all BFD sessions or for a specific BFD session.

Parameter	Description
`session <ID>`	Specifies a session ID.

Examples

Clearing statistics for all BFD sessions:

```
switch# clear bfd statistics
```

Clearing statistics for BFD session 1:

```
switch# clear bfd statistics session 1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	Manager (#)	Administrators or local user group members with execution rights for this command.

ip ospf bfd

```
ip ospf bfd
no ip ospf bfd
```

Description

Enables BFD for OSPFv2 on the current interface. The interface must have OSPFv2 enabled on it. This overrides the global settings defined with the command **bfd all-interfaces**.

The **no** form of this command sets the current interface to the global settings defined with the command **bfd all-interfaces**.

Examples

On the 6400 Switch Series, interface identification differs.

Enabling BFD on interface `1/1/1`:

```
switch(config)# interface 1/1/1
switch(config-if)# ip ospf bfd
```

Disabling BFD on interface `1/1/1`:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip ospf bfd
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	config-if	Administrators or local user group members with execution rights for this command.

ip ospf bfd disable

```
ip ospf bfd disable
```

Description

Disables BFD for OSPFv2 on the current interface. This overrides the global settings defined with the command **bfd all-interfaces**.

Examples

On the 6400 Switch Series, interface identification differs.

Enabling BFD on interface `1/1/1`:

```
switch(config)# interface 1/1/1
switch(config-if)# ip ospf bfd disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	config-if	Administrators or local user group members with execution rights for this command.

ip route bfd

```
ip route <DEST-IPV4-ADDR>/<NETMASK> [<NEXT-HOP-IP-ADDR> | <INTERFACE>] [bfd]
no ip route <DEST-IPV4-ADDR>/<NETMASK> [<NEXT-HOP-IP-ADDR> | <INTERFACE>] [bfd]
```

Description

Enables or disables BFD on the specified static route. To disable BFD, issue the command without the `bfd` option.

Parameter	Description
<DEST-IPV4-ADDR>	Specifies a route destination in IPv4 format (**x.x.x.x**), where **x** is a decimal number from 0 to 255.
<NETMASK>	Specifies the number of bits in the address mask in CIDR format (**x**), where **x** is a decimal number from 0 to 128.
<NEXT-HOP-IP-ADDR>	Specifies the next hop address for reaching the destination in IPv4 format (**x.x.x.x**), where **x** is a decimal number from 0 to 255.
<INTERFACE>	Specifies the next hop as an outgoing interface.
`bfd`	Enables BFD on the static route. Omit this parameter to disable BFD.

Examples

On the 6400 Switch Series, interface identification differs.

Enabling BFD on a static route:

```
switch(config)# interface 1/1/1
switch(config-if)# ip address 20.1.1.2/24
switch(config-if)# no shutdown
switch(config-if)# routing
switch(config-if)# exit
switch(config)# ip route 192.0.0.0/8 20.1.1.1 bfd
```

Disabling BFD on a static route:

```
switch(config)# ip route 192.0.0.0/8 20.1.1.1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	`config`	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 bfd

```
ipv6 ospfv3 bfd
no ipv6 ospfv3 bfd
```

Description

Enables BFD for OSPFv3 on the current interface. The interface must have OSPFv3 enabled on it. This overrides the global settings defined with the command **bfd all-interfaces**.

The **no** form of this command sets the current interface to the global settings defined with the command **bfd all-interfaces**.

Examples

Enabling BFD:

```
switch(config-if)# ipv6 ospfv3 bfd
```

Disabling BFD:

```
switch(config-if)# no ipv6 ospfv3 bfd
```

Enabling BFD on a subinterface:

```
switch(config-subif)# ipv6 ospfv3 bfd
```

Disabling BFD on a subinterface:

```
switch(config-subif)# no ipv6 ospfv3 bfd
```

Command History

Release	Modification
10.14	Support added for the 9300 and 9300P switch series.
10.12.1000	Support added for IPv6 neighbors on the 8100, 8320, 8325, 8360, and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400	config-if	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
9300 10000		

ipv6 ospfv3 bfd disable

```
ipv6 ospfv3 bfd disable
```

Description

Disables BFD on the current OSPFv3 interface. This overrides the global settings defined with the command bfd all-interfaces.

Examples

On the 6400 Switch Series, interface identification differs.

Enabling BFD on interface `1/1/1` :

```
switch(config)# interface 1/1/1
switch(config-if)# routing
switch(config-if)# ipv6 ospfv3 bfd disable
```

Command History

Release	Modification
10.14	Support added for the 9300 and 9300P switch series.
10.12.1000	Support added for IPv6 neighbors on the 8100, 8320, 8325, 8360, and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-if`	Administrators or local user group members with execution rights for this command.

neighbor fall-over bfd (context: config-router)

```
neighbor {<IP-ADDRESS>|<PEER-GROUP-NAME>} fall-over bfd
no neighbor {<IP-ADDRESS>|<PEER-GROUP-NAME>} fall-over bfd
```

Description

Enables BGP to register with BFD to receive fast peering session deactivation messages from BFD.

The **no** form of this command disables BGP for BFD.

BFD is supported with IPv6 neighbors on the 6300, 6400, 8100, 8320, 8325, 8360, 8400, 9300, and 10000 switch series.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (**x.x.x.x**), where **x** is a decimal number from 0 to 255.
<PEER-GROUP-NAME>	Specifies a peer group.

Examples

```
switch(config-router)# neighbor 1.1.1.1 fall-over
switch(config-router)# no neighbor 1.1.1.1 fall-over bfd
```

```
switch(config-router)# neighbor PG fall-over
switch(config-router)# no neighbor PG fall-over bfd
```

Command History

Release	Modification
10.14	Support added for the 9300 and 9300P switch series.
10.12.1000	Command added for IPv6 neighbors on the 8100, 8320, 8325, 8360, and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	config-router	Administrators or local user group members with execution rights for this command.

show bfd

```
show bfd [session <ID>] [all-vrfs | vrf <NAME>] [vsx-peer]
```

Description

Shows information for all BFD sessions or for a specific BFD session.

Parameter	Description
`session <ID>`	Session ID.
`all-vrfs`	All VRFs.
`vrf <NAME>`	Specifies the name of a VRF.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

Possible values for `State` are:

- Up
- Down
- AdminDown
- Init

Possible values for **Local diagnostic** and **Remote diagnostic** are:

- Control detection time expired (1): The session has stopped receiving BFD control packets from the peer after one detection time.
- Echo function failed: The session has stopped receiving BFD Echo packets, so the session was declared Down.
- Neighbor signaled session down: A packet from the peer was received with either AdminDown or Down state.
- Forwarding plane reset: Not set in this release.
- Path down: The forwarding path when Down.
- Concatenated path down: Not set in this release.
- Administratively down: The administrator has disabled BFD.
- Reverse concatenated path down: Not set in this release.

BFD IPv6 Echo is not supported.

Examples

Showing information for all BFD sessions:

```
switch# show bfd

Admin status : Enabled
Echo source IP : 2.2.2.2
Statistics:
Total Number of Control Packets Transmitted : 42
Total Number of Control Packets Received : 42
Total Number of Control Packets Dropped : 0

Session Interface VRF       Source IP                       Destination IP
```

```
         Echo     State    Application
------- --------- --------- ------------------------------- ----------------------
--------- -------- -------- ------------
1       vlan10    blue      10.10.10.1                      10.10.10.2
         disabled up       ospf
1       vlan10    blue      N/A                             10.10.10.2
         disabled up       static_routes
2       vlan40    red       40.10.10.1                      40.10.10.2
         disabled up       ospf
3       vlan30    red       30.10.10.1                      30.10.10.2
         disabled up       ospf
4       vlan20    blue      20.10.10.1                      20.10.10.2
         disabled up       ospf
5       vlan50    black     50.10.10.1                      50.10.10.2
         disabled up       ospf
6       vlan60    black     60.10.10.1                      60.10.10.2
         disabled up       ospf
7       vlan10    blue      fe80::409:7380:a62:2400
fe80::409:7380:a49:a200         disabled up       ospfv3

Admin status : Enabled
Echo source IP : 2.2.2.2
Statistics:
Total Number of Control Packets Transmitted : 42
Total Number of Control Packets Received : 42
Total Number of Control Packets Dropped : 0

Session Interface VRF       Source IP                       Destination IP
         Echo     State    Application
------- --------- --------- ------------------------------- ----------------------
--------- -------- -------- ------------
1       vlan10    blue      10.10.10.1                      10.10.10.2
         disabled up       ospf
1       vlan10    blue      N/A                             10.10.10.2
         disabled up       static_routes
2       vlan40    red       40.10.10.1                      40.10.10.2
         disabled up       ospf
3       vlan30    red       30.10.10.1                      30.10.10.2
         disabled up       ospf
4       vlan20    blue      20.10.10.1                      20.10.10.2
         disabled up       ospf
5       vlan50    black     50.10.10.1                      50.10.10.2
         disabled up       ospf
6       vlan60    black     60.10.10.1                      60.10.10.2
         disabled up       ospf
7       vlan10    blue      fe80::409:7380:a62:2400
fe80::409:7380:a49:a200         disabled up       ospfv3
```

Showing information for BFD session 1:

```
switch# show bfd session 1
BFD Session Information – Session 1
VRF: blue
Min Tx Interval (msec) : 10000
Min Rx Interval (msec) : 10000
Min Echo Rx Interval (msec) : 700
Detect Multiplier : 3
Application : ospf
Local Discriminator : 1
Remote Discriminator : 1
Echo : Enabled
```

```
Local Diagnostic : no_diagnostic
Remote Diagnostic: administratively_down
State flaps: 0
Interface Source IP       Destination IP  State      Pkt In   Pkt Out  Pkt Drop
--------- --------------- --------------- ---------- -------- -------- --------
1/1/1     100.100.100.100 100.100.100.101 Up         100      101      0
BFD Session Information - Session 1
VRF: blue
Min Tx Interval (msec) : 10000
Min Rx Interval (msec) : 10000
Min Echo Rx Interval (msec) : 700
Detect Multiplier : 3
Application : ospf
Local Discriminator : 1
Remote Discriminator : 1
Echo : Enabled
Local Diagnostic : no_diagnostic
Remote Diagnostic: administratively_down
State flaps: 0
Interface Source IP       Destination IP  State      Pkt In   Pkt Out  Pkt Drop
--------- --------------- --------------- ---------- -------- -------- --------
1/1/1     100.100.100.100 100.100.100.101 Up         100      101      0
```

Showing information for all BFD sessions related to a particular VRF in the system:

```
switch# show bfd vrf blue

Admin status: enabled
Echo source IP: 100.1.1.1
Statistics:
Total number of control packets transmitted: 2226
Total number of control packets received: 2222
Total number of control packets dropped: 0
Session Interface VRF       Source IP                       Destination IP
         Echo     State    Application
------- --------- --------- ------------------------------- ----------------------
--------- -------- -------- ------------
1       vlan10    blue      10.10.10.1                      10.10.10.2
         disabled up       ospf
1       vlan10    blue      N/A                             10.10.10.2
         disabled up       static_routes
4       vlan20    blue      20.10.10.1                      20.10.10.2
         disabled up       ospf
7       vlan10    blue      fe80::409:7380:a62:2400
fe80::409:7380:a49:a200         disabled up       ospfv3
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	Manager (#)	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8100 8320 8325 8360 8400 9300 10000		

show bfd interface

`show bfd interface <NAME>`

Description

Shows information for all BFD sessions related to the specified interface.

Parameter	Description
`interface <NAME>`	Specifies an interface.

BFD IPv6 Echo is not supported.

Examples

Showing information for all BFD sessions related to the specified interface:

```
switch# show bfd interface vlan10

BFD session information - Session 1
Min Tx interval (msec): 3000
Min Rx interval (msec): 3000
Min echo Rx interval (msec): 500
Detect multiplier: 5
Application: ospf
Local discriminator: 13211
Remote discriminator: 13211
Echo: disabled
Local diagnostic: no_diagnostic
Remote diagnostic: no_diagnostic
State flaps: 0
Interface Source IP                                  Destination IP
       State        Pkt Rx   Pkt Tx   Pkt drop
--------- ------------------------------------- --------------------------------
------- ------------ -------- -------- --------
vlan10    10.10.10.1                             10.10.10.2
       up           453      455      0

================================================
BFD session information - Session 1
Min Tx interval (msec): 3000
Min Rx interval (msec): 3000
Min echo Rx interval (msec): 500
Detect multiplier: 5
Application: static_routes
Local discriminator: 13211
```

```
Remote discriminator: 13211
Echo: disabled
Local diagnostic: no_diagnostic
Remote diagnostic: no_diagnostic
State flaps: 0
Interface Source IP                                    Destination IP
       State        Pkt Rx   Pkt Tx   Pkt drop
--------- ---------------------------------------- --------------------------------
------- ------------ -------- -------- --------
vlan10    N/A                                      10.10.10.2
       up           453      455      0

================================================
BFD session information - Session 7
Min Tx interval (msec): 3000
Min Rx interval (msec): 3000
Min echo Rx interval (msec): 500
Detect multiplier: 5
Application: ospfv3
Local discriminator: 1402
Remote discriminator: 1402
Echo: disabled
Local diagnostic: no_diagnostic
Remote diagnostic: no_diagnostic
State flaps: 0
Interface Source IP                                    Destination IP
       State        Pkt Rx   Pkt Tx   Pkt drop
--------- ---------------------------------------- --------------------------------
------- ------------ -------- -------- --------
vlan10    fe80::409:7380:a62:2400                  fe80::409:7380:a49:a200
       up           58       58       0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show hsc

```
show hsc
```

Description

Displays connection information for the remote controller.

Example

Displaying connection information for the remote controller:

```
switch# show hsc

BFD status : Enabled

Controller IP   Port    Connection Connection
address                 status     state
--------------- ------- ---------- -------------
192.168.16.17   6640    UP         ACTIVE
192.168.16.17   6650    UP         IDLE
192.168.16.17   6660    DOWN       BACKOFF
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8100 8320 8325 8360 8400 9300 10000	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Chapter 4
ERPS

ERPS supported on the following switches:

- 4100i
- 6300
- 6400
- 8320
- 8325
- 8360
- 8400
- 9300

Ethernet Ring Protection Switching (ERPS) is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to eliminate loops at Layer 2. Because the standard number is ITU-T G.8032/Y1344, ERPS is also called G.8032. ERPS defines Ring Auto Protection Switching (RAPS) Protocol Data Units (PDUs) and protection switching mechanisms.

ERPS has two versions:

- ERPSv1 released by ITU-T in June 2008, and
- ERPSv2 released in August 2010.

EPRSv2, fully compatible with ERPSv1, provides the following enhanced functions:

- Multi-ring topologies, such as intersecting rings
- RAPS PDU transmission on non-virtual-channels (NVCs) in sub-rings
- Forced Switch (FS) and Manual Switch (MS)
- Revertive and non-revertive switching

Generally, redundant links are used on an Ethernet switching network such as a ring network to provide link backup and enhance network reliability. The use of redundant links, however, may result in creating network loops, causing broadcast storms, and rendering the MAC address table unstable. As a result, communication quality deteriorates, and communication services may even be interrupted.

Ethernet networks demand faster protection switching. STP does not meet the requirement for fast convergence.

ERPS, a standard ITU-T protocol, prevent loops on ring networks. It optimizes detection and performs fast convergence. ERPS allows all ERPS-capable devices on a ring network to communicate.

Benefits of ERPS include:

- Prevents broadcast storms and implements fast traffic switchover on a network where there are loops.

- Provides fast convergence and carrier-class reliability.
- Allows all ERPS-capable devices on a ring network to communicate.

Limitations, Conflicts, or Exclusions

- ERPS coexists with STP with the following limitations:
  - Ring ports are excluded from STP operation.

    

    It is not recommended to configure any Spanning Tree interface context-related commands on the ERPS ring port. Before configuring ring port ensure all Spanning Tree interface context-related commands are removed from the interface.

  - With VSX, STP operates on ISL ports despite being ring ports.
  - Only default MSTP instance (CIST) is supported with ERPS.
  - ERPS cannot be enabled with more than 252 RPVST instances. This limitation is applicable for all supported platforms.
- Dynamic VLANs (MVRP) are not supported on ERPS ring ports.
- MCLAG configuration on ERPS ring ports is not supported.
- ERPS and loop protect are not supported on the same port. If enabled together, the behavior is undefined.
- Active GW is not recommended on VLANs that are not part of VSX-LAGs. This can lead to two active GWs on a ring when ISL fails as SVIs of those VLANs are not shut down on VSX-secondary. This results in frequent MAC moves for gateway MAC address across ring nodes.
- On such deployments, where gateways are serving VLANs across the ring, VRRP is recommended.
- Multiple major-rings (MRs) are not supported in a VSX solution since VSX-ISL can be part of a maximum of one MR.
- Topologies must have either a subring or MCLAG to connect downstream switches and not a mix of both.
- Square VSX topology cannot be part of single MR since MCLAG is not supported as a ring port.
- On switches with both ERPS and STP enabled, a loop involving ring ports and STP ports is not protected.
- Redundant links from downstream switches to ring nodes must be VSX-LAGs.
- Do not enable loop-protect, MVRP, and MCLAG on ERPS ring ports. Enabling these features on an ERPS ring port leads to undefined behavior.
- HA limitations:
  - With UDLD, redundancy switchover is not hitless and results in traffic loss.
  - UDLD can be used only on ring nodes that are connected through repeaters. This limitation is not applicable with VSX because UDLD does not have to be enabled on ISL, and LAN traffic can reach a ring through ISL. This limitation is applicable for VSF switchover.
- Increase the guard interval to 1-2 seconds to prevent Ethernet ring nodes from acting on outdated R-APS messages and the possibility of forming a closed loop.
- Avoid using **vlan trunk allowed all** on interconnection link interfaces. Doing so causes looping of the subring R-APS packet and causes undefined behavior for all rings configured on the switch.

- Protected VLANs in a subring that are not part of a major ring are allowed to accommodate guest VLANs. Clients on those VLANs can only reach the gateway for further routing. These clients cannot reach other clients on the same VLAN. Such VLANs must have VRRP enabled gateways on both ring interconnection nodes.
- RPL neighbor configuration on the rings increases convergence time to the order of 300ms across link failures. Networks critical of convergence time carrying real-time traffic must avoid RPL neighbor configuration.
- Users must explicitly handle the dynamic change of a port from trunk to access in the following cases:
  - Defaulting a LAG interface that is part of an ERPS ring.
  - Swapping or removing an ISL link from a VSX that is part of an ERPS ring.

  These cases lead to traffic loss in the ERPS ring, so before performing any of these actions, users must consider the protocol used on the interface. If it is part of an ERPS ring, configure the port back to trunk from access.
- Enabling ip neighbor-flood on SVI interfaces is recommended for faster convergence of routed traffic.
- SNMP is not supported with ERPS.
- VLANs that have ring ports must be included in protected VLAN lists of at least one ERPS instance.

If VLANs with ring ports are not included in protected VLAN lists, the VLAN-port combination is not managed by ERPS or STP and the port state of the VLAN becomes undefined causing a loop in the network.

ERPS Commands

clear erps ring <RINGID> instance <ID>

`clear erps ring <RINGID> instance <ID>`

Description

Removes the protection switching and triggers reversion both in revertive and non-revertive operation. This command will not change the configured revertive operation mode.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239.
<ID>	Required, specifies the ID of the ring instance. Range: 1-2.

Examples

Removes the protection switching and triggers reversion for ring 3, instance 2:

```
switch# clear erps ring 3 instance 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear erps statistics

`clear erps statistics [ring <ID>] [instance <ID>]`

Description

This command clears the ERPS statistics for a ring or a ring instance.

Parameter	Description
<RINGID>	Optional, specifies the ID of the ring. Range: 1-239.
<ID>	Optional, specifies the ID of the ring instance. Range: 1-64.

Examples

Clear ERPS statistics for ring 1:

```
switch# clear erps statistics ring 1
```

Clear ERPS statistics for instance 1 of ring 1:

```
switch# clear erps statistics ring 1 instance 1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

erps ring

```
erps ring <RINGID>
no erps ring <RINGID>
```

Description

This command creates an ERPS ring with a given ID.

The `no` form of this command removes all the configurations of the ring, including instances.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239

Examples

Create an ERPS ring:

```
switch(config)# erps ring 2
switch(config-ring-2)#
```

Remove an ERPS ring:

```
switch(config)# no erps ring 2
switch(config-ring-2)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300	`config`	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
6400 8100 8320 8325 8360 8400 9300 10000		

erps ring <RINGID> <port0|port1> interface

```
erps ring <RINGID>
        <port0|port1> interface <ifname>
```

Description

This command configures the ERPS ring member port. An L2 interface in the switch is associated to one of the two member ports of an ERPS ring. In case of an interconnection node, only port0 is applicable for the sub-ring.

The `no` form of this command removes the association of the ring port to the L2 interface on the switch.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<PORT0>	Required, set port0 of the ring.
<PORT1>	Required, set port1 of the ring.
<ifname>	Required, interface name (string).

Examples

Configure the ERPS ring member port:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# port0 interface 1/1/1
```

Remove the association of the ring port to the L2 interface on the switch:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no port0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> description

```
erps ring <RINGID>
        description <LINE>
```

Description

This command adds descriptive information to help administrators and operators understand the purpose of a ring. 1-64 printable ASCII characters are allowed.

The `no` form of this command removes the ring instance description.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<LINE>	Required, specifies the description text. Maximum length is 64 characters.

Examples

Add descriptive information to a ring:

```
switch(config)# erps ring 3
switch(config-erps-ring-3) description HPE RnD ring
```

Remove descriptive information from a ring:

```
switch(config)# erps ring 3
switch(config-erps-ring-3) no description
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> guard-interval

```
erps ring <RINGID>
        guard-interval <10 milliseconds>
```

Description

Guard timer is used in nodes recovering from a local failure to avoid loops due to earlier Signal Fail (SF) messages that may be in the ring.

The configuration specifies the guard timer duration in units of 10 ms. The timer period must be greater than the maximum expected forwarding delay in which an R-APS message traverses the entire ring. The default value is 50.

The `no` form of this command removes the configured value of the guard interval and sets it to the default value of 50.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<10 milliseconds>	Required, specifies the guard timer duration in units of 10 ms. Default: 50.

Examples

Specify the guard timer duration:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)#  guard-interval 100
```

Remove the configured value of the guard interval and set it to the default value of 50:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no guard-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> hold-off-interval

```
erps ring <RINGID>
        hold-off-interval <100 milliseconds>
```

Description

Specifies hold-off interval in units of 100 ms. If specified, a defect is not reported immediately. Instead, the hold-off timer is started. On expiration of the timer, if the defect still exists, it is reported to protection switching. The default value for hold-off timer is 0.

The `no` form of this command removes the configured value of the hold-off interval and sets it to the default value of 0.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<100 milliseconds>	Required, specifies the hold-off interval in units of 100 ms. Default: 0.

Examples

Specify the hold-off interval:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# hold-off-interval 100
```

Remove the configured value of the hold-off interval and set it to the default value of 0:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no hold-off-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> instance

```
erps ring <RINGID>
        instance <ID>
```

Description

On a common ERPS network, a physical ring can be configured with a single ERPS ring, and only one blocked port can be specified in the ring. When the ERPS ring is in normal state, the blocked port prohibits all service packets from passing through. As a result, all service data is transmitted through one path over the ERPS ring, and the other link on the blocked port becomes idle, leading to ineffective use of bandwidth.

To improve link use efficiency, logical rings can be configured in the same physical ring in the ERPS multi-instance. A port may have different roles in different ERPS rings and different ERPS rings use different control VLANs.

An ERPS ring must be configured with an ERP instance, and each ERP instance specifies a range of VLANs. The topology calculated for a specific ERPS ring only takes effect in the ERPS ring. Different VLANs can use separate paths, implementing traffic load balancing and link backup.

The `no` form of this command removes the instance of the ring.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<ID>	Required, specifies the ERPS ring instance identifier. Range: 1-2.

Examples

Create a ring instance:

```
switch(config)# erps ring 3
switch(config-ring-3)# instance 2
```

Remove a ring instance:

```
switch(config)# erps ring 3
switch(config-ring-3)# no instance 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> instance <ID> control-vlan

```
erps ring <RINGID>
        instance <ID> control-vlan <VID>
```

Description

This command adds a control-channel VLAN to a ring instance. In an ERPS ring, the control VLAN should be used only to forward RAPS PDUs and not service packets. All the devices in an ERPS ring instance must be configured with the same control VLAN, and different ERPS ring instances must use different control VLANs.

The `no` form of this command removes the control-channel VLAN of the ring instance.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<ID>	Required, specifies the ERPS ring instance identifier. Range: 1-2.
<VID>	Required, VLAN ID. Range: 1-4094.

Examples

Add a control-channel VLAN to a ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) control-vlan 10
```

Remove the control-channel VLAN of the ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no control-vlan
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> instance <ID> description

```
erps ring <RINGID>
        instance <ID> description <LINE>
```

Description

This command adds descriptive information to help administrators and operators understand the purpose of a ring instance. 1-64 printable ASCII characters are allowed.

The `no` form of this command removes the ring instance description.

Command context

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<ID>	Required, specifies the ERPS ring instance identifier. Range: 1-2.
<LINE>	Required, descriptive information about the ring instance. 1-64 printable ASCII characters allowed.

Examples

Add ring instance description:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) description HPE RnD DataVlan
```

Remove ring instance description:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no description
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> instance <ID> enable

```
erps ring <RINGID>
        instance <ID> enable
```

Description

This configuration enables protection switching on the given instance of the ring. It is disabled by default.

The `no` form of this command disables protection switching on the given instance of the ring.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<ID>	Required, specifies the ERPS ring instance identifier. Range: 1-2.

Examples

Enable protection switching on the given instance of the ring:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) enable
```

Disable protection switching on the given instance of the ring:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> instance <ID> protected-vlans

```
erps ring <RINGID>
        instance <ID> protected-vlans <VID-LIST>
```

Description

This command specifies the set of VLANs that are protected by this ring instance.

The `no` form of this command removes a set of VLANs that are protected by this ring instance.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<ID>	Required, specifies the ERPS ring instance identifier. Range: 1-2.
<VID-LIST>	Required, range of VLANs to be protected by this ring instance. Range: 1-4094.

Examples

Specify a set of VLANs that are protected by this ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) protected-vlans 1,10-50
```

Remove a set of VLANs that are protected by this ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no protected-vlans 11,13
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> instance <ID> protection-switch {{manual|force} <PORT0>|<PORT1>}

`erps ring <RINGID> instance <ID> protection-switch {{manual|force} <PORT0>|<PORT1>}`

Description

Blocks a specific ring interface in one of the two following ways:

- Force: The switch blocks a specific ring interface regardless of the protection switching state of the ring instance.
- Manual: The switch blocks a specific ring interface if no other protection switch event is active on the ring instance.

The user can verify whether the protection-switch is successful by verifying the status of instance and port state over which this command is executed.

```
switch# erps ring 1 instance  1 protection-switch force port0
switch# show erps  status
Status for ERPS Ring 1 Instance 1:
==================================
Ring ID                         : 1
Instance ID                     : 1
Port0                           : 1/1/5 (Block)
Port1                           : 1/1/6 (Up)
Node Role (RPL)                 : Owner (port0)
Control VLAN                    : 50
Protected VLAN                  : 1-49
Subring (TCN)                   : No (No)
Revertive Operation             : Revertive
MEG Level                       : 7
Transmission Interval           : 5 sec
Guard Interval                  : 0 sec 500 ms
Hold-Off Interval               : 0 sec 0 ms
WTR Interval                    : 1 min
Status                          : Forced-switch
Oper Down Reason                : None
```

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<ID>	Required, specifies the ERPS ring instance identifier. Range: 1-2.
manual	A type of protection switch event in which the switch blocks a specific ring interface if no other protection switch event is active on the ring instance.
force	A type of protection switch event in which the switch blocks a specific ring interface regardless of the protection switching state of the ring instance.

Examples

Block ring 3, interface 2, port 0 if no other protection switch event is active on the ring instance:

```
switch# erps ring 3 instance 2 protection-switch manual port0
```

Block ring 3, instance 2, regardless of the protection switching state of the ring instance:

```
switch# erps ring 3 instance 2 protection-switch force port1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

erps ring <RINGID> instance <ID> revertive

`erps ring <RINGID> instance <ID> revertive`

Description

Configures the default revertive mode of operation for an ERPS ring. In revertive operation, after the conditions causing protection switching are cleared, traffic channels are restored to the recovered link blocking the RPL. This configuration is meaningful only on the RPL node.

The `no` form of this command configures non-revertive mode of operation for an ERPS ring. In non-revertive operation, the traffic channels continue to use the RPL, if it has not failed, after conditions causing protection switching are cleared. This configuration is meaningful only on the RPL node.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<ID>	Required, specifies the ERPS ring instance identifier. Range: 1-2.

Examples

Configuring the default revertive mode of operation for ERPS ring 3, instance 2:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2)# revertive
```

Configuring non-revertive mode of operation for ERPS ring 3, instance 2:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2)# no revertive
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> instance <ID> role

```
erps ring <RINGID>
        instance <ID> role <RPL-OWNER|RPL-NEIGHBOR>
```

Description

In ERPS, there is a central node called RPL Owner Node which blocks one of the ports to ensure that there is no loop formed for the Ethernet traffic. The link blocked by the RPL owner node is called the Ring Protection Link or RPL. The node at the other end of the RPL is known as RPL Neighbor Node. It uses R-APS control messages to coordinate the activities of switching on/off the RPL link.

This command specifies the role of the node as owner or neighbor.

The `no` form of this command removes the configuration of the node role from the instance.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<ID>	Required, specifies the ERPS ring instance identifier. Range: 1-2.
<RPL-OWNER>	Blocks traffic at one end of the RPL. The blocked end sends out periodic R-APS.
<RPL-NEIGHBOR>	Blocks traffic at one end of the RPL. The blocked end does not generate periodic R-APS.

Examples

Specify the role of the node as owner:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) role rpl-owner
```

Specify the role of the node as neighbor:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 3
switch(config-erps-ring-3-inst-2) role rpl-neighbour
```

Remove the configuration of the node role from the instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no role
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> instance <ID> rpl

```
erps ring <RINGID>
        instance <ID> rpl <port0|port1>
```

Description

In ERPS, there is a central node called RPL Owner Node which blocks one of the ports to ensure that there is no loop formed for the Ethernet traffic. The link blocked by the RPL owner node is called the Ring Protection Link or RPL. The node at the other end of the RPL is known as RPL Neighbor Node. It uses R-APS control messages to coordinate the activities of switching the RPL link on and off.

This command specifies which of the ERPS ring ports is the RPL.

The `no` form of this command removes the RPL port configuration from the ERPS ring instance.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<ID>	Required, specifies the ERPS ring instance identifier. Range: 1-2.

Parameter	Description
<PORT0>	Required, configure port0 to be RPL port in this ERPS ring instance.
<PORT1>	Required, configure port1 to be RPL port in this ERPS ring instance.

Examples

Configure port0 to be RPL port in this ERPS ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) role rpl-owner
switch(config-erps-ring-3-inst-2) rpl port0
```

Configure port1 to be RPL port in this ERPS ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 3
switch(config-erps-ring-3-inst-2) role rpl-neighbour
switch(config-erps-ring-3-inst-2) rpl port1
```

Remove the RPL port configuration from the ERPS ring Instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no rpl port0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> meg-level

```
erps ring <RINGID>
        meg-level <-0-7>
```

Description

The R-APS messages transmitted by ERPS take the form of OAM PDUs as defined in G.8013. Each OAM PDU is transmitted at a specified level known as the Maintenance Entity Group (MEG) level. This command configures the level with which the ERPS packets must be transmitted.

The `no` form of this command removes the configured MEG level and sets it to the default value of 7.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<0-7>	Required, specifies the meg-level. Range: 0-7. Default: 7.

Examples

Specify the meg-level:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# meg-level 4
```

Remove the configured meg-level and set it to the default value of 7:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no meg-level
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> parent-ring

```
erps ring <RINGID>
        parent-ring <RINGID>
```

Description

This command associates a sub-ring to a parent-ring and is required for the sub-ring to notify the parent-ring on change in topology.

The `no` form of this command removes the parent ring identifier.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<RINGID>	Required, specifies the ID of the parent-ring. Range: 1-239

Examples

Associate a sub-ring to a parent-ring:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)#  parent-ring 2
```

Remove a parent-ring identifier:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no parent-ring 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> sub-ring

```
erps ring <RINGID>
        sub-ring
```

Description

This command is to configure a sub-ring. If not specified, the ring is a major-ring.

The `no` form of this command removes the sub-ring configuration of the ring and configures it to be a major-ring.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239

Examples

Configure a sub-ring:

```
switch(config)# erps ring 2
switch(config-erps-ring-2)# sub-ring
```

Remove the sub-ring configuration from ring 2 and configure it to be a major-ring:

```
switch(config)# erps ring 2
switch(config-erps-ring-2)# no sub-ring
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	config-erps-ring-*<ringid>*	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> tcn-propogation

```
erps ring <RINGID>
        tcn-propogation
```

Description

This command is to configure a sub-ring interconnection node to pass a topology change notification to the ring instance for the parent ring whenever the topology of the sub-ring changes. The parent ring instance performs a Forwarding Database (FDB) flush and sends a protocol message to ensure that other nodes on the parent ring also perform an FDB flush.

The `no` form of this command disables topology change notifications.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239

<RINGID>
Required, specifies the ID of the ring. Range: 1-239

Examples

Configure topology change notifications:

```
switch(config)# erps ring 2
switch(config-erps-ring-2)# tcn-propogation
```

Disable topology change notifications:

```
switch(config)# erps ring 2
switch(config-erps-ring-2)# no tcn-propogation
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	config-erps-ring-*<ringid>*	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> transmission-interval

```
erps ring <RINGID>
        transmission-interval <SECONDS>
```

Description

Specifies the R-APS periodic transmission interval in units of seconds. Default is 5 seconds.

The no form of this command removes the configured value of the transmission interval and sets it to the default value of 5 seconds.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<SECONDS>	Required, specifies the R-APS periodic transmission interval in units of seconds. Range: 5 seconds.

Examples

Specify the R-APS periodic transmission interval as 10 seconds:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)#  transmission-interval 10
```

Remove the configured value of the transmission interval and set it to the default value of 5 seconds:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no transmission-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

erps ring <RINGID> wtr-interval

```
erps ring <RINGID>
        wtr-interval <MINUTES>
```

Description

The RPL owner node uses a delay timer before initiating an RPL block in case of both revertive mode of operation or before reverting to idle state after clearing operator commands (FS, MS).

The Wait to Restore (WTR) timer can be configured in 1-minute increments up to 12 minutes. The default value is 5 minutes. When recovering from an SF, the delay timer must be long enough to allow the recovering network to become stable. In the default revertive mode of operation, the WTR timer is used to prevent frequent operation of protection switching due to intermittent SF defects.

The `no` form of this command removes the configured value of the wtr-interval and sets it to the default value of 5 minutes.

Parameter	Description
<RINGID>	Required, specifies the ID of the ring. Range: 1-239
<MINUTES>	Required, specifies the wtr-interval in minutes. Range: 1-12. Default: 5.

Examples

Specify the wtr-interval:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# wtr-interval 7
```

Remove the configured value of the wtr-interval and set it to the default value of 5 minutes:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no wtr-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	`config-erps-ring-<ringid>`	Administrators or local user group members with execution rights for this command.

show erps statistics

`show erps statistics [ring <RINGID>] [instance <ID> [<PORT0>|<PORT1>]]`

Description

This command displays ERPS statistics. The statistics can be displayed for the ring, the instance, or the instance ports.

Parameter	Description
<RINGID>	Optional, specifies the ID of the ring. Range: 1-239.
<ID>	Optional, specifies the ID of the ring instance. Range: 1-2.
<PORT0>	Optional, specifies the ring member port 0.
<PORT1>	Optional, specifies the ring member port 1.

Examples

```
switch# show erps statistics ring 1

Statistics for ERPS ring 1 instance 1:
=======================================
                Port0                   Port1
                -----                   -----
Local Failures  4                       1

R-APS           Port0(Tx/Rx)            Port1(Tx/Rx)
-----           ------------            ------------
NR              1/1                     1/1
NR,RB           0/1                     0/1
SF              1/0                     1/0
MS              0/0                     0/10
FS              30/0                    0/0

Statistics for ERPS ring 1 instance 2:
=======================================
                Port0                   Port1
                -----                   -----
Local Failures  4                       1
R-APS           Port0(Tx/Rx)            Port1(Tx/Rx)
-----           ------------            ------------
NR              1/1                     1/1
NR,RB           0/1                     0/1
SF              1/0                     1/0
MS              0/0                     0/10
FS              30/0                    0/0
```

```
switch# show erps  statistics
Statistics for ERPS Ring 1   Instance 1  :
=========================================
                Port0                   Port1
                -----                   -----
Local Failures  4                       1
R-APS           Port0(Tx/Rx)            Port1(Tx/Rx)
-------         ----------              -----------
NR              33/9                     33/9
NR,RB           58/0                     58/0
SF              4/0                      4/0
MS              0/0                      0/0
FS              0/0                      0/0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show erps status

`show erps status [ring <RINGID>] [instance <ID>]`

Description

This command displays detailed information about a specific ring or all instances of a ring.

The ring instance may be in one of the following states:

- **Idle**: The ring instance is operational.
- **Initializing**: The ring instance is not operational.
- **Protection**: Protection switching has been triggered by a local or remote link failure.
- **Pending**: Pending clearance of a previous protection switch.
- **Down**: Ring instance is not active.
- **Manual-switch**: Manual protection switching triggered by Admin-down.
- **Force-switch**: Forced protection switching triggered by admin.

A ring instance has the following reasons for "down" state:

- **Disabled**: Ring instance is administratively disabled.
- **Inconsistent Port Config**: The same port is configured as port0 and port1 or RPL port is configured by Admin-down.
- **Incomplete Port Config**: Only one or no ring port is configured.
- **Protected VLANs Not Configured**: Protected VLAN list is empty.
- **Control VLAN Not Configured**: Control VLAN is not configured.

The ring ports can be in one of the following states:

- **Up**: Port forwards control and data traffic.
- **Blocked**: Port blocks both control and data traffic.

Parameter	Description
<RINGID>	Optional, specifies the ID of the ring. Range: 1-239.
<ID>	Optional, specifies the ID of the ring instance. Range: 1-2.

Examples

Show ERPS status for ring 1 and instance 1:

```
Status for ERPS Ring 1 Instance 1
=================================
Ring ID                          : 1
Ring description                 : ring_1
Instance ID                      : 1
Instance description             : inst_1
Port0                            : 1/0/1 (Blocked)
Port1                            : 1/0/2 (Up)
Node Role (RPL)                  : Owner (Port0)
Control VLAN                     : 100
Protected VLAN                   : None
Subring (TCN)                    : Yes (Yes)
Revertive Operation              : Revertive
MEG Level                        : 1
Transmission Interval            : 5 sec
Guard Interval                   : 500 ms
Hold-Off Interval                : 1 sec
WTR Interval                     : 5 min
Status                           : Initializing
Oper Down Reason                 : Protected Vlans Not Configured
```

Show ERPS status for ring 1:

```
switch# show erps status ring 1

Status for ERPS Ring 1 Instance 1
=================================
Ring ID                          : 1
Ring description                 : ring_1
Instance ID                      : 1
Instance description             : inst_1
Port0                            : 1/0/1 (Blocked)
Port1                            : 1/0/2 (Up)
Node Role (RPL)                  : Owner (Port0)
Control VLAN                     : 100
Protected VLAN                   : 1-10
Subring (TCN)                    : Yes (Yes)
Revertive Operation              : Non-Revertive
MEG Level                        : 1
Transmission Interval            : 5 sec
Guard Interval                   : 500 ms
Hold-Off Interval                : 1 sec
WTR Interval                     : 5 min
Status                           : Idle
Oper Down Reason                 : None


Status for ERPS Ring 1 Instance 2
=================================
```

```
Ring ID                         : 1
Ring description                : ring_1
Instance ID                     : 2
Instance description            : inst_2
Port0                           : 1/0/3 (Blocked)
Port1                           : 1/0/4 (Up)
Node Role (RPL)                 : Owner (Port0)
Control VLAN                    : 110
Protected VLAN                  : 20-30
Subring (TCN)                   : No
Revertive Operation             : Revertive
MEG Level                       : 1
Transmission Interval           : 5 sec
Guard Interval                  : 500 ms
Hold-Off Interval               : 1 sec
WTR Interval                    : 5 min
Status                          : Admin-Down
Oper Down Reason                : None
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show erps summary

```
show erps summary
```

Description

This command displays a summary of the ERPS configuration and state for the ERPS ring instances.

Examples

```
switch# show erps summary

ERPS Summary
============

Flags: R - RPL, M - Major Ring, S - Sub Ring, T - TCN Enabled
```

```
       * - RPL port

Per-Instance Summary
====================
Ring  Instance    Port0     Port1       Status         Flags
----  --------    -----     -----       ------         -----
1     1           1/1/1     *1/1/2      Pending        R,M
1     2           1/1/1     1/1/2       Idle           M
2     1           *1/1/3      -         Protection     R,S,T
2     2           1/1/3       -         Admin-down     S,T
3     1           1/1/4     1/1/5       Manual-switch  M
3     2           1/1/4     1/1/5       Force-switch   M
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6200 6300 6400 8100 8320 8325 8360 8400 9300 10000	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Chapter 5
Support and Other Resources

Accessing Aruba Support

Aruba Support Services	https://www.arubanetworks.com/support-services/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
HPE Aruba Networking Support Portal	https://networkingsupport.hpe.com/home
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-408-754-1200 (Primary - Toll Number) +1-650-385-6582 (Backup - Toll Number - Use only when all other numbers are not working)
International telephone	https://www.arubanetworks.com/support-services/contact-support/

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Other useful sites

Other websites that can be used to find information:

Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
HPE Aruba Networking	https://www.arubanetworks.com/techdocs/hardware/DocumentationPortal/Content/home.htm

Hardware Documentation and Translations Portal	
HPE Aruba Networking software	https://networkingsupport.hpe.com/downloads
Software licensing	https://lms.arubanetworks.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/
Aruba Developer Hub	https://developer.arubanetworks.com/

Accessing Updates

You can access updates from the HPE Aruba Networking Support Portal or the HPE My Networking Website.

Aruba Support Portal

https://networkingsupport.hpe.com

If you are unable to find your product in the Aruba Support Portal, you may need to search My Networking, where older networking products can be found:

My Networking

https://www.hpe.com/networking/support

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

https://support.hpe.com/portal/site/hpsc/aae/home/

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts:

https://networkingsupport.hpe./notifications/subscriptions (requires an active HPE Aruba Networking Support Portal account to manage subscriptions). Security notices are viewable without an HPE Aruba Networking Support Porta laccount.

Warranty Information

To view warranty information for your product, go to https://www.arubanetworks.com/support-services/product-warranties/.

Regulatory Information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Aruba is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements, environmental data (company programs, product recycling, energy efficiency), and safety information and compliance data, (RoHS and WEEE). For more information, see https://www.arubanetworks.com/company/about-us/environmental-citizenship/.

Documentation Feedback

Aruba is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback-switching@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.