

# Redundancy Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches

**First Published:** 2022-04-26

**Last Modified:** 2026-09-28

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2022 –2026 Cisco Systems, Inc. All rights reserved.

# Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

# Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

## Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

## Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



# CONTENTS


**Full Cisco Trademarks with Software License** iii

**Communications, services, and additional information** iv

Cisco Bug Search Tool iv

Documentation feedback iv

CHAPTER 1 **New and Changed Feature Information** 1

Added or Modified Features in Cisco IOS XE 17.18.1 1

CHAPTER 2 **Parallel Redundancy Protocol** 3

Information about PRP 3

Role of switches 5

PRP Channels 5

Mixed traffic and supervision frames 5

VLAN tags in supervision frame 6

Prerequisites 7

Guidelines and limitations 8

TrustSec on a PRP interface 9

Examples for configuring TrustSec on a PRP interface 10

CTS and PRP show commands 11

Default Settings 14

Create a PRP channel and group 14

Examples of creating a PRP channel and group 16

Verify PRP channel 16

Configure PRP channel with supervision frame VLAN tagging 17

Configuration example for VLAN tagging 19

Verify VLAN tagging 22
Add static entries to the node and VDAN tables 22
Display PRP node table and VDAN table 23
Clear all node table and VDAN table dynamic entries 24
Disable the PRP channel and group 24
Errors and warnings as syslog messages 25
Configure the PRP Logging Interval 25
Verify PRP logging interval 26
Example for creating VLANs and PRP Channels 26

CHAPTER 3 PTP over PRP 35
PTP over PRP 35
PTP over PRP packet flow 36
Configuration of PTP over PRP 38
Guidelines and limitations for PTP over PRP 38
Supported PTP profiles and clock modes 40
PRP RedBox types 40
PRP RedBox as Doubly Attached BC (DABC) with P2P 40
PRP RedBox as a Doubly Attached BC (DABC) with E2E 42
PRP RedBox as Doubly Attached TC (DATC) with P2P 44
LAN-A and LAN-B failure detection and handling 46
CLI commands for PTP over PRP 46
show ptp clock running 46
show prp channel detail 47
show prp statistics ptpPacketStatistics 47
show ptp lan port int 48
ptp clock boundary domain 48
Feature history for PTP over PRP 49

CHAPTER 4 Resilient Ethernet Protocol 51
Feature history for Resilient Ethernet Protocol 51
Resilient Ethernet Protocol 52
REP segments 52
REP open segment 52

REP ring segment 53
Edge no-neighbor ports 53
Link integrity detection 54
Fast convergence 55
VLAN load balancing 55
Spanning tree interaction 57
Resilient Ethernet Protocol (REP) Negotiated (Deprecated) 57
REP ports 58
Resilient Ethernet Protocol Fast 59
Configure REP Fast 59
REP Zero Touch Provisioning technologies 61
Day 0 processes 61
REP ZTP features 64
REP segment ID auto-discovery 65
REP segment ID auto-discovery deployment 65
REP segment ID auto-discovery limitations 66
REP segments 67
Default REP configurations 67
Guidelines and limitations for REP configuration 68
Guidelines for REP ZTP configuration 70
Configure the REP administrative VLAN 70
Configure a REP interface 71
Manually trigger VLAN load balancing on a segment 74
Configure SNMP Traps for REP 74
Configure REP ZTP 75
Configure REP segment ID auto-discovery 76
Preventive best practices 77
Monitoring REP configurations 78
Check the REP ZTP status 80
PTP over REP 82
Guidelines for PTP over REP 83
PTP clock types profiles and their accuracy 83
Configure PTP over REP 85
Configure REP 85

Configure PTP over REP using power profile 86
Configure PTP over REP using default profile 88

CHAPTER 5 FlexLink+ 91
FlexLink+ redundancy functions 91
Guidelines and restrictions 92
Configure active port for Flex Link+ 92
Configure standby port for FlexLink+ 93
Configure VLAN load balancing on FlexLink+ 94
Configure time for VLAN load balancing on FlexLink+ 95
Configure manual preemption for VLAN load balancing on FlexLink+ 95
Configure FlexLink+ topology change messages 96

CHAPTER 6 Media Redundancy Protocol 97
Media Redundancy Protocol 97
MRP modes 98
MRP roles and states 99
Guidelines and limitations of MRP 101
Guidelines and limitations to MRA 103
Guidelines and limitations to PROFINET MRP mode 103
MRP features in IE9300 stacks 104
Precision Time Protocol over MRP 104
Configure PTP over MRP 105
Configure the PROFINET MRP 106
Prerequisites to MRP CLI mode configuration 109
MRP CLI configuration parameters 110
Configure the Switch as MRA in MRP CLI mode 110
Configure the ring ports and modes for MRP 112
Configuration examples for MRP CLI mode 112
Examples of configuration verification commands and outputs 113
Media Redundancy Client 115
MRC mode functionality 115
Configure MRC 115

CHAPTER 7 **High-availability Seamless Redundancy** 117

Feature History 117

High-availability Seamless Redundancy 117

Loop avoidance mechanisms 119

HSR RedBox operation modes 120

HSR SAN mode in RedBox ring topology 121

CDP and LLDP for HSR 121

HSR alarms 121

PTP over HSR 123

Supported PTP profiles and modes 123

Operating HSR RedBox as Doubly Attached BC (DABC) with P2P 124

Configure HSR RedBox as DABC with P2P 125

HSR RedBox as Doubly Attached TC (DATC) with P2P 128

Configure HSR RedBox as DATC with P2P 128

HSR Uplink Redundancy Enhancement 129

Guidelines for configuring HSR on IE9300 Series switches 132

Default settings 136

Configure an HSR ring 137

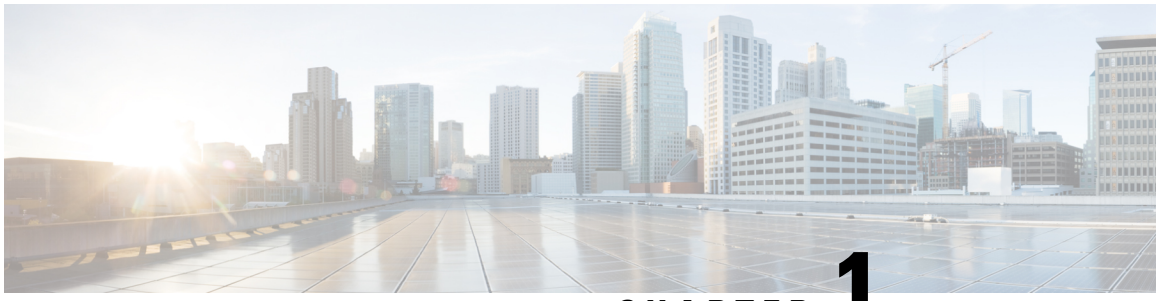
Enable HSR alarms 139

Clear all node table and VDAN table dynamic entries 139

HSR verification commands 140

Configuration examples 143

Related documents for the IE9300 Series 147



CHAPTER 1

# New and Changed Feature Information

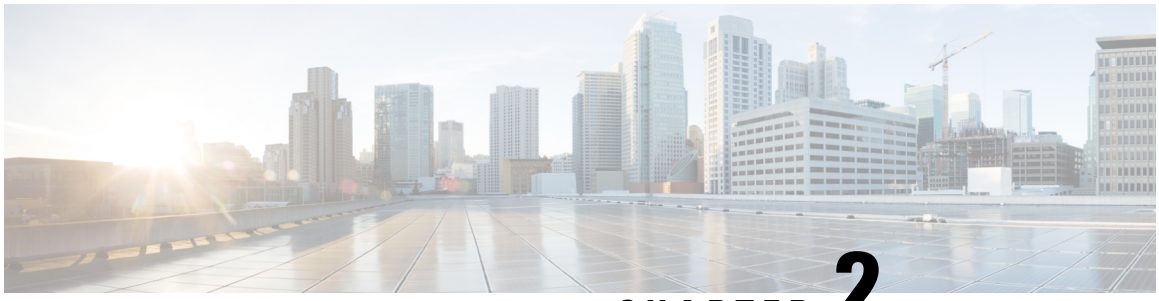

- Added or Modified Features in Cisco IOS XE 17.18.1, on page 1


# Added or Modified Features in Cisco IOS XE 17.18.1

This table summarizes the new and changed feature information for the Redundancy Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches, and tells you where they are documented.

***Table 1: Added or Modified Features***

| Feature | Description | Where documented |
|---|---|---|
| Enhanced ring convergence profiles for standalone IE9300 switches | This feature was introduced. | Media Redundancy Protocol |
| PTP over MRP | This feature was introduced. | Precision Time Protocol over MRP, on page 104 |



CHAPTER 2

# Parallel Redundancy Protocol


- Information about PRP, on page 3
- Prerequisites, on page 7
- Guidelines and limitations, on page 8
- TrustSec on a PRP interface, on page 9
- Default Settings, on page 14
- Create a PRP channel and group, on page 14
- Configure PRP channel with supervision frame VLAN tagging, on page 17
- Add static entries to the node and VDAN tables, on page 22
- Clear all node table and VDAN table dynamic entries, on page 24
- Disable the PRP channel and group, on page 24
- Errors and warnings as syslog messages , on page 25
- Example for creating VLANs and PRP Channels, on page 26


# Information about PRP

Parallel Redundancy Protocol (PRP) is defined in the International Standard IEC 62439-3. PRP provides redundancy in Ethernet networks, enabling recovery to occur instantly after failures.

PRP is supported on several Cisco Catalyst IE9300 Rugged Series Switches .

- IE-9320-26S2C-E and IE-9320-26S2C-A beginning with Cisco IOS XE Cupertino Release 17.7.1.
- IE-9320-22S2C4X-E and IE-9320-22S2C4X-A beginning with Cisco IOS XE Dublin Release 17.12.1.
- IE-9310-16P8S4X-E and IE-9310-16P8S4X-A beginning with Cisco IOS XE 17.18.1 onwards.

### Traditional redundancy vs. PRP

To recover from network failures, redundancy can be provided by network elements connected in mesh or ring topologies using protocols like RSTP, REP, or MRP, where a network failure causes some reconfiguration in the network to allow traffic to flow again (typically by opening a blocked port). Network recovery and resumption of traffic with these redundancy schemes can take from a few milliseconds to several seconds.

PRP uses a different scheme. The end nodes implement redundancy by connecting two network interfaces to two independent, parallel networks, LAN-A and LAN-B. Each of these Dually Attached Nodes (DANs) then have redundant paths to all other DANs in the network.

### How PRP works with dually attached nodes (DANs)

The DAN sends two packets simultaneously through its two network interfaces to the destination node. Each frame includes a redundancy control trailer (RCT) with a sequence number. This addition helps the destination node distinguish between duplicate packets. When the destination DAN receives the first packet successfully, it removes the RCT and consumes the packet. If the second packet arrives successfully, it is discarded. If a failure occurs in one of the paths, traffic continues to flow over the other path uninterrupted, and recovery occurs instantly.

### Singly attached nodes (SANs)

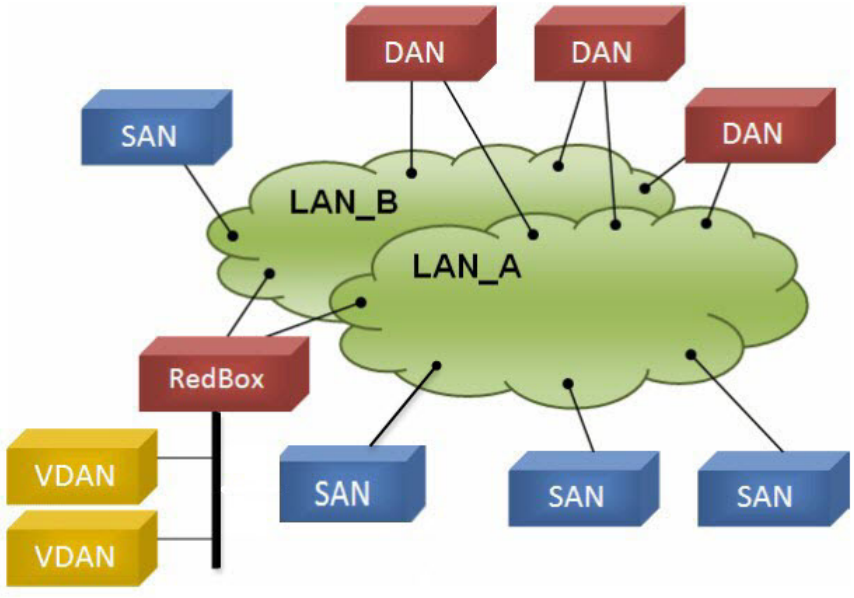
Non-redundant endpoints in the network that attach only to either LAN-A or LAN-B are known as Singly Attached Nodes (SANs).

### Redundancy box (RedBox) and virtual DAN (VDAN)

A Redundancy Box (RedBox) is used when an end node that does not have two network ports and does not implement PRP needs to implement redundancy. Such an end node can connect to a RedBox, which provides connectivity to the two different networks on behalf of the device. Because a node behind a RedBox appears for other nodes like a DAN, it is called a Virtual DAN (VDAN). The RedBox itself is a DAN and acts as a proxy for the VDANs it represents.

The image here shows a PRP redundant network.

***Figure 1: PRP Redundant Network***



### Supervision frames

Supervision frames are special types of frames used for monitoring and maintaining the integrity of redundant networks. To manage redundancy and check the presence of other DANs, a DAN periodically sends Supervision frames and can evaluate the Supervision frames sent by other DANs.

# Role of switches

IE-9320-26S2C-A, IE-9320-26S2C-E, IE-9320-22S2C4X-A, IE-9320-22S2C4X-E, IE-9310-16P8S4X-E, and IE-9310-16P8S4X-A switches implement RedBox functionality using Gigabit Ethernet port connections to each of the two LANs.

# PRP Channels

A PRP channel, also called a channel group, aggregates two Gigabit Ethernet interfaces—either access, trunk, or routed—into a single logical link. In a channel group, the Gigabit Ethernet member port with the lower number is the primary port and connects to LAN-A. The port with the higher number functions is the secondary port and connects to LAN-B.

At least one member port must remain up and send traffic for the PRP channel to operate. If both member ports are down, the channel is also down. Each switch supports a maximum of two PRP channel groups.

The interfaces available for each group on each switch series are fixed. The tables in this section show the specific interfaces.

***Table 2: Supported interfaces for PRP channel***

| Switch Model | PRP Channel Number | LAN-A Interfaces | LAN-B Interfaces |
|---|---|---|---|
| IE-9320-26S2C-A, IE-9320-26S2C-E, IE-9320-22S2C4X-A, IE-9320-22S2C4X-E | Channel 1 | Gi1/0/21 | Gi1/0/22 |
| | Channel 2 | Gi1/0/23 | Gi1/0/24 |
| IE-9310-16P8S4X-E, IE-9310-16P8S4X-A | Channel 1 | Gi1/0/1 or Gi1/0/9 | Gi1/0/2 or Gi1/0/10 |
| | Channel 2 | Gi1/0/3 or Gi1/0/11 | Gi1/0/4 or Gi1/0/12 |

# Mixed traffic and supervision frames

Traffic egressing the RedBox PRP channel group can be mixed, meaning that it is destined to either SANs (connected only on either LAN-A or LAN-B) or DANs. To prevent duplication of packets for SANs, the switch learns source MAC addresses in two ways: from received supervision frames for DAN entries, and from non-PRP (regular traffic) frames for SAN entries, maintaining these addresses in the node table. When forwarding packets out the PRP channel to SAN MAC addresses, the switch looks up the entry to determine the appropriate LAN and prevents packet duplication.

A RedBox with VDANs must send supervision frames on behalf of those VDANs. When traffic arrives on all other ports and exits through PRP channel ports, the switch learns source MAC addresses, adds them to the VDAN table, and begins sending supervision frames for these addresses. Learned VDAN entries are subject to aging.

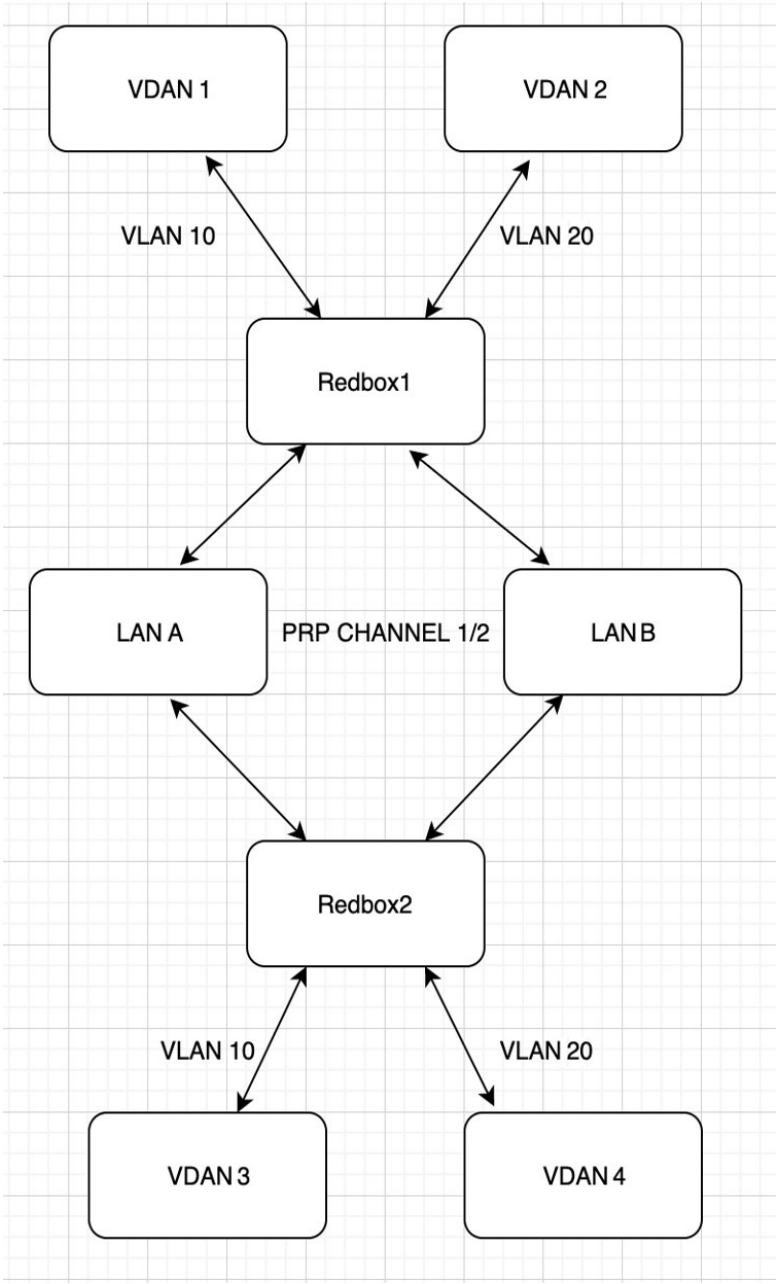
# VLAN tags in supervision frame

Cisco Catalyst IE9300 Rugged Series Switches support VLAN tagging for supervision frames. PRP VLAN tagging requires that PRP interfaces be configured in trunk mode. This feature allows you to specify a VLAN ID in the supervision frames for a PRP channel.

### Example: Configuring PRP channel with supervision frame VLAN tagging

In the example configuration diagram below, PRP channel 1 interface is configured in trunk mode with allowed VLANs 10 and 20. Supervision frames are tagged with VLAN ID 10. RedBox1 sends Supervision frames on behalf of VDANs with the PRP VLAN ID, but the regular traffic from VDANs goes over the PRP channel based on the PRP trunk VLAN configuration.

*Figure 2: Configuring PRP Channel with Supervision Frame VLAN Tagging*




See Configure PRP channel with supervision frame VLAN tagging, on page 17 for configuration information.

# Prerequisites

These prerequisites are applicable for setting up PRP.

- You must have a IE-9310-16P8S4X-E, IE-9310-16P8S4X-A, IE-9320-26S2C-A , IE-9320-26S2C-E , IE-9320-22S2C4X-A , or IE-9320-22S2C4X-E switch.

- Network Essentials license is sufficient for PRP. However, if you plan to run TrustSec over PRP, the Network Advantage license is required.

# Guidelines and limitations

Review these guidelines and limitations before you configure PRP.

### Feature availability and support limitations

- PRP or HSR is not supported when devices are stacked.
- Load-balancing is not supported.
- PRP traffic load cannot exceed 90 percent bandwidth of the Gigabit Ethernet interface channels.

### Commands and operational monitoring guidelines

- For PRP statistics, use the show interface prp-channel [ 1 | 2 ] command. Physical interface show commands, such as show interface gi1/0/21, do not provide PRP statistics information.
- PRP functionality can be managed using the CIP protocol. These CIP commands for PRP are available:
  - show cip object prp <0-2>
  - show cip object nodetable <0-2>
- The Protocol status displays incorrectly for the Layer type = L3 section when you enter the show prp channel detail command. Refer to the Ports in the group section of the output for the correct Protocol status.
- When an individual PRP interface goes down, show interface status continues to show a status of UP for the link. This is because the port status is controlled by the PRP module. Use the show prp channel command to confirm the status of the links, which will indicate if a link is down.

### Interface configuration guidelines

- A PRP channel must have two active ports that are configured within a channel to remain active and maintain redundancy.
- Each interface within a channel group must have the same configuration.
- For Layer 3, you must configure the IP address on the PRP channel interface.
- To configure supervision frame VLAN tagging, you must configure interfaces in trunk mode.

  You cannot configure access mode on PRP interfaces when supervision frame VLAN tag configuration exists. If you attempt to configure access mode on a PRP interface with supervision frame VLAN tagging, the following message is displayed:

  ```
  %PRP_MSG-4-PRP_VLANTAG: Warning: Do not configure access mode for PRP interfaces with
  tagged supervision frames.
  ```

### Hardware and physical interface limitations

- On Cisco Catalyst IE9300 Rugged Series Switches, use `Gi1/0/23` or `Gi1/0/24` for PRP — `shutdown` is not permitted if the port is in PRP-channel group.
- UDLD must be disabled on interfaces where PRP is enabled. This is particularly important if the interfaces have media-type SFP.
- PRP DANs and RedBoxes add a 6-byte PRP trailer to the packet. Therefore, PRP packets can be dropped by some switches with a maximum transmission unit (MTU) size of 1500. To ensure that all packets can flow through the PRP network, increase the MTU size for switches within the PRP LAN-A and LAN-B network to 1506. Use this command:

  ```
  system mtu 1506
  ```

### Spanning tree protocol (STP) guidelines

- The spanning-tree bpdufilter enable command is required on the prp-channel interface. Spanning-tree BPDU filter drops all ingress/egress BPDU traffic. This command is required to create independent spanning-tree domains (zones) in the network.
- The spanning-tree portfast edge trunk command is optional on the prp-channel interface but highly recommended. It improves the spanning-tree convergence time in PRP LAN-A and LAN-B.

### Node and VDAN table limitations

- The switch supports up to 512 (SAN+DANP) entries in the node table.
- You can configure up to 16 static Node or VDAN entries.
- Hash collisions can limit the number of MAC addresses. If the node table is out of resources for learning a MAC address from a node, the switch will default to treating that node as a DAN.
- After reload, before any MAC address is learned, the switch temporarily treats the unlearned node as a DAN. It duplicates egress packets until an ingress packet or supervision frame is received from the node, which populates an entry in the node table.
- The switch supports up to 512 VDAN entries in the VDAN table. If the VDAN table is full, the switch cannot send supervision frames for new VDANS.

# TrustSec on a PRP interface

You can configure Cisco TrustSec (CTS) on member interfaces of a PRP channel. This feature is supported on IE-9320-26S2C-A, IE-9320-26S2C-E, IE-9320-22S2C4X-A, IE-9320-22S2C4X-E, IE-9310-16P8S4X-E and IE-9310-16P8S4X-A switches only.

Because TrustSec is supported only on physical interfaces, you cannot configure TrustSec on the logical PRP channel interface. A PRP channel includes two interfaces, for example, Gi1/0/21 and Gi1/0/22. To configure TrustSec on interfaces that are members of a PRP channel, ensure that

- you have a Network Advantage license.
- you configure TrustSec on each interface first, before it is part of the PRP channel.

- both PRP channel interfaces have identical TrustSec configuration. This allows inline tagging and propagation with LAN-A and LAN-B.

**Note** CTS plus Security Association Protocol (SAP) and CTS plus MACsec Key Agreement (MKA) methods are not supported over PRP interface.

# Examples for configuring TrustSec on a PRP interface

This section provides examples for configuring TrustSec on a PRP interface. You can configure the PRP channel interfaces by configuring each individual interface or by using the **interface range** <>.

### Configuring TrustSec on each interface

The following example shows configuring TrustSec on each interface, one at a time, and then making that individual interface part of a PRP channel.

```
switch#configure terminal
switch(config)#int gi1/0/21
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 30
switch(config-if)#cts manual
switch(config-if-cts-manual)#policy static sgt 1000 trusted
switch(config-if-cts-manual)#exit
switch(config-if)#prp-channel-group 1
Creating a PRP-channel interface PRP-channel 1

switch(config-if)#
switch(config-if)#int gi1/0/22
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 30
switch(config-if)#cts manual
switch(config-if-cts-manual)#policy static sgt 1000 trusted
switch(config-if-cts-manual)#exit
switch(config-if)#prp-channel-group 1
switch(config-if)#end
```

### Configuring TrustSec on a range of interfaces

The following example shows configuring TrustSec on a range of interfaces and then making the interfaces part of a PRP channel.

```
switch#configure terminal
switch(config-if)#int range gi1/0/21-1/0/22
switch(config-if)#switchport mode access switch
switch(config-if)#switchport access vlan 30
switch(config-if)#cts manual
switch(config-if-cts-manual)#policy static sgt 1000 trusted
switch(config-if-cts-manual)#exit
switch(config-if)#prp-channel-group 1
Creating a PRP-channel interface PRP-channel 1
```

### Configuring TrustSec when interface is a member of a PRP channel

The configuration in the following example is invalid because the interface is configured as a member of a PRP channel before the attempt to configure TrustSec.

```
switch#configure terminal
switch(config)#int gi1/0/21
switch(config-if)#prp-channel-group 1
Creating a PRP-channel interface PRP-channel 1

switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 30
switch(config-if)#cts manual
Interface is a member of a port channel. To change CTS first remove from port channel.
switch(config-if)#
```

# CTS and PRP show commands

This section provides sample outputs for the **show** commands that you can use when configuring TrustSec on PRP member interfaces.

### show cts interface summary

```
switch#show cts interface summary
CTS Interfaces
----------------------
Interface                      Mode    IFC-state dot1x-role peer-id    IFC-cache
Critical-Authentication
-------------------------------------------------------------------------------
Gi1/0/21                       MANUAL  OPEN      unknown    unknown    invalid  Invalid
Gi1/0/22                       MANUAL  OPEN      unknown    unknown    invalid  Invalid
R1#show cts pacs
AID: 51F577DCE176855650F2F5609418AC6
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: 51F577DC7E176855650F2F5609418AC6
  I-ID: petra3400ipv4
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 09:06:08 UTC Wed Nov 01 2023
PAC-Opaque:
000200B800030001000400105 1F577DC7E176855650F2F5609418AC60006009C000301002BBB79441FEE97B0E0B339B9036F9C710000001364C8D
1A000093A8054BC5FA1780A24E23B60A4BFF46AF47A317EB20391BFCA6F0CAABA7F66393F05799A3B0EAB602B54749DCF7225A45FDDB1349A81977D857B9C3
1959A2B54CFC4505CD903D84394E69E5795D31543BB575FB8D51A6FA021FB5E6A0C296F8CA21318377688073516714125D38973D9BF2A66792E3AD1C0A05C3
E739CA1
Refresh timer is set for 12w4d
R1#show cts interface GigabitEthernet1/0/21
Global Dot1x feature is Disabled
Interface GigabitEthernet1/0/21:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Interface Active for 00:03:25.772
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    SUCCEEDED
        Peer SGT:            30
        Peer SGT assignment: Trusted
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Enabled
    Cache Info:
        Expiration            : N/A
```

```
        Cache applied to link : NONE
    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0
    L3 IPM:   disabled.
```

### show cts role-based counters

```
switch# show cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor
HW-Monitor
*       *       0          0          0          0          0          0
122     0       0          0          0          0          0          0
200     0       0          0          0          2845       0          0
201     130     0          0          0          0          0          0
130     200     0          0          0          2845       0          0
```

### show prp channel detail

```
switch#show prp channel 1 summary
Flags:  D - down        P - bundled in prp-channel
        R - Layer3      S - Layer2
        U - in use
Number of channel-groups in use: 1
Group  PRP-channel   Ports
------+-------------+-----------------------------------------
1      PR1(SU)       Gi1/0/21(P), Gi1/0/22(P)
R1#show prp channel 1 detail
PRP-channel: PR1
------------
 Layer type = L2
 Ports: 2 Maxports = 2
 Port state = prp-channel is Inuse
 Protocol = Enabled
Ports in the group:
  1) Port: Gi1/0/21
   Logical slot/port = 1/1 Port state = Inuse
 Protocol = Enabled
  2) Port: Gi1/0/22
   Logical slot/port = 1/2 Port state = Inuse
 Protocol = Enabled
```

### show prp statistics ingressPacketStatistics

```
switch#sh prp statistics ingressPacketStatistics
 PRP prp_maxchannel 2 INGRESS STATS:
 PRP channel-group 1 INGRESS STATS:
   ingress pkt lan a: 1010
   ingress pkt lan b: 1038
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 20
```

```
   ingress danp pkt dscrd: 20
   ingress supfrm rcv a: 382
   ingress supfrm rcv b: 390
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt a: 0
   ingress pri over pkt b: 0
   ingress oversize pkt a: 0
   ingress oversize pkt b: 0
   ingress byte lan a: 85127
   ingress byte lan b: 85289
   ingress wrong lan id a: 402
   ingress wrong lan id b: 402
   ingress warning lan a: 1
   ingress warning lan b: 1
   ingress warning count lan a: 137
   ingress warning count lan b: 137
   ingress unique count a: 0
   ingress unique count b: 0
   ingress duplicate count a: 20
   ingress duplicate count b: 20
   ingress multiple count a: 0
   ingress multiple count b: 0
PRP channel-group 2 INGRESS STATS:
   ingress pkt lan a: 0
   ingress pkt lan b: 0
   ingress crc lan a: 0
   ingress crc lan b: 0
   ingress danp pkt acpt: 0
   ingress danp pkt dscrd: 0
   ingress supfrm rcv a: 0
   ingress supfrm rcv b: 0
   ingress over pkt a: 0
   ingress over pkt b: 0
   ingress pri over pkt a: 0
   ingress pri over pkt b: 0
   ingress oversize pkt a: 0
   ingress oversize pkt b: 0
   ingress byte lan a: 0
   ingress byte lan b: 0
   ingress wrong lan id a: 0
   ingress wrong lan id b: 0
   ingress warning lan a: 0
   ingress warning lan b: 0
   ingress warning count lan a: 0
   ingress warning count lan b: 0
   ingress unique count a: 0
   ingress unique count b: 0
   ingress duplicate count a: 0
   ingress duplicate count b: 0
   ingress multiple count a: 0
   ingress multiple count b: 0
```

### show prp statistics egressPacketStatistics

```
switch#sh prp statistics egressPacketStatistics
 PRP channel-group 1 EGRESS STATS:
   duplicate packet: 20
   supervision frame sent: 427
   packet sent on lan a: 934
   packet sent on lan b: 955
   byte sent on lan a: 96596
   byte sent on lan b: 96306
   egress packet receive from switch: 517
```

```
  overrun pkt: 0
  overrun pkt drop: 0
PRP channel-group 2 EGRESS STATS:
  duplicate packet: 0
  supervision frame sent: 0
  packet sent on lan a: 0
  packet sent on lan b: 0
  byte sent on lan a: 0
  byte sent on lan b: 0
  egress packet receive from switch: 0
  overrun pkt: 0
  overrun pkt drop: 0
```

# Default Settings

By default, no PRP channel exists on the switch until you create it. Interfaces that can be configured for PRP are fixed, as described in PRP Channels, on page 5 .

# Create a PRP channel and group

To create and enable a PRP channel and group on the switch, follow these steps.

**Before you begin**

- Review the specific interfaces supported for each switch type, described in PRP Channels, on page 5.
- Review the Prerequisites, on page 7 and Guidelines and limitations, on page 8.
- Ensure that the member interfaces of a PRP channel are not participating in any redundancy protocols such as FlexLinks, EtherChannel, or REP, before creating a PRP channel.

**Procedure**

**Step 1** Use the **interface range GigabitEthernet***interface range/channel group* command to assign two Gigabit Ethernet interfaces to the PRP channel group.

- For channel 1, enter:

  **interface range GigabitEthernet1** *interface range/channel group*

- For channel 2, enter:

  **interface range GigabitEthernet2***interface range/channel group*

**Example:**

```
switch(config)#interface range GigabitEthernet1/0/21-22
switch(config)#interface range GigabitEthernet1/0/23-24
```

Use the **no interface prp-channel 1 | 2** command to disable PRP on the defined interfaces and shut down the interfaces.

**Note**

You must apply the Gi1/0/21 interface before the Gi1/0/22 interface. We recommend using the **interface range** command. Similarly, you must apply the Gi1/0/23 interface before the Gi1/0/24 for PRP channel 2.

**Step 2** Perform these optional steps, as required.

| Option | Description |
|---|---|
| Configure a switch port | Use the **switchport** command for Layer 2 traffic.<br>`switch(config)#switchport`<br>Use the **no switchport** command for Layer 3 traffic.<br>`switch(config)#no switchport` |
| Set a nontrunking, nontagged single VLAN Layer 2 (access) interface | Use the **switchport mode access** command.<br>`switch(config)#switchport mode access` |
| Create a VLAN for the Gigabit Ethernet interfaces | Use the **switchport access vlan** < *value* > command.<br>`switch(config-if)#switchport access vlan 2`<br>**Note**<br>This step is required only for Layer 2 traffic. |
| Disable Precision Time Protocol (PTP) on the switch | Use the **no ptp enable** command.<br>`switch(config)#no ptp enable`<br>PTP is enabled by default. You can disable it if you do not need to run PTP. |

**Step 3** Use the **no keepalive** command to disable loop detection for the redundancy channel.

**Step 4** Use the **udld port disable** command to disable UDLD for the redundancy channel.

**Step 5** Use the **prp-channel-group** *prp-channel group* command to enter subinterface mode and create a PRP channel group.

Value of *prp-channel group*: 1 or 2

**Example:**

```
switch(config)#prp-channel-group 2
```

The two interfaces that you assigned in step 1 are assigned to this channel group.

The **no** form of this command is not supported.

**Step 6** Use the **no shutdown** command to bring up the PRP channel.

**Step 7** Use the **interface prp-channel** *prp-channel-number* command to specify the PRP interface and enter interface mode.

Value of *prp-channel-number*: 1 or 2

**Example:**

```
switch(config)#interface prp-channel1
```

**Step 8** Use the **spanning-tree bpdufilter enable** command to configure bpdufilter on the prp-channel interface.

The spanning-tree BPDU filter drops all ingress and egress BPDU traffic. This command is required to create independent spanning-tree domains (zones) in the network.

**Step 9** (Optional) Use the **spanning-tree portfast edge trunk** command to configure LAN-A/B ports to quickly get to FORWARD mode.

This command is optional but highly recommended. It improves the spanning-tree convergence time on PRP RedBoxes and LAN-A and LAN-B switch edge ports. It is also highly recommended to configure this command on the LAN_A/LAN_B ports that are directly connected to a RedBox PRP interface.

# Examples of creating a PRP channel and group

This section shows examples of creating a PRP channel and group.

This example shows how to create a PRP channel, create a PRP channel group, and assign two ports to that group.

```
switch# configure terminal
switch(config)# interface range GigabitEthernet1/0/21-22
switch(config-if)# no keepalive
switch(config-if)# udld port disable
switch(config-if)# prp-channel-group 1
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface prp-channel 1
switch(config)# spanning-tree bpdufilter enable
```

```
switch# configure terminal
switch(config)# interface range GigabitEthernet1/0/21-22
switch(config-if)# switchport
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 2
switch(config-if)# no ptp enable
switch(config-if)# no keepalive
switch(config-if)# udld port disable
switch(config-if)# prp-channel-group 1
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface prp-channel 1
switch(config)# spanning-tree bpdufilter enable
```

This example shows how to create a PRP channel on a switch configured with Layer 3.

```
switch# configure terminal
switch(config)# interface range GigabitEthernet1/0/21-22
switch(config-if)# no switchport
switch(config-if)# no ptp enable
switch(config-if)# no keepalive
switch(config-if)# udld port disable
switch(config-if)# prp-channel-group 1
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface prp-channel 1
switch(config)# spanning-tree bpdufilter enable
switch(config)# ip address 192.0.0.2 255.255.255.0
```

# Verify PRP channel

Use the **show prp channel** command to verify that the PRP channel is created.

This example shows the output when one of the interfaces in the PRP channel is down.

```
show prp channel 2 detail
PRP-channel: PR2
------------
Layer type = L2
Ports: 2 Maxports = 2
Port state = prp-channel is Inuse
Protocol = Enabled
Ports in the group:
1) Port: Gi1/0/23
Logical slot/port = 1/0/23 Port state = Inuse
Protocol = Enabled
2) Port: Gi1/0/24
Logical slot/port = 1/0/24 Port state = Not-Inuse (link down)
Protocol = Enabled
```

# Configure PRP channel with supervision frame VLAN tagging

**Before you begin**

- Review the specific interfaces supported for each switch type, as described in PRP Channels, on page 5.
- Review the Prerequisites, on page 7 and Guidelines and limitations, on page 8.
- Ensure that the member interfaces of a PRP channel are not participating in any redundancy protocols such as FlexLinks, EtherChannel, REP, and so on before creating a PRP channel.

To create and enable a PRP channel and group on the switch with VLAN-tagged supervision frames, follow these steps:

**Procedure**

**Step 1** Use the **interface range GigabitEthernet***interface range/channel group* command to assign two Gigabit Ethernet interfaces to the PRP channel group.

- For channel 1, enter:

  **interface range GigabitEthernet1** *interface range/channel group*

- For channel 2, enter:

  **interface range GigabitEthernet2***interface range/channel group*

**Example:**

```
switch(config)#interface range GigabitEthernet1/0/21-22
switch(config)#interface range GigabitEthernet1/0/23-24
```

Use the **no interface prp-channel 1 | 2** command to disable PRP on the defined interfaces and shut down the interfaces.

**Note**
You must apply the Gi1/0/21 interface before the Gi1/0/22 interface. We recommend using the **interface range** command. Similarly, you must apply the Gi1/0/23 interface before the Gi1/0/24 for PRP channel 2.

**Step 2** Use the **switchport mode trunk** command to configure the PRP interface for trunk administrative mode, to allow the interface to carry traffic for more than one VLAN.

**Step 3** Use the **switchport trunk allowed vlan** *value* command to specify the allowed VLANS for the trunk interface.

**Example:**

```
switch(config)# switchport trunk allowed vlan 10
```

*value*: Allowed VLAN number from 0 to 4095 or list of VLANs separated by commas.

**Step 4** (Optional) Use the **no ptp enable** command to disable Precision Time Protocol (PTP) on the switch.

PTP is enabled by default. You can disable it if you do not need to run PTP.

**Step 5** Use the **no keepalive** command to disable loop detection for the redundancy channel.

**Step 6** Use the **udld port disable** command to disable UDLD for the redundancy channel.

**Step 7** Use the **prp-channel-group** *prp-channel group* command to enter subinterface mode and create a PRP channel group.

Value of *prp-channel group*: 1 or 2

**Example:**

```
switch(config)#prp-channel-group 2
```

The two interfaces that you assigned in step 2 are assigned to this channel group.

The **no** form of this command is not supported.

**Step 8** Use the **no shutdown** command to bring up the PRP channel.

**Step 9** Use the **interface prp-channel** *prp-channel-number* command to specify the PRP interface and enter interface mode.

Value of *prp-channel-number*: 1 or 2

**Example:**

```
switch(config)#interface prp-channel 1
```

**Step 10** Use the **spanning-tree bpdufilter enable** command to configure bpdufilter on the prp-channel interface.

The spanning-tree BPDU filter drops all ingress and egress BPDU traffic. This command is required to create independent spanning-tree domains (zones) in the network.

**Step 11** Use the **prp channel-group** *prp-channel-number* **supervisionFrameOption vlan-id** *value* command to set the VLAN ID to be used in VLAN tags for supervision frames.

*prp-channel-number*: 1 or 2

*value*:VLAN number from 0 to 4095

**Step 12** (Optional) Use the **prp channel-group** *prp-channel-number* **supervisionFrameOption vlan-cos** *value* command to configure the Class of Service (COS) value to be set in the VLAN tag of the Supervision frame.

*prp-channel-number*: 1 or 2

*value*: Range is 1 to 7. The default is 1.

**Step 13** Use the **prp channel-group** *prp-channel-number* **supervisionFrameOption vlan-tagged** *value* command to enable VLAN tagging on the interface.

*prp-channel-number*: 1 or 2

**Step 14** (Optional) Use the **spanning-tree portfast edge trunk** command to configure LAN-A/B ports to quickly get to FORWARD mode.

This command is optional but highly recommended. It improves the spanning-tree convergence time on PRP RedBoxes and LAN-A and LAN-B switch edge ports. It is also highly recommended to configure this command on the LAN_A/LAN_B ports directly connected to a RedBox PRP interface.

# Configuration example for VLAN tagging

This example shows the configuration of a switch with PRP channel interfaces configured for VLAN tagging of supervision frames.

```
PRP_IE9300#sh running-config
Building configuration...

Current configuration : 8171 bytes
!
! Last configuration change at 05:19:31 PST Mon Mar 22 2021
!
version 17.5
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service call-home
no platform punt-keepalive disable-kernel-core
no platform punt-keepalive settings
no platform bridge-security all
!
hostname PRP_IE9300
!
!
no logging console
enable password Cisco123
!
no aaa new-model
clock timezone PST -8 0
rep bpduleak
ptp mode e2etransparent
!
!
!
!
!
!
!
ip dhcp pool webuidhcp
   cip instance 1
!
!
!
login on-success log
!
!
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint TP-self-signed-559094202
 enrollment selfsigned
```

```
 subject-name cn=IOS-Self-Signed-Certificate-559094202
 revocation-check none
 rsakeypair TP-self-signed-559094202
!
!
!
diagnostic bootup level minimal
!
!
!
spanning-tree mode rapid-pvst
no spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
memory free low-watermark processor 89983
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
prp channel-group 1 supervisionFrameOption vlan-tagged
prp channel-group 1 supervisionFrameOption vlan-id 30
prp channel-group 1 supervisionFrameTime 500
prp channel-group 1 supervisionFrameLifeCheckInterval 24907
prp channel-group 1 supervisionFrameRedboxMacaddress ecce.13eb.71a2
prp channel-group 2 supervisionFrameOption vlan-tagged
prp channel-group 2 supervisionFrameOption vlan-id 40
prp channel-group 2 supervisionFrameTime 0
prp channel-group 2 supervisionFrameLifeCheckInterval 0
prp channel-group 2 supervisionFrameRedboxMacaddress f8b7.e2e5.c1f9
!
!
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
lldp run
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface PRP-channel1
 switchport mode trunk
 switchport trunk allowed vlan 30,40

 spanning-tree bpdufilter enable
!
interface PRP-channel2
 switchport mode trunk
 switchport trunk allowed vlan 30,40
 no keepalive
 spanning-tree bpdufilter enable
!
```

```
interface GigabitEthernet1/0/21
 switchport mode trunk
 switchport trunk allowed vlan 30,40
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/22
 switchport mode trunk
 switchport trunk allowed vlan 30,40
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable
!
interface AppGigabitEthernet1/1
!
interface GigabitEthernet1/0/23
 switchport mode trunk
 switchport trunk allowed vlan 30,40
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/24
 switchport mode trunk
 switchport trunk allowed vlan 30,40
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan30
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
 ip address 40.40.40.1 255.255.255.0
!
interface Vlan197
 ip address 9.4.197.30 255.255.255.0
!
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
ip tftp source-interface Vlan197
ip tftp blocksize 8192
!
!
!
!
!
!
```

```
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login
 transport input ssh
line vty 5 15
 login
 transport input ssh
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
 address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
!
!
!
!
!
!
!
!
!
!
!
end

PRP_IE9300#
```

# Verify VLAN tagging

Use the **show prp control supervisionFrameoption** command to verify successful VLAN tagging configuration.

```
REDBOX1#
show prp control supervisionFrameoption
PRP channel-group 1 Super Frame Option
COS value is 7
CFI value is 0
VLAN value is 1
MacDA value is 200
VLAN id value is 30
```

# Add static entries to the node and VDAN tables

Follow the steps in this section to add a static entry to the node or VDAN table.

**Procedure**

**Step 1** Use the **prp channel-group** *prp-channel group* **nodeTableMacaddress** *mac-address* {dan | lan-a | lan-b} command to specify the MAC address to add to the node table for the channel group and specify whether the node is a DAN or a SAN (attached to either LAN-A or LAN-B).

- *prp-channel group*: 1 or 2
- *mac-address*: MAC address of the node

**Example:**

```
switch(config-if)#prp channel-group 1 nodeTableMacaddress 0000.0000.0001 lan-a
```

**Note**
Use the **no** form of the command to remove the entry.

**Step 2** Use the **prp channel-group** *prp-channel group* **vdanTableMacaddress** *mac-address* command to specify the MAC address to add to the VDAN table:

- *prp-channel group*: 1 or 2
- *mac-address*: MAC address of the node or VDAN

**Example:**

```
switch(config-if)#prp channel-group 1 vdanTableMacaddress 0000.0000.0001
```

**Note**
Use the **no** form of the command to remove the entry.

# Display PRP node table and VDAN table

Use the **show prp node-table** and **show prp vdan-table** to display the entries in the PRP node table and VDAN table

This example shows how to display the PRP node table and PRP VDAN table.

```
Switch#
show prp node-table
PRP Channel 1 Node Table
==================================
Mac Address Type Dyn TTL
---------------- ----- --- -------
B0AA.7786.6781 lan-a Y 59
F454.3317.DC91 dan Y 60
==================================
Channel 1 Total Entries: 2
Switch#
show prp vdan-table
PRP Channel 1 VDAN Table
============================
Mac Address Dyn TTL
---------------- --- -------
```

```
F44E.05B4.9C81 Y 60
============================
Channel 1 Total Entries: 1
```

# Clear all node table and VDAN table dynamic entries

Follow the steps in this section to clear all node table and VDAN table dynamic entries.

### Procedure

**Step 1** Use the **clear prp node-table** [ **channel-group** *group*] command to clear all dynamic entries in the node table.

**Example:**

```
switch(config)# clear prp node-table [channel-group 1]
```

**Step 2** Use the **clear prp vdan-table** [ **channel-group** **group**] command to clear all dynamic entries in the VDAN table.

**Example:**

```
switch(config)# clear prp vdan-table [channel-group 1]
```

If you do not specify a channel group, the dynamic entries are cleared for all PRP channel groups.

**Note**
The **clear prp node-table** and **clear prp vdan-table** commands clear only dynamic entries. To clear static entries, use the **no** form of the **nodeTableMacaddress** or **vdanTableMacaddress** commands as shown in Add static entries to the node and VDAN tables, on page 22.

# Disable the PRP channel and group

Follow the steps in this section to disable the PRP channel and group.

### Procedure

**Step 1** USe the **configure terminal** command to enter global configuration mode.

**Step 2** Use the **no interface prp-channel** *prp-channel-number*command to disable the PRP channel.

*prp-channel-number*: 1 or 2

**Example:**

```
switch(config)# no interface prp-channel 2
```

# Errors and warnings as syslog messages

You can configure IE-9320-26S2C-A , IE-9320-26S2C-E , IE-9320-22S2C4X-A , and IE-9320-22S2C4X-E switches to convert errors and warnings into syslog messages. This helps to convert the syslogs into Simple Network Management Protocol (SNMP) traps for proper alerting and maintenance.

You can configure these errors and warnings to be converted into syslog messages:

- Wrong LAN ID A

  The number of frames with a wrong LAN identifier received on port A.

- Wrong LAN ID B

  The number of frames with a wrong LAN identifier received on port B.

- Warning LAN A

  There is a potential problem with the PRP ports for LAN A. (Packet loss condition/Wrong LAN packet counter incremented)

- Warning LAN B

  There is a potential problem with the PRP ports for LAN B. (Packet loss condition/Wrong LAN packet counter incremented)

- Oversize packet A
- Oversize packet B

You can configure the interval at which the syslog messages are generated. See the section Configure the PRP Logging Interval, on page 25 for more information.

# Configure the PRP Logging Interval

Complete the following steps to configure a logging interval for the creation of PRP syslogs from errors and warnings.

The default value is 300 seconds; however, you can choose a value from 60 seconds to 84,400 seconds.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode,

**Step 2** Use the **prp logging-interval** *interval in seconds* command to set the logging interval.

**Example:**

```
switch(config)# prp logging-interval 120
```

To use the default interval of 300 seconds, do not enter a value. Enter a value only to specify a logging interval different from the 300-second default.

The switch generates syslogs from the PRP errors and warnings listed in the section Errors and warnings as syslog messages , on page 25 .

This text shows sample output after configuring the logging interval.

```
*Sep 28 13:18:27.623: %PRP_WRONG_LAN-5-WRONG_LAN: PRP channel 2, LAN A is connected to LAN
 B on its peer
*Sep 28 13:18:27.623: %PRP_WRONG_LAN-5-WRONG_LAN: PRP channel 2, LAN B is connected to LAN
 A on its peer
*Sep 28 13:18:27.623: %PRP_WARN_LAN-5-WARN_LAN: PRP channel 2, PRP LAN warning is set on
LAN B
*Sep 28 13:18:27.623: %PRP_OVERSIZE_PKT-5-OVERSIZE_LAN: PRP channel 2, PRP oversize packet
 warning is set on LAN A
```

## Verify PRP logging interval

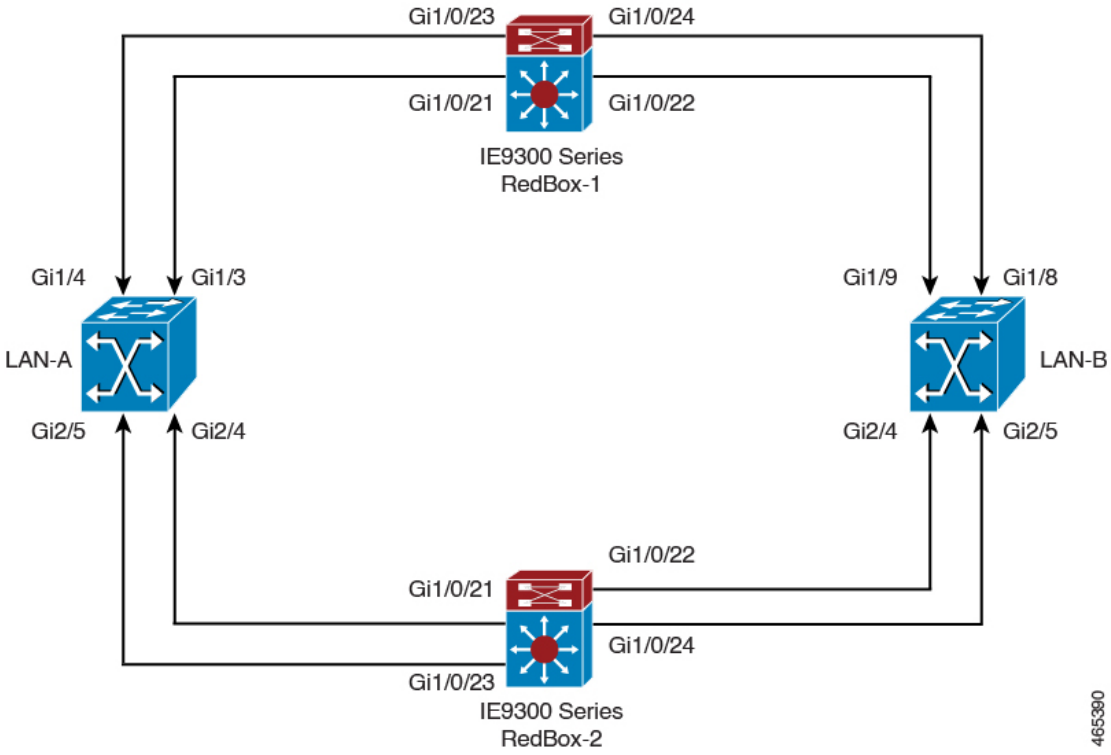
Use the **prp logging-interval** command to verify that the PRP logging interval is successfully configured.

```
switch(config)#prp logging-interval 600
PRP syslog logging interval is 600 in seconds
switch(config)#
```

# Example for creating VLANs and PRP Channels

In this example, the configuration establishes two LANs, LAN-A and LAN-B, and two PRP channels. Within the topology, a Cisco Catalyst IE9300 Rugged Series Switch is identified as RedBox-1 and another Cisco Catalyst IE9300 Rugged Series Switch is identified as RedBox-2.

This diagram shows a network configuration in which the Cisco Catalyst IE9300 Rugged Series Switches might operate. The commands in this example highlight the configuration of features and switches to support that configuration.




Following is the configuration for LAN-A:

```
diagnostic bootup level minimal
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 88589
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
!
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
interface GigabitEthernet1/3
 switchport access vlan 35
 switchport mode access
!
interface GigabitEthernet1/4
 switchport access vlan 25
 switchport mode access
!
interface GigabitEthernet1/5
 shutdown
!
interface GigabitEthernet1/6
 shutdown
!
interface GigabitEthernet1/7
 shutdown
!
interface GigabitEthernet1/8
 shutdown
!
interface GigabitEthernet1/9
 shutdown
!
interface GigabitEthernet1/10
 shutdown
!
interface AppGigabitEthernet1/1
!
interface GigabitEthernet2/1
 shutdown
!
interface GigabitEthernet2/2
 shutdown
!
interface GigabitEthernet2/3
 shutdown
!
interface GigabitEthernet2/4
 switchport access vlan 35
 switchport mode access
!
interface GigabitEthernet2/5
 switchport access vlan 25
 switchport mode access
!
interface GigabitEthernet2/6
 shutdown
!
interface GigabitEthernet2/7
 shutdown
!
interface GigabitEthernet2/8
 shutdown
!
interface Vlan1
```

```
 no ip address
 shutdown
!
interface Vlan35
 no ip address
!
interface Vlan25
 no ip address
```

The configuration for LAN-B is shown below:

```
diagnostic bootup level minimal
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 88589
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
!
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
interface GigabitEthernet1/3
 shutdown
!
interface GigabitEthernet1/4
 shutdown
!
interface GigabitEthernet1/5
 shutdown
!
interface GigabitEthernet1/6
 shutdown
!
interface GigabitEthernet1/7
 shutdown
```

```
!
interface GigabitEthernet1/8
 switchport access vlan 25
 switchport mode access
!
interface GigabitEthernet1/9
 switchport access vlan 35
 switchport mode access
!
interface GigabitEthernet1/10
 shutdown
!
interface AppGigabitEthernet1/1
!
interface GigabitEthernet2/1
 shutdown
!
interface GigabitEthernet2/2
 shutdown
!
interface GigabitEthernet2/3
 shutdown
!
interface GigabitEthernet2/4
 switchport access vlan 35
 switchport mode access
!
interface GigabitEthernet2/5
 switchport access vlan 25
 switchport mode access
!
interface GigabitEthernet2/6
 shutdown
!
interface GigabitEthernet2/7
 shutdown
!
interface GigabitEthernet2/8
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan35
 no ip address
!
interface Vlan25
 no ip address
```

Following is the configuration for RedBox-1:

```
!
!
spanning-tree mode rapid-pvst
no spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
memory free low-watermark processor 88589
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
```

```
prp channel-group 1 supervisionFrameOption vlan-id 35
prp channel-group 1 supervisionFrameTime 25000
prp channel-group 1 supervisionFrameLifeCheckInterval 8500
prp channel-group 1 supervisionFrameRedboxMacaddress 34c0.f9e5.59ba
prp channel-group 2 supervisionFrameOption vlan-id 25
prp channel-group 2 supervisionFrameTime 9834
prp channel-group 2 supervisionFrameLifeCheckInterval 12345
prp channel-group 2 passRCT!
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
!
!
interface PRP-channel1
 switchport access vlan 35
 switchport mode access
 spanning-tree bpdufilter enable
!
interface PRP-channel2
 switchport access vlan 25
 switchport mode access
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/21
 switchport access vlan 35
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/22
 switchport access vlan 35
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
!
interface GigabitEthernet1/0/23
 switchport access vlan 25
 switchport modeaccess
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/24
 switchport access vlan 25
```

```
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan35
 ip address 35.35.35.1 255.255.255.0
!
interface Vlan25
 ip address 25.25.25.1 255.255.255.0
!
interface Vlan100
 ip address 15.15.15.149 255.255.255.0
!
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
ip tftp source-interface Vlan100
ip tftp blocksize 8192
!
```

Following is the configuration for RedBox-2:

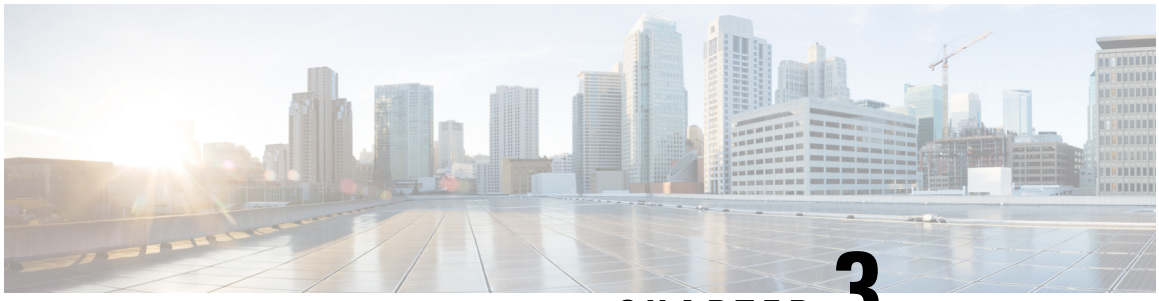
```
!
spanning-tree mode rapid-pvst
no spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
memory free low-watermark processor 88589
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
prp channel-group 1 supervisionFrameOption vlan-id 35
prp channel-group 1 supervisionFrameTime 776
prp channel-group 1 supervisionFrameLifeCheckInterval 15000
prp channel-group 1 passRCT
prp channel-group 2 supervisionFrameOption vlan-id 25
prp channel-group 2 supervisionFrameTime 9834
prp channel-group 2 supervisionFrameLifeCheckInterval 12345
prp channel-group 2 passRCT

!
!
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
lldp run
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
interface PRP-channel1
 switchport access vlan 35
 switchport mode access
 spanning-tree bpdufilter enable
!
interface PRP-channel2
 switchport access vlan 25
 switchport mode access
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/21
 switchport access vlan 35
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/22
 switchport access vlan 35
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/23
 description *** PRP 2 channel *****
 switchport access vlan 25
 switchport mode access
 no ptp enable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/24
 description *** PRP 2 channel *****
 switchport access vlan 25
 switchport mode access
 no ptp enable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!

interface Vlan1
 no ip address
 shutdown
!
interface Vlan35
 ip address 35.35.35.2 255.255.255.0
!
interface Vlan25
 ip address 25.25.25.2 255.255.255.0
```

```
!
interface Vlan100
 ip address 15.15.15.169 255.255.255.0
!
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
ip tftp source-interface Vlan100
ip tftp blocksize 8192
!
!
!
```



CHAPTER 3

# PTP over PRP


- PTP over PRP, on page 35
- Guidelines and limitations for PTP over PRP, on page 38
- Supported PTP profiles and clock modes, on page 40
- PRP RedBox types, on page 40
- LAN-A and LAN-B failure detection and handling, on page 46
- CLI commands for PTP over PRP, on page 46
- Feature history for PTP over PRP, on page 49


## PTP over PRP

Precision Time Protocol (PTP) can operate over Parallel Redundancy Protocol (PRP) on Cisco Catalyst IE9300 Rugged Series Switches.

PRP provides high availability through redundancy for PTP. For more information about PTP, see *Precision Time Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches* on Cisco.com.

The PRP method achieves redundancy by transmitting in parallel over two independent paths; however, this approach does not work for PTP. The delay that a frame experiences is not the same in the two LANs. In addition, some frames are modified in the transparent clocks (TCs) while transiting through the LAN. A Dually Attached Node (DAN) does not receive the same PTP message from both ports even when the source is the same. Specifically:

- Sync/Follow_Up messages are modified by TCs to adjust the correction field.
- Boundary Clocks (BCs) present in the LAN are not PRP-aware and generate their own Announce and Sync frames with no Redundancy Control Trailer (RCT) appended.
- Follow_Up frames are generated by every 2-step clock and carry no RCT.
- TCs are not PRP-aware and are not obliged to forward the RCT, which is a message part that comes after the payload.

Before PTP was supported over both LAN-A and LAN-B, PTP traffic was permitted only on LAN-A to avoid issues with PTP and parallel transmission. However, when LAN-A went down, the system lost PTP synchronization. To enable PTP to leverage the benefit of redundancy offered by the underlying PRP infrastructure, PTP packets over PRP networks are handled differently than other types of traffic.

The implementation of the PTP over PRP feature is based on the PTP over PRP operation that is detailed in IEC 62439-3:2016, Industrial communication networks - High availability automation networks - Part 3:

Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR) . This approach overcomes the problems mentioned earlier by not appending an RCT to PTP packets and bypassing the PRP duplicate/discard logic for PTP packets.

This table summarizes the feature support for the specified switch models and their corresponding minimum supported Cisco IOS XE software versions.

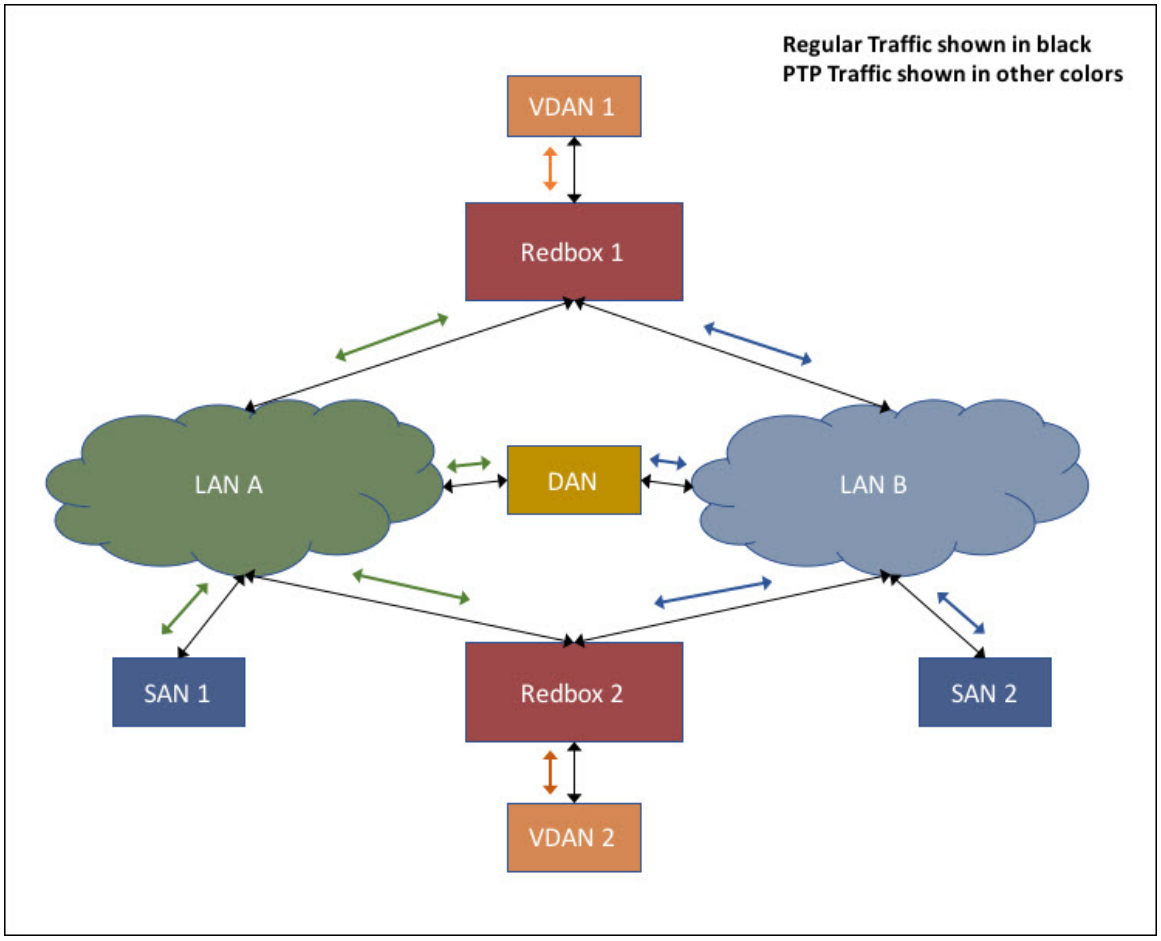
***Table 3: Switch models and supported Cisco IOS XE software versions***

| Switch Model | Supported IOS XE Version |
|---|---|
| IE-9320-26S2C-A | Cisco IOS XE Cupertino 17.9.1 |
| IE-9320-26S2C-E | |
| IE-9320-22S2C4X-A | Cisco IOS XE Dublin 17.12.1 |
| IE-9320-22S2C4X-E | |

# PTP over PRP packet flow

This figure illustrates the operation of PTP over PRP.

*Figure 3: PTP over PRP Packet Flow*




In the figure, VDAN 1 is the grandmaster clock (GMC). Dually attached devices receive PTP synchronization information over both their PRP ports. The LAN-A port and LAN-B port use a different virtual clock that is synchronized to the GMC. However, only one port known as time recipient, is used to synchronize the local clock (VDAN 2 in the figure). When the LAN-A port is serving as the time recipient, its virtual clock synchronizes VDAN 2. The other PRP port, LAN-B, is referred to as PASSIVE. The LAN-B port's virtual clock stays synchronized to the GMC but does not synchronize VDAN 2.

If LAN-A goes down, the LAN-B port takes over as the time recipient and is used to continue synchronizing the local clock on RedBox 2. VDAN 2 attached to RedBox 2 continues to receive PTP synchronization from RedBox 2 as before. Similarly, all DANs, VDANs, and RedBoxes shown in the figure continue to remain synchronized. For SANs, redundancy is not available, and in this example, SAN 1 loses synchronization if LAN-A goes down.

When the time recipient port changes, VDAN 2 may experience an instantaneous shift in its clock because of the offset between the LAN-A and LAN-B virtual clocks. This shift should be only a few microseconds, since both clocks are synchronized to the same GMC. The shift also occurs when the LAN-A port resumes its role as time recipient and the LAN-B port becomes passive.

**Note** Cisco is moving from the traditional Master/Slave nomenclature. In this document, the terms Grandmaster clock (GMC) or time source and time recipient are used instead, where possible. Exceptions may be present due to language that is hard-coded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

### Supported location of GMC

The GMC can be located in a PTP over PRP topology as one of these:

- A RedBox that is connected to both LAN A and LAN B, for example, RedBox 1 in the figure.
- A VDAN, for example, VDAN 1 in the figure.
- A DAN, for example, the DAN in the figure.

The GMC cannot be a SAN attached to LAN-A or LAN-B, because only the devices in LAN-A or LAN-B will be synchronized to the GMC.

# Configuration of PTP over PRP

PTP over PRP does not require configuration beyond how you would normally configure PTP and PRP separately. This feature does not include any new user interface. Previously, PTP operated only over LAN-A. With the PTP over PRP feature, it now operates over both LAN-A and LAN-B. Review the Guidelines and Limitations before implementing PTP over PRP.

Use this high-level workflow to implement PTP over PRP in your network.

1. Refer to the section RedBox Types in this guide to determine the location of the PRP RedBox. Refer to *Precision Time Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches* on Cisco.com to determine the PTP mode and profile.
2. Configure PTP as described in *Precision Time Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches* on Cisco.com. Use the procedure relevant to the PTP profile determined in step 1.
3. Configure PRP as described in the section Create a PRP Channel and Group.

**Note** There are four PRP-capable ports on IE-9320-26S2C-A, IE-9320-26S2C-E, IE-9320-22S2C4X-A, and IE-9320-22S2C4X-Eswitches:

- Gi1/0/21 and Gi1/0/22 are enabled for PRP channel 1.
- Gi1/0/23 and Gi1/0/24 are enabled for PRP channel 2.

# Guidelines and limitations for PTP over PRP

Review these guidelines and limitations before you configure PTP over PRP.

- You must configure PTP and PRP separately. PTP over PRP works automatically without any additional configuration.

  No PTP configuration is available under **interface prp-channel** . You need to configure each PRP channel member interface individually for PTP. In most cases, you do not need to configure PTP on the interfaces because PTP is enabled by default on all physical Ethernet interfaces.



**Note** You can use the **show ptp port** command to verify PTP over PRP configuration. In the command output, the LAN_B port may be displayed as "PASSIVE_SLAVE".

- PTP over PRP can coexist with Device Level Ring (DLR). In this scenario, the PRP RedBox is also part of a DLR network.
- No configuration compatibility is enforced on the PRP channel member interfaces with respect to PTP.

  You can have different PTP configurations on PRP member interfaces. However, for seamless transitions between PASSIVE_SLAVE and SLAVE states, use identical PTP configurations on the interfaces that are part of the same PRP channel.
- We recommend that the grandmaster (GM) clock be dually attached to both PRP LANs (as RedBox, VDAN, or DAN). If the GM is connected to only one PRP LAN, only devices in that LAN will synchronize to the GM.
- PTP over PRP supports only the RedBox types described in PRP RedBox Types. These RedBox types described in IEC 62439-3, Section A, are not supported:
  - PRP RedBoxes as three-port BCs (TWBC) - Section A.4.5.2
  - PRP RedBox as DATC with E2E - Section A.4.5.4.1
  - PRP RedBox as a stateless TC (SLTC) - Section A.4.5.5
- When PTP over PRP is configured for the system, do not configure other switches in PRP LAN-A or LAN-B for PTP boundary mode. This prevents any switch within PRP LAN-A or LAN-B from becoming a Grand Master. PTP transparent mode on PRP LAN-A/B switches is recommended in a time-sensitive environment.
- IE switch platforms do not support PTP profile conversion. For example, if RedBox S in PRP RedBox as DAB with P2P were an IE switch, it would not support Delay_Req/Delay_Resp message exchange with LAN D shown in the figure. It would only support Peer-to-Peer delay measurement mechanism using PDelay messages.
- The PTP over PRP feature does not change PTP VLAN behavior.
- PTP over PRP is not supported for Cisco Catalyst IE9300 Rugged Series Switches.

# Supported PTP profiles and clock modes

This table summarizes PTP over PRP support for the various PTP profiles and clock modes. In unsupported PTP profile/clock mode combinations, PTP traffic flows over LAN-A only. LAN-A is the lower numbered interface. See PRP Channels for PRP interface numbers.

| PTP Profile | Clock Mode | Supported? | PRP RedBox type as per IEC 62439-3 |
|---|---|---|---|
| End-to-End Delay Request-Response default profile | BC | Yes | PRP RedBox as doubly attached BC (DABC) with E2E |
| | E2E TC | No | PRP RedBox as doubly attached TC (DATC) with E2E |
| Power Profile | BC | Yes | PRP RedBox as doubly attached BC (DABC) with P2P |
| | P2P TC | Yes | PRP RedBox as doubly attached TC (DATC) with P2P |

# PRP RedBox types

The switch plays the role of a RedBox in PRP networks. This section describes the types of PRP RedBoxes supported for PTP over PRP as defined in IEC 62439-3.

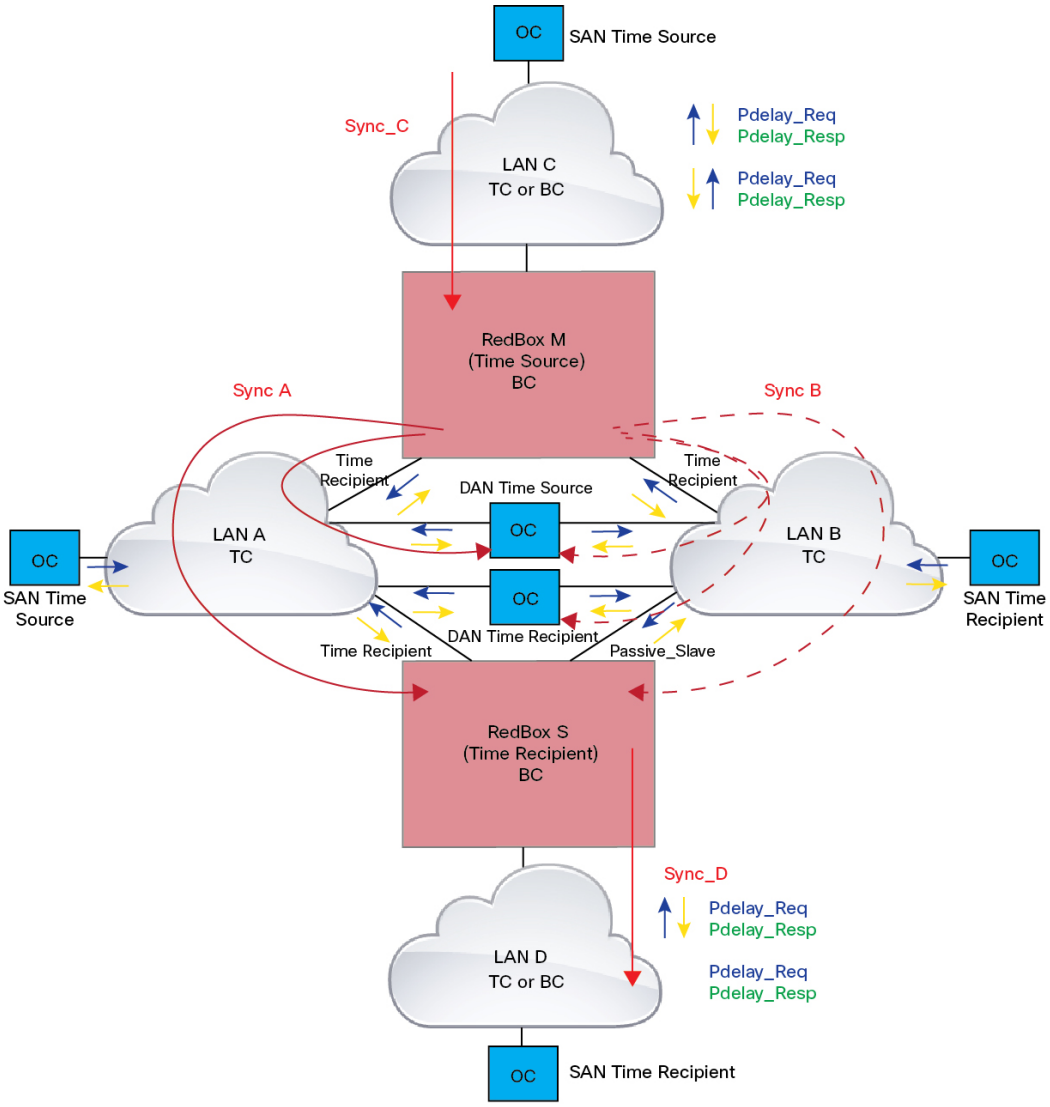
## PRP RedBox as Doubly Attached BC (DABC) with P2P

This figure shows an example where Redbox M and Redbox S are configured to run in Power Profile mode as Boundary Clocks using the Peer-to-Peer (P2P) delay measurement mechanism. The GMC acts as the ordinary clock attached through LAN C. Each clock runs Peer-to-Peer delay measurement, with peer delay regularly calculated and maintained on every link.

The BMCA on Redbox M determines that ports A and B are connected to the time source. The PTP protocol on Redbox M treats both ports as individual time source ports and sends Sync and Follow_Up messages separately on each port.

## PRP RedBox as Doubly Attached BC (DABC) with P2P

*Figure 4: PRP Redbox as DABC with P2P*




On Redbox S, the regular BMCA operation determines port A to be time recipient and port B to be PASSIVE. However, with the knowledge that ports A and B are part of the same PRP channel, port B is forced into PASSIVE_SLAVE state. Port A and Port B on Redbox S operate in these ways:

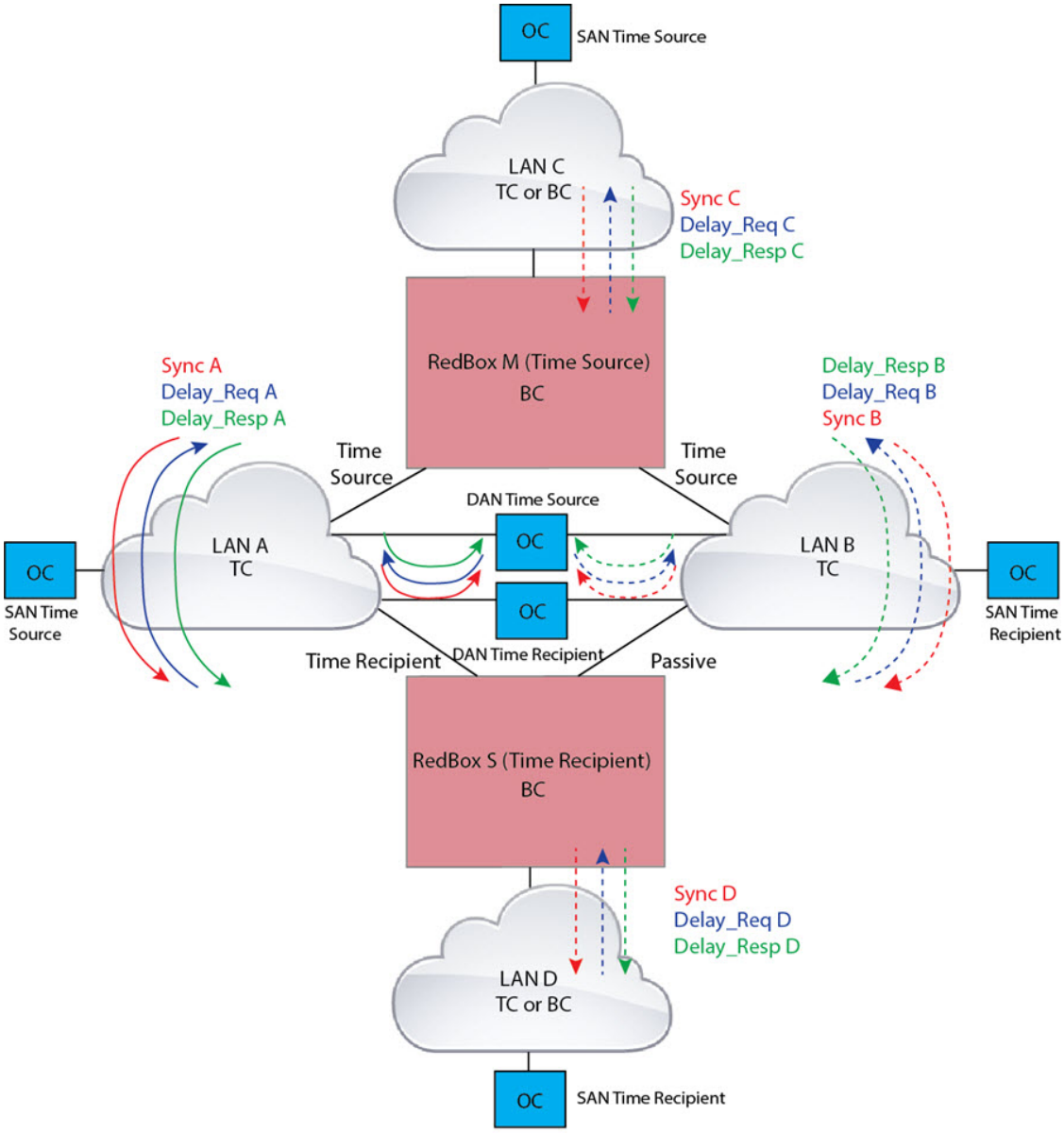
- Port A acts as a regular time recipient port. It uses Sync and Follow_Up messages, along with their correction field, to calculate the delay and offset from the time source and synchronize the local clock. Unlike an E2E BC, Port A does not need to generate Delay_Req messages because all link delays and residence times along the PTP path are accumulated in the correction field of the Follow_Up messages.
- Port B is in PASSIVE_SLAVE state. Like port A, it maintains the delay and offset from the time source, but it does not perform any operation on the local clock. Because all synchronization information is

available, Port B can seamlessly become the new time recipient if port A loses communication with the GM.

# PRP RedBox as a Doubly Attached BC (DABC) with E2E

The figure illustrates two RedBoxes, M and S, as Boundary Clocks (BCs). These RedBoxes use the End-to-End delay measurement mechanism and the IEEE1588v2 Default Profile. The Best Master Clock Algorithm (BMCA) on RedBox M determines that port A and port B should be connected to the time source. The PTP protocol on RedBox M treats ports A and B as individual time source ports. It sends out Sync and Follow_Up messages separately on each port.

*Figure 5: PRP Redbox as DABC with E2E*




On RedBox S, the regular BMCA operation assigns port A as a time recipient and port B as PASSIVE. However, with the knowledge that ports A and B are part of the same PRP channel, port B is forced into PASSIVE_SLAVE state. Port A and Port B on RedBox S operate in these roles:

- Port A works as a regular time recipient port. It uses the end-to-end delay measurement mechanism to calculate delay and offset from the time source. Using the calculated delay and offset, it synchronizes the local clock.
- Port B is in PASSIVE_SLAVE state. It uses the end-to-end delay measurement mechanism to calculate delay and offset from the time source.

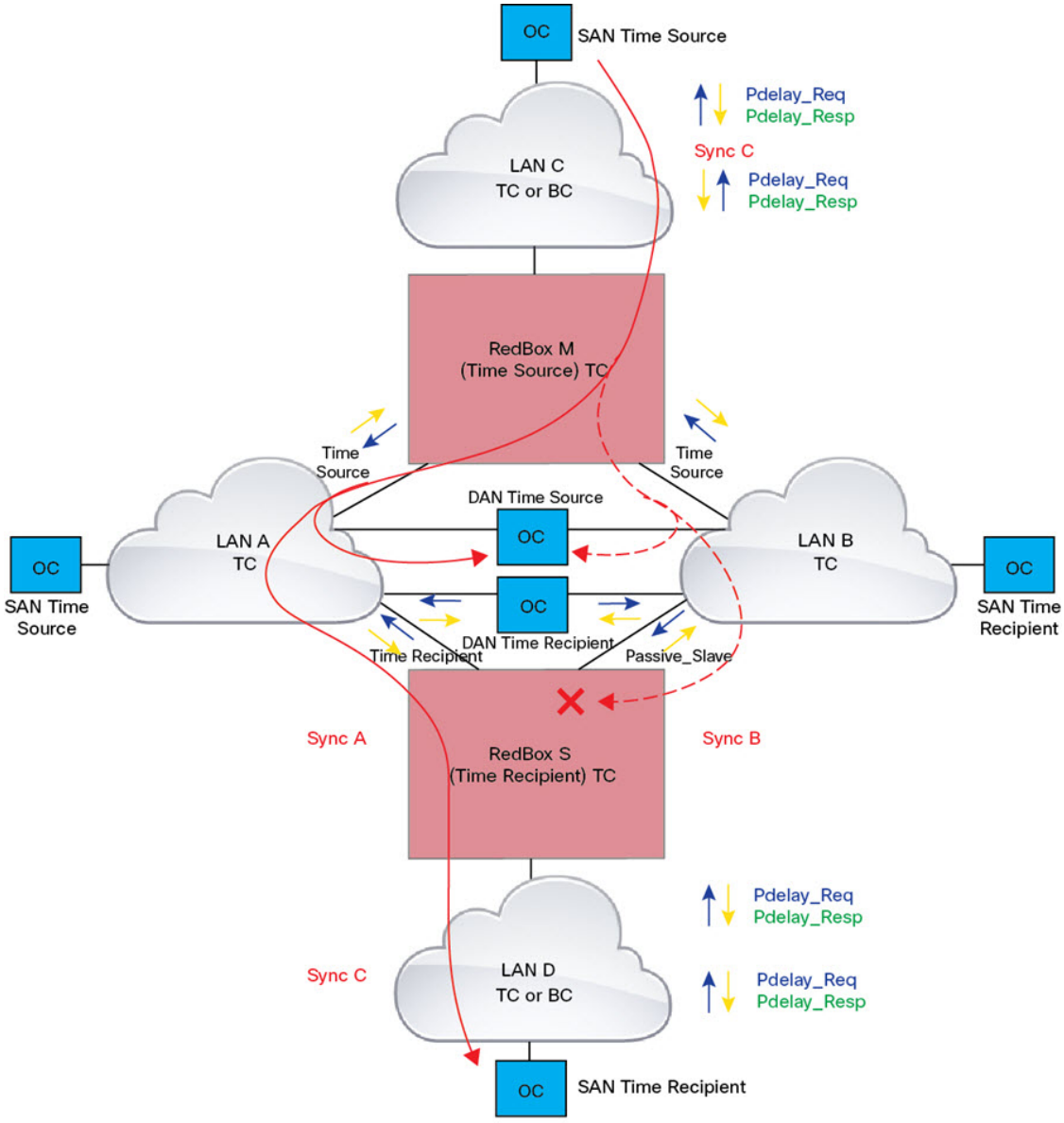
It remains passive by maintaining the calculated delay and offset instead of performing any operation on the local clock. The availability of delay and offset information enables Port B to quickly become a time recipient if port A loses connectivity to the time source.

# PRP RedBox as Doubly Attached TC (DATC) with P2P

This figure shows an example where Redbox M and Redbox S are configured to run in Power Profile mode as Transparent Clocks. In this example, the GMC is the ordinary clock attached through LAN C. All clocks are configured for Peer-to-Peer Delay measurement, and peer delay is regularly calculated and maintained on each link shown in the figure.

Redbox M and Redbox S run BMCA, even though a P2P TC is not required to run BMCA. On Redbox M, the BMCA determines ports A and B to be connected to the time source. Redbox M forwards all Sync and Follow_Up messages received on port C out of ports A and B.

*Figure 6: PRP Redbox as DATC with P2P*




On Redbox S, port A is determined to be time recipient and port B operates as PASSIVE_SLAVE as described earlier. Port A and Port B on Redbox S operate as follows:

- Port A works as a regular time recipient port. It uses the Sync and Follow_Up messages along with their correction field to calculate the delay and offset from time source and synchronize the local clock. (Unlike an E2E BC, it does not need to generate Delay_Req messages since all the link delays and residence times along the PTP path are accumulated in the correction field of the Follow_Up messages).
- Like port A, port B maintains the delay and offset from the time source but does not affect the local clock. Because all synchronization information is available, port B can seamlessly become the new time recipient if port A loses communication with the GMC.

# LAN-A and LAN-B failure detection and handling

Failures in LAN-A and LAN-B are detected and handled in the same way for all RedBox types that are described in PRP RedBox Types.

In the configuration described for PRP RedBox as DATC with P2P and the GMC as a SAN in LAN C, a failure related to PTP in LAN-A or LAN-B can occur for several reasons:

- a device within the LAN goes down,
- a link within the LAN goes down resulting in loss of connectivity, or
- PTP messages are dropped within the LAN.

These events result in PTP Announce Receipt Timeout on RedBox S, which triggers the BMCA calculation. Refer to section 7.7.3.1 of the IEEE 1588v2 standard for details on Announce Receipt Timeout.

Once invoked, the BMCA changes the state of the PASSIVE_SLAVE port to time recipient. It also changes the time recipient port to PASSIVE_SLAVE, PASSIVE, or FAULTY.

The state changes are performed atomically. This process prevents transient cases with two time recipient ports or two PASSIVE_SLAVE ports.

RedBox S now synchronizes to the GMC over the new time recipient port. The change to synchronization should be quick and seamless, unless the delays experienced by PTP packets on the two LANs are very different or if there are some non-PTP devices in the LANs.

The SAN time recipient in LAN D also sees this shift in the timing from RedBox S and must converge to the new clock. This is similar to a GMC change event for this clock, but as mentioned earlier, the change is usually seamless.

# CLI commands for PTP over PRP

After you enable PTP over PRP on a switch, you can use CLI **show** commands to display PTP clock data for PRP.

You can find information about CLI commands specific to PTP in *Precision Time Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches*. This guide also covers information about CLI commands specific to PRP.

## show ptp clock running

The **show ptp clock running** command shows the summary of the running PTP clock and information about its ports. Use the command to verify that the boundary clock is `PHASE_ALIGNED` —that the clock is in sync with the Grandmaster Clock. Also ensure that one port is in the `Slave` state and the other is in the `Passive Slave` state.

```
RedBox2#show ptp clock running
                      PTP Boundary Clock [Domain 0]  [Profile: default]
        State           Ports          Pkts sent      Pkts rcvd      Redundancy Mode
        PHASE_ALIGNED   2              168704         150444         Hot standby
                               PORT SUMMARY
                                                                        PTP Master
Name     Tx Mode      Role         Transport    State           Sessions     Port Addr
```

```
dyn1     mcast        negotiated   Ethernet     Slave           1            UNKNOWN
dyn2     mcast        negotiated   Ethernet     Passive Slave   1            UNKNOWN
```

# show prp channel detail

Use the **show ptp channel detail** command to view detailed information about both port channels. Ensure that Gi1/0/21 and Gi1/0/22 are in the `Inuse` state.

```
RedBox2#show prp channel detail
               PRP-channel listing:
               --------------------
PRP-channel: PR1
------------
 Layer type = L2
 Ports: 2       Maxports = 2
 Port state = prp-channel is Inuse
 Protocol = Enabled
Ports in the group:
  1) Port: Gi1/0/21
   Logical slot/port = 1/21     Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/0/22
   Logical slot/port = 1/22     Port state = Inuse
        Protocol = Enabled
PRP-channel: PR2
------------
 Layer type = L2
 Ports: 2       Maxports = 2
 Port state = prp-channel is Inuse
 Protocol = Enabled
Ports in the group:
  1) Port: Gi1/0/23
   Logical slot/port = 1/23     Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/0/24
   Logical slot/port = 1/24     Port state = Inuse
        Protocol = Enabled
```

# show prp statistics ptpPacketStatistics

The **show prp statistics ptpPacketStatistics** command displays the number of PTP packets ingressing and egressing out of the clock ports when in PRP is enabled. It also displays the drop at the ingress level.

```
RedBox2#show prp statistics ptpPacketStatistics
 PRP channel-group 1 PTP STATS:
   ingress lan a: 250
   ingress drop lan a: 0
   ingress lan b: 377
   ingress drop_lan b: 0
   egress lan a: 185
   egress lan b: 188
 PRP channel-group 2 PTP STATS:
   ingress lan a: 384
   ingress drop lan a: 0
   ingress lan b: 388
   ingress drop_lan b: 0
   egress lan a: 191
   egress lan b: 193
RB2#
```

# show ptp lan port int

The **show ptp lan port int** command displays the port level PTP information for LAN ports, including the port state for PRP.

The following example shows the command and output for port gi1/0/23 on PRP channel 2. Ensure that the port is in SLAVE state.

```
RedBox2#show ptp lan port int gi1/0/23
  PTP PORT DATASET: GigabitEthernet1/0/23
    Port identity: clock identity: 0x84:eb:ef:ff:fe:61:70:3f
    Port identity: port number: 3
    PTP version: 2
    Port state: SLAVE
    Peer delay request interval(log mean): 0
    Peer mean path delay(ns): 0
    Sync fault limit: 10000
    Rogue master block: FALSE
    Ingress phy latency: 725
    Egress phy latency: 0
```

The following example shows the command and output for port gi1/0/24 on PRP channel 1. Ensure that the port is in PASSIVE_SLAVE state.

```
RedBox2#show ptp lan port int gi1/0/24
  PTP PORT DATASET: GigabitEthernet1/0/24
    Port identity: clock identity: 0x84:eb:ef:ff:fe:61:70:3f
    Port identity: port number: 4
    PTP version: 2
    Port state: PASSIVE_SLAVE
    Peer delay request interval(log mean): 0
    Peer mean path delay(ns): 2
    Sync fault limit: 10000
    Rogue master block: FALSE
    Ingress phy latency: 725
    Egress phy latency: 0
```

# ptp clock boundary domain

You can configure a default profile PTP clock boundary domain or a power profile PTP clock boundary domain. When you configure either domain, you must add both PRP member interfaces to the PTP clock.

The following example sets a PTP clock boundary domain for a default profile:

```
ptp clock boundary domain 0 profile default
clock-port dyn1
transport ipv4 multicast interface Gi1/0/21
clock-port dyn2
transport ipv4 multicast interface Gi1/0/22
```

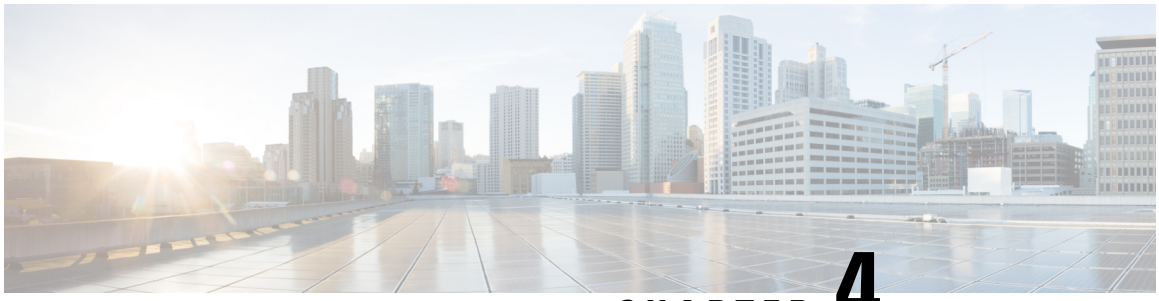
The following example sets a PTP clock boundary domain for a power profile:

```
ptp clock boundary domain 0 profile power
clock-port dyn1
transport ethernet multicast interface Gi1/0/21
clock-port dyn2
transport ethernet multicast interface Gi1/0/22
```

# Feature history for PTP over PRP

The following table provides release and related information for the features that are documented in this guide. The features are available in all the releases after the initial release, unless noted otherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Dublin 17.12.1 | Precision Timing Protocol (PTP) over Parallel Redundancy Protocol (PRP) | This feature became available for Cisco Catalyst IE9300 Rugged Series Switches IE-9320-22S2C4X-A and IE-9320-22S2C4X-E in this release. |
| Cisco IOS XE Cupertino 17.9.x | PTP over PRP | This feature became available for Cisco Catalyst IE9300 Rugged Series Switches IE-9320-26S2C-A and IE-9320-26S2C-E in this release. |



CHAPTER 4

# Resilient Ethernet Protocol


- Feature history for Resilient Ethernet Protocol, on page 51
- Resilient Ethernet Protocol, on page 52
- Resilient Ethernet Protocol Fast, on page 59
- REP Zero Touch Provisioning technologies, on page 61
- REP segment ID auto-discovery, on page 65
- REP segments, on page 67
- Preventive best practices, on page 77
- Monitoring REP configurations, on page 78
- PTP over REP , on page 82


## Feature history for Resilient Ethernet Protocol

The table provides release and related information for the features documented in this guide.

***Table 4: Feature History for Resilient Ethernet Protocol***

| Release | Feature | Feature Information |
|---|---|---|
| **Cisco IOS XE 26.2.1** | Enhanced scale limit | Starting from Cisco IOS XE release 26.2.1, REP Fast supports 26 open segments and 12 closed segments. |
| **Cisco IOS XE 26.1.1** | Enhanced scale limit | Starting with IOS-XE 26.1.1, a standalone Cisco Catalyst IE9300 Rugged Series Switch supports upto 26 open REP segments and 13 REP ring segments. |
| **Cisco IOS XE 17.15.2** | Resilient Ethernet Protocol | Starting with this release, the Cisco Catalyst IE9300 Rugged Series Switches supports up to 8 REP segments or 3 REP Fast segments. This is an increase from the previous limit of 4 REP segments or 3 REP Fast segments. |

| Release | Feature | Feature Information |
|---|---|---|
| **Cisco IOS XE 17.14.x** | Resilient Ethernet Protocol Zero Touch Provisioning | This feature was introduced in this release for Cisco Catalyst IE9300 Rugged Series Switches. |
| **Cisco IOS XE Cupertino 17.9.x** | Resilient Ethernet Protocol Fast | This feature was introduced in this release for Cisco Catalyst IE9300 Rugged Series Switches. |

# Resilient Ethernet Protocol

Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time. REP controls a group of ports that are connected in a segment. It ensures that the segment does not create any bridging loops and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing.

## REP segments

A REP segment is a chain of ports that connect to each other and are configured with a segment ID. Each segment consists of standard (nonedge) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment. Each segment port can have only one external neighbor. A segment can pass through a shared medium. However, on any link, only two ports can belong to the same segment. REP operates only on trunk ports.

### Characteristics of REP segments

REP segments have these characteristics.

- If all ports in a segment are operational, one port (called the ALT port) is blocked for each VLAN. If VLAN load balancing is configured, two ALT ports in the segment determine which VLANs are blocked.
- If a port is not operational, and causes a link failure, all ports forward traffic on all VLANs to ensure connectivity.
- In case of a link failure, alternate ports are unblocked as quickly as possible. When the failed link is restored, a logically blocked port per VLAN is selected with minimal disruption to the network.

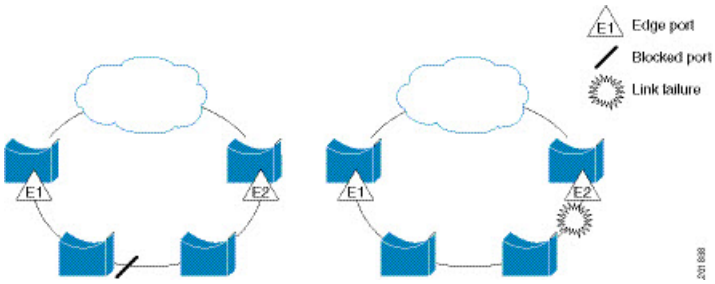
You can construct almost any type of network that is based on REP segments.

## REP open segment

- Network Topology: The figure illustrates a network segment consisting of six ports distributed across four switches.
- Edge Port Configuration: Ports E1 and E2 are specifically configured as edge ports.
- Normal Operation: Under normal conditions (as shown in the left segment), one port is blocked to prevent network loops. This blocked port is marked with a diagonal line and is formally known as the **Alternate (ALT) port**.

- Network Failover: In the event of a network failure, the ALT port automatically transitions to a forwarding state to maintain connectivity and minimize service disruption.

*Figure 7: REP open segment*

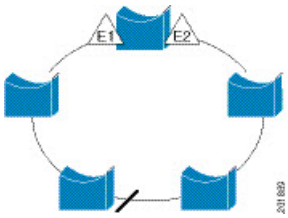



- Open Segment Status: The segment illustrated is an open segment. There is no direct connectivity between the two edge ports.
- Loop Prevention: Because the segment is open, it cannot cause a bridging loop, allowing you to safely connect the segment edges to any network.
- Connectivity and Redundancy: Hosts connected to switches within the segment have two potential paths to the rest of the network via the edge ports. Only one of these connections is active at any time to prevent loops.
- Failover Mechanism: If a failure occurs on any part of the REP segment, the protocol automatically unblocks the Alternate (ALT) port. This ensures that connectivity is maintained through the remaining available gateway.

## REP ring segment

The segment shown in the figure is a closed segment, also called a ring segment. In this topology, both edge ports are located on the same switch. This configuration allows you to create a redundant connection between any two routers in the segment.

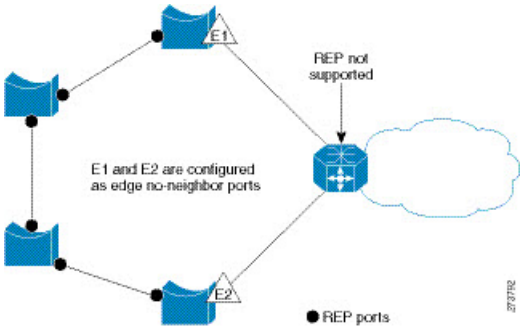
*Figure 8: REP ring segment*




## Edge no-neighbor ports

In access ring topologies, the neighboring switch might not support REP as shown in the figure. In this case, you can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports. You can configure the edge no-neighbor port to send an STP topology change notice (TCN) towards the aggregation switch.

*Figure 9: Edge No-Neighbor Ports*




REP has these limitations:

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment. Multiple port failures within the REP segment cause loss of network connectivity.
- Only configure REP in networks with redundancy. If you configure REP in a network without redundancy, connectivity will be lost.

# Link integrity detection

REP does not use an end-to-end polling function between edge ports to verify link integrity; instead, it implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. On an interface, all VLANs are blocked until the neighbor is detected. When REP identifies the neighbor, it selects the neighbor port to act as the alternate port and designates the ports that will forward traffic.

### Port identification and initialization

Each port in a segment has a unique port ID. The port ID format is similar to the format used by the spanning tree algorithm: a port number (unique on the bridge) combined with a MAC address (unique in the network). When a segment port comes online, its LSL sends packets that include the segment ID and the port ID. The port becomes operational after successfully completing a three-way handshake with a neighbor in the same segment.

### Conditions preventing port operation

A segment port does not become operational if:

- no neighbor has the same segment ID.
- more than one neighbor has the same segment ID.
- a neighbor does not acknowledge a local port as a peer.

### Neighbor adjacency and role assignment

Each port creates an adjacency with its immediate neighbor. After establishing neighbor adjacencies, the ports negotiate to select the blocked port for the segment, which functions as the alternate port. The remaining ports become unblocked.

### REP packet transmission

By default, REP packets are sent to a bridge protocol data unit-class MAC address. Devices can also send packets to a Cisco multicast address, which is used only to transmit blocked port advertisement (BPA) messages during a segment failure. Devices that do not run REP drop these packets.

## Fast convergence

- Protocol Efficiency: REP operates on a physical link basis rather than per-VLAN. This allows a single hello message to cover all VLANs, significantly reducing the protocol load.
- Configuration Requirements: To ensure proper operation, VLANs must be created consistently across all switches in a segment. Additionally, the same set of allowed VLANs must be configured on all REP trunk ports.
- Performance and Flooding: To minimize latency, REP can flood specific packets to a multicast address using the hardware flood layer (HFL). These messages are distributed throughout the entire network.
- External Handling: Switches located outside of the REP segment treat these HFL messages as standard data traffic.
- Flooding Control: You can manage and control the flooding of these messages by configuring an administrative VLAN for the entire domain or for a specific segment.

## VLAN load balancing

One edge port in the REP segment acts as the primary edge port; and another as the secondary edge port. It is the primary edge port that always participates in VLAN load balancing in the segment. REP VLAN balancing is achieved by blocking some VLANs at a configured alternate port and all the other VLANs at the primary edge port.

### Specifying alternate port for VLAN load balancing

When you configure VLAN load balancing, you can specify the alternate port in one of the three ways:

- By entering the port ID of the interface. To identify the port ID of a port in the segment, enter the **show interface rep detail** interface configuration command for the port.
- By entering the preferred keyword to select the port that you previously configured as the preferred alternate port with the **rep segment** *segment-id* **preferred** interface configuration command.
- By entering the neighbor offset number of a port in the segment, which identifies the downstream neighbor port of an edge port. The neighbor offset number range is –256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers indicate the secondary edge port (offset number -1) and its downstream neighbors.

### Configuring offset numbers

Configure offset numbers on the primary edge port by identifying a port's downstream position from the primary (or secondary) edge port. Never enter an offset value of 1 because that is the offset number of the primary edge port.

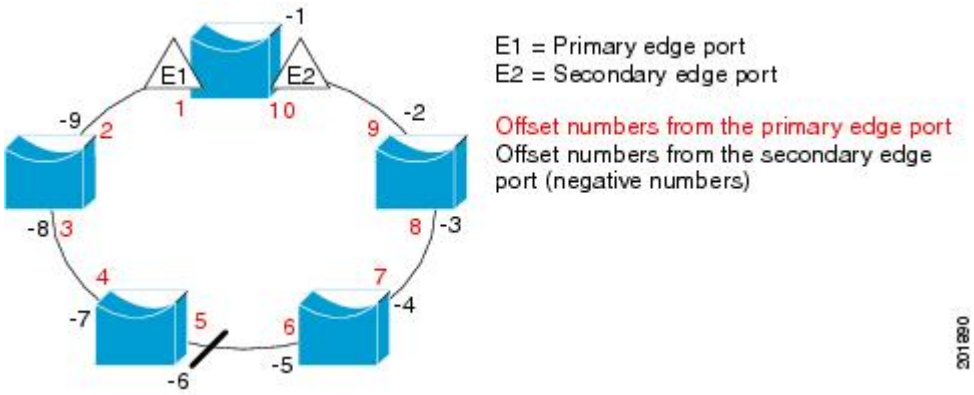
This figure shows neighbor offset numbers for a segment, where E1 is the primary edge port and E2 is the secondary edge port. The red numbers inside the ring are numbers offset from the primary edge port; the black numbers outside of the ring show the offset numbers from the secondary edge port.

You can identify all ports—excluding the primary edge port—using offset numbers:

- Positive offset: Indicates the port's position downstream from the primary edge port.
- Negative offset: Indicates the port's position downstream from the secondary edge port.

If E2 became the primary edge port, its offset number would then be 1 and E1 would be -1.

***Figure 10: Neighbor offset numbers in a segment***




### Configuring VLAN load-balancing triggers

When the REP segment is complete, all the VLANs are blocked. When you configure VLAN load balancing, you must also configure triggers in one of the two ways:

- **Manual Trigger**: Manually trigger VLAN load balancing at any time by entering the **rep preempt segment** *segment-id* privileged EXEC command on the switch that has the primary edge port.
- **Preempt Delay Time**: Configure a preempt delay time by entering the **rep preempt delay seconds** interface configuration command. After a link failure and recovery, VLAN load balancing begins after the configured preemption time period elapses. Note that the delay timer restarts if another port fails before the time has elapsed.

### VLAN load balancing execution

When VLAN load balancing is configured, it does not start working until triggered by either manual intervention or a link failure and recovery.

When VLAN load balancing is triggered, the primary edge port sends out a message to alert all the interfaces in the segment about the preemption. When the secondary port receives the message, the message is sent to the network to notify the alternate port to block the set of VLANs specified in the message and to notify the primary edge port to block the remaining VLANs.

### Blocking all VLANs on a port

You can also configure a particular port in the segment to block all the VLANs. Only the primary edge port initiates VLAN load balancing, which is not possible if the segment is not terminated by an edge port on each end. The primary edge port determines the local VLAN load-balancing configuration.

### Reconfiguring VLAN load balancing

Reconfigure the primary edge port to reconfigure load balancing. When you change the load-balancing configuration, the primary edge port waits for the **rep preempt segment** command or for the configured preempt delay period after a port failure and recovery, before executing the new configuration.

If you change an edge port to a regular segment port, the existing VLAN load-balancing status does not change. Configuring a new edge port might cause a new topology configuration.

## Spanning tree interaction

REP does not interact with STP, but it can coexist. A port that belongs to a segment is removed from spanning tree control and STP BPDUs are not accepted or sent from segment ports. Therefore, STP cannot run on a segment.

To migrate from an STP ring configuration to REP segment configuration, you begin by configuring a single port in the ring as part of the segment. Next, configure contiguous ports to minimize the number of segments. Each segment always contains a blocked port, so multiple segments means multiple blocked ports and a potential loss of connectivity. After configuring the segment in both directions up to the edge ports, configure the edge ports.

## Resilient Ethernet Protocol (REP) Negotiated (Deprecated)



**Note** Starting IOS-XE release 17.17.1, 17.15.3, 17.12.5, 17.9.7, REP-Negotiated feature is deprecated. You can use REP-ZTP as an alternative.

REP and Spanning Tree Protocol (STP) are two different loop avoidance protocols. REP has certain advantages over STP in terms of convergence time. REP can be configured to run in a ring topology in such a way that it can provide the redundant path in case of a single link failure in the ring.

Cisco switches are STP enabled by default. If a switch that is STP enabled is inserted in an already running REP ring (for addition of a new node or replacement of existing node) the following conditions apply:

- The new switch will cause a break in the REP ring.
- The new switch will not be able to communicate over the ring until it is configured to be part of the REP ring.

The REP Negotiated feature tries to solve these issues by negotiating the REP status with the peers. The following table identifies when REP Negotiation events will trigger and the action to take. There are two events: both peers are negotiating, and neither peer is negotiating.

**Note** REP Negotiated works only on uplink ports.

| SELF REP Negotiated | PEERS REP Negotiated | Event Triggered | Action |
|---|---|---|---|
| True | True | REPN | Configure REP |
| True | False | REPNN | Configure STP |
| False | X | REPNN | Remain in STP |

This feature depends on 3 different protocols to get the required data and decide the correct configuration. The different protocols involved, and their purpose is given below:

- **STP**: By default, STP is enabled on all the ports on the Cisco Switch.
- **REP**: The customer network is configured to form a REP ring to provide better convergence time and redundancy.
- **Cisco Discovery Protocol (CDP)**: The feature depends on user defined TLVs sent through CDP messages to negotiate the correct (STP or REP) configuration for the interface.

# REP ports

REP segments consist of Failed, Open, or Alternate ports:

- A port configured as a regular segment port starts as a failed port.
- After the neighbor adjacencies are determined, the port transitions to alternate port state, blocking all the VLANs on the interface. Blocked-port negotiations occur. When the segment settles, one blocked port remains in the alternate role, and all other ports become open ports.
- When a failure occurs in a link, all the ports move to the Failed state. When the Alternate port receives the failure notification, it changes to the Open state, forwarding all the VLANs.

Converting a regular segment port to an edge port, or converting an edge port to a regular segment port, does not always result in a topology change. If you convert an edge port into a regular segment port, VLAN load balancing is not implemented unless it has been configured. For VLAN load balancing, you must configure two edge ports in the segment.

A segment port that is reconfigured as a spanning tree port restarts according to the spanning tree configuration. By default, this is a designated blocking port. If PortFast is configured or if STP is disabled, the port goes into the forwarding state.

# Resilient Ethernet Protocol Fast

The Resilient Ethernet Protocol (REP) Fast feature allows faster link failure detection and convergence on the switch copper Gigabit Ethernet (GE) ports.

**Note** REP Fast is not supported on Trustsec.

### REP design and link detection times

REP was originally designed for Fast Ethernet (FE 10/100) ports. On Fiber GE ports, link down detection time is also 10 ms. On GE copper interfaces, link drop detection and recovery times range from 750 ms to 350 ms. As a result, link loss and recovery are detected more quickly on GE fiber interfaces than on copper interfaces. Consequently, the convergence time for REP is much longer when using GE copper interfaces.

To improve link down detection time, the beacon mechanism triggers faster link failure detection (within 5–10 ms) when a REP interface is configured in REP Fast mode. The switch has two timers for each REP interface. The first timer is triggered every 3 ms to transmit the beacon frame to the neighbor node. After the frame is successfully transmitted and received, both timers are reset. If the packet is not received after transmission, the second timer is triggered to check reception within 10 ms. If the packet is not received when the timer expires, the switch sends a link down message.

### Operation and compatibility

REP Fast operates on an individual link basis and does not affect the REP Protocol. Both ends of the link must support REP Fast for the feature to work. REP Fast can be used on any interface link pair configured for REP, but it was developed to address an issue on Gigabit copper links. It increases the speed of link failure detection on Gigabit copper interfaces.

### Mixed REP and REP fast links

A REP Ring can have a mix of normal REP links and links with REP Fast. Interfaces with REP Fast transmit 3000 packets a second as part normal operation. Enabling REP Fast does not affect REP ring size, because it operates only on the interfaces configured for it. Because REP Fast has to generate Beacon frames, only six interfaces on a single REP node can be configured for REP Fast at a time.

### Convergence and compatibility requirements

If the neighbor acknowledges and is configured for REP Fast mode, convergence occurs within 50 ms. If a neighbor switch does not support the REP Fast feature, normal REP mode must be used for link up/down detection. In this case, you must disable fast mode on both ends of the link.

For information about configuring REP Fast, see Configure REP Fast in this guide.

# Configure REP Fast

Follow these steps to configure REP Fast:

### Before you begin

Enable REP on the switch and configure the REP topology as described in Configuring REP.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Step 2** Use the **interface** *interface-id* command to specify the interface and enter interface configuration mode.

**Step 3** Use the **REP fastmode** command to enable REP Fast.

**Step 4** Use the **end** command to return to privileged exec mode.

### Example

```
gabitEthernet 1/0/1
switch-RJ(config-if)#rep seg
switch-RJ(config-if)#rep segment ?
<1-1024> Between 1 and 1024

switch-RJ(config-if)#rep segment 10
switch-RJ(config-if)#rep fastmode
switch(config)#int <interface number>
switch(config-if)#
switch(config-if)#rep ?
  fastmode       REP fastmode
switch (config-if)#rep fastmode ?
  <cr>  <cr>

switch#sh run int <interface number>
Building configuration...

Current configuration : 89 bytes
!
interface <interface number>
 switchport mode trunk
 rep segment <segment id>
 rep fastmode
end
switch#

switch#sh run int <interface number>
Building configuration...

Current configuration : 89 bytes
!
interface <interface number>
 switchport mode trunk
 rep segment <segment id>
 rep fastmode
end
```

# REP Zero Touch Provisioning technologies

REP Zero Touch Provisioning (ZTP) is a feature that enables automated provisioning of REP rings in a network, eliminating the need for manual configuration during device deployment.

- Automates the configuration of REP rings using zero-touch technologies.
- Introduces a new TLV extension into REP LSL packets.
- Reduces manual intervention required for Day 0 REP ring provisioning.

### How REP ZTP works

ZTP technologies automate bringing devices such as routers and switches into a functional state with little or no manual configuration. The Cisco Network Plug and Play (PnP) and autoinstall Day 0 solutions offer a unified, secure approach to help enterprise and industrial network customers simplify device rollouts and provisioning updates.

However, PnP does not support REP because of REP's design. Prior to the REP ZTP feature, REP ring provisioning for Day 0 required manual intervention. The REP ZTP feature introduces a new TLV extension into the REP LSL packets to support configuring REP rings with zero-touch technologies.

## Day 0 processes

Zero Touch Provisioning (ZTP) and Cisco PnP process enable a switch with no startup configuration to automatically obtain its configuration from a DHCP and PnP server.

- Switches with no startup configuration trigger the Cisco PnP agent to initiate DHCP discovery.
- The DHCP server provides IP configuration and the address or hostname of the PnP server using option 43.
- The PnP server downloads the required Day 0 configuration to the switch to complete provisioning.

### ZTP deployment workflow

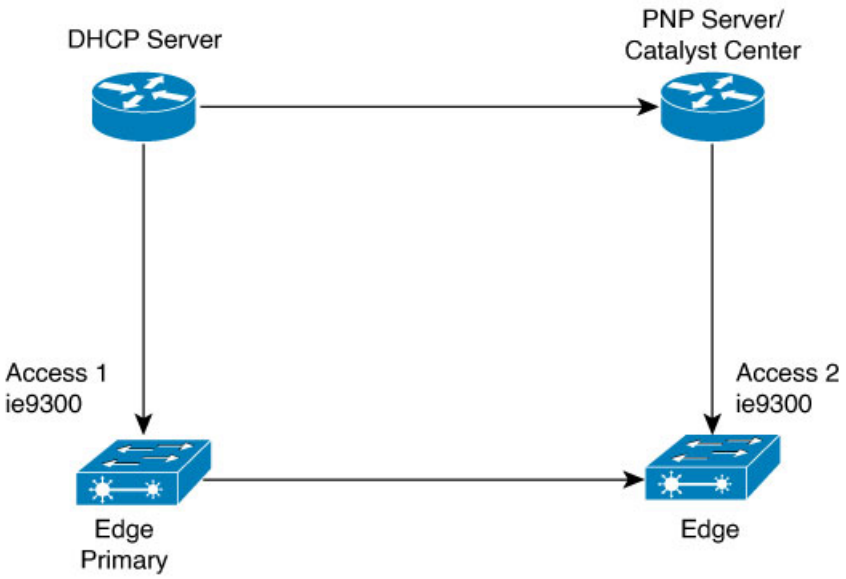
- Initiation: A switch without a startup configuration triggers the Cisco PnP agent to begin a DHCP discovery process.
- Identification: Upon receiving a DHCP DISCOVER message with Option 60 ("cisco pnp"), the DHCP server responds with the PnP server's address via Option 43.
- Connection: The switch's PnP agent extracts the PnP server information from the DHCP response to establish a direct connection.
- Provisioning: The PnP server completes the process by deploying the required Day 0 configuration to the switch.



**Note** The DHCP Server and the PnP Server/Cisco Catalyst Center are not part of the REP ring.

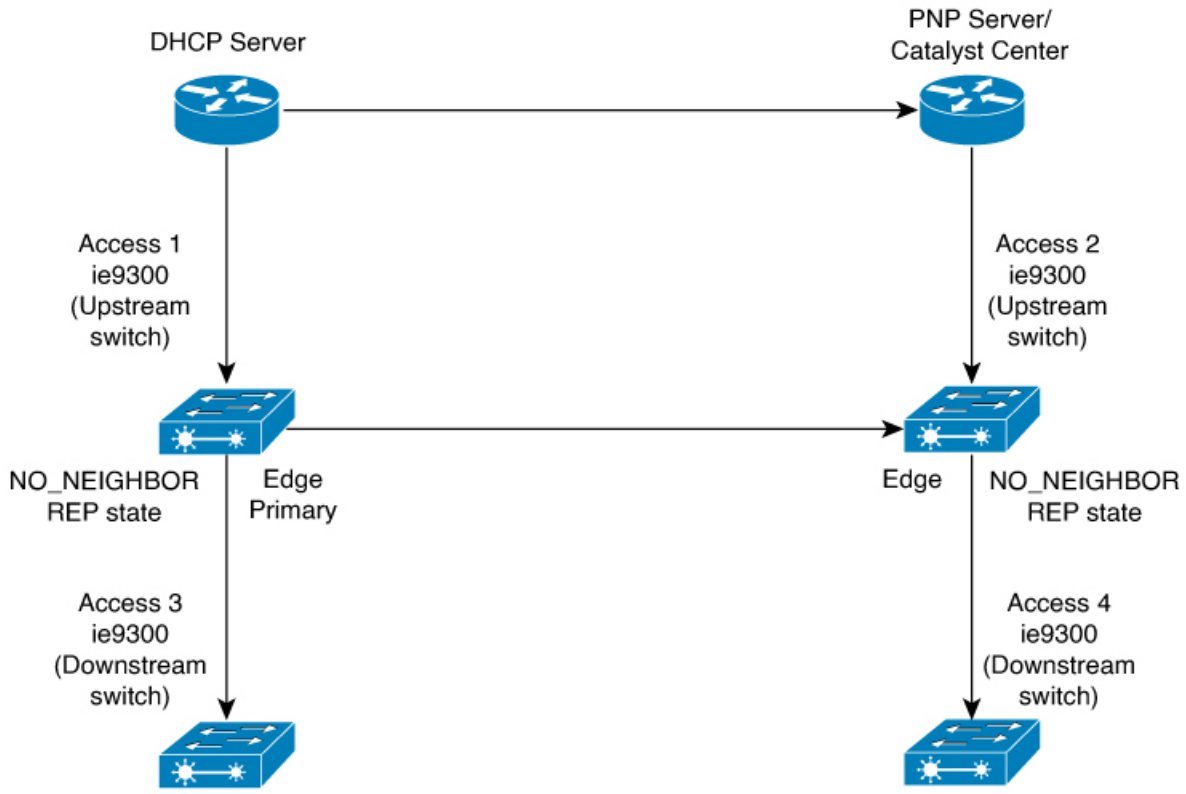
The example diagrams illustrate REP ring provisioning on Day 0, prior to the introduction of REP ZTP.

***Figure 11: Adding edge nodes to the REP ring***



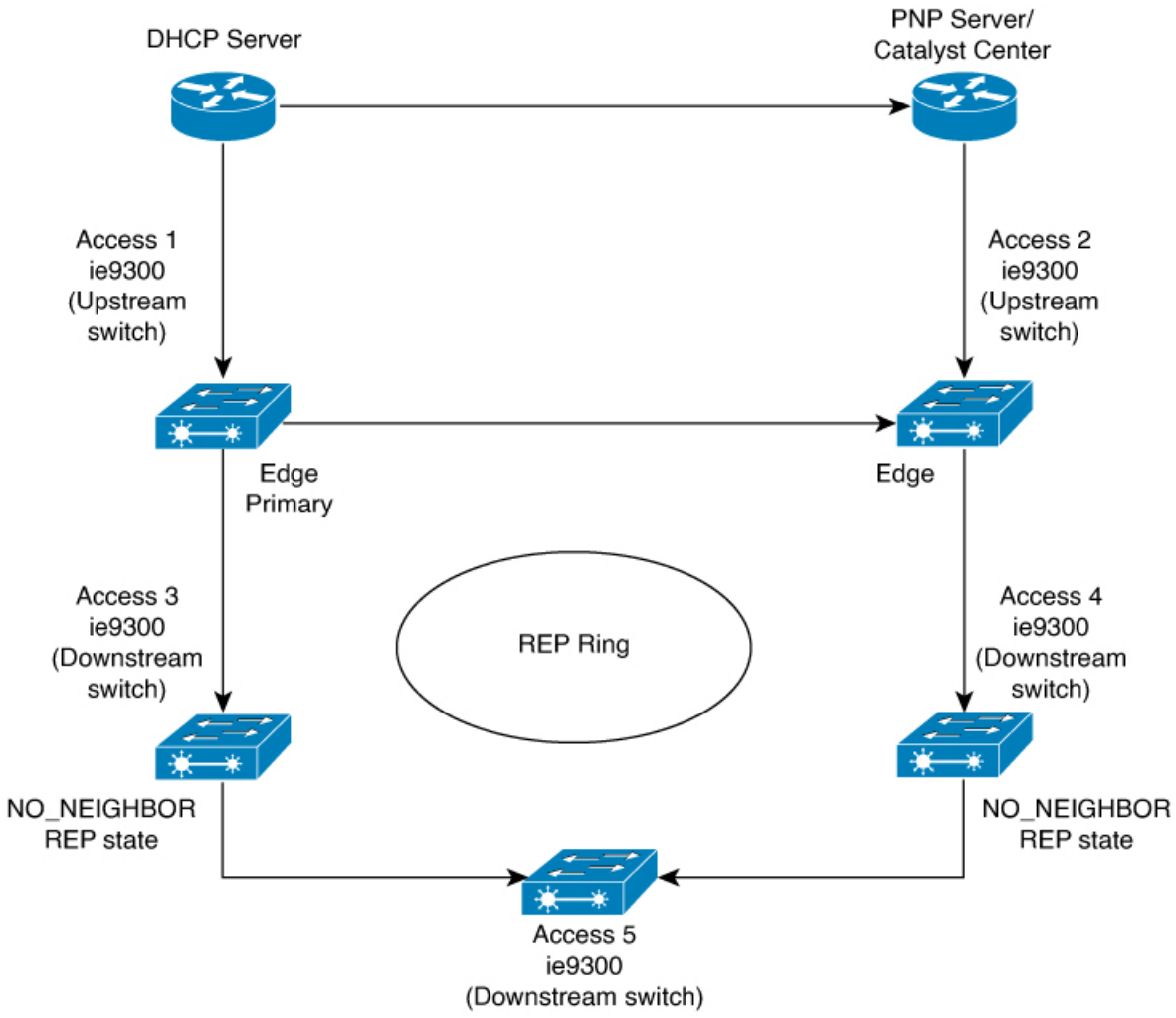

The first set of nodes to be provisioned are Access 1 and Access 2 in the diagram. These are the 2 edge nodes of the REP ring. Note that PnP has configured the downlink port as primary edge on Access 1 and secondary edge on Access 2.

*Figure 12: Adding downstream nodes*




- When Access 3 or Access 4 is powered on, the REP edge primary port initiates negotiation and detects that the neighbor is not REP-enabled.
- Since switches require PnP provisioning via DHCP to join the REP ring, they must first contact the DHCP server. However, an upstream REP port enters the NO_NEIGHBOR state when it fails to discover a REP peer.
- In this NO_NEIGHBOR state, the port blocks all VLAN traffic, preventing the new switch's DHCP discovery messages from reaching the server.
- This blockage stalls the PnP provisioning process and persists for every subsequent switch added to the ring until the initial provisioning issue is resolved.

*Figure 13: NO_NEIGHBOR REP state*




# REP ZTP features

REP ZTP mechanisms are Zero Touch Provisioning protocols for REP rings that

- enables upstream switches to temporarily unblock the PNP startup VLAN for downstream switches during provisioning,
- allows new switches to join a REP ring automatically, and
- requires both upstream and downstream switches to support REP ZTP.

### How REP ZTP works and operational considerations

When a new downstream switch is powered on, it initiates PnP/autoinstall. The upstream switch's interface is configured for REP and blocks the interface to the downstream switch because the downstream switch is not REP by default (the upstream switch is in REP_NO_NEIGHBOR state).

To enable REP ZTP provisioning, follow these steps involving REP LSL packets, TLV signaling, VLAN unblocking, and interface configuration.

- The upstream switch transmits REP LSL packets to the downstream.
- The downstream switch (with REP ZTP enhancement) sends REP LSL packets with a new TLV, signaling an attempt to provision.
- Upon recognizing this TLV, the upstream switch unblocks the PNP startup VLAN for that interface only.
- The downstream switch completes PNP provisioning over the unblocked VLAN.
- Once configuration is complete (including REP enablement), or on failure, the upstream interface returns the PNP VLAN to blocked state.
- To activate this behavior, the upstream switch must have the interface explicitly configured with the **rep ztp-enable** command.
- The PNP startup VLAN is unblocked only on interfaces connected to the downstream joining switch, even if the upstream switch is in multiple REP rings.
- Downstream switches transmit the REP LSL with the new TLV by default when no startup configuration exists.



**Note** For more on configuration, see Configure REP ZTP, on page 75.

# REP segment ID auto-discovery

A REP segment ID auto-discovery feature is a network feature that

- automatically configures and retains segment IDs in REP segments,
- allows switches to learn and store segment ID information through dedicated CLI commands, and
- supports both standard REP and REP Fast protocols starting with Cisco IOS XE 26.1.x or later.

### REP segment ID auto-discovery reference information

REP segment ID auto-discovery reduces manual configuration errors and supports deployments with multiple REP rings by automating segment ID assignment and retention. This feature simplifies the process of adding switches to existing REP segments or creating new ones without manual intervention.

# REP segment ID auto-discovery deployment

REP Segment-ID auto-discovery allows for simplified configuration when adding a switch to a REP segment or creating a new REP segment, reducing manual configuration in both scenarios.

- Auto-discovery can be enabled when adding a switch to an existing REP segment or when building a new segment.
- Manual configuration steps are reduced by using REP segment-ID auto-discovery.

- Deployment order and configuration steps vary depending on whether you are adding a switch, building a new segment, or building a segment with uplinks.

### Add new switch to a REP segment

- When you add a switch to an existing REP segment, use the **rep autodisc** command on the switches connected to the upstream and downstream devices to enable auto-discovery.
- After connecting the new switch, the upstream and downstream switches send Cisco Discovery Protocol (CDP) packets with REP segment ID information to the new switch interfaces.
- Use the **rep segment auto** command on the new switch interfaces. This action allows the interfaces to learn the segment ID.

### Build new REP segment

- When you build a closed REP segment, you must start with a static REP segment ID configuration from an edge device. The primary and secondary edge devices in a closed segment are on the same switch.
- When you build an open REP segment, you must start a static REP segment ID configuration from both primary and secondary edge devices.
- The remaining steps apply to both closed and open REP segments. Begin by bringing up the next node in the REP ring. Then, add a new node between the two switches to enable auto-discovery.

### Build REP segment with uplinks

- When you build a ring segment with uplinks (daisy chain), you must start with a static REP segment ID configuration from the REP edge node. Connect the next device to one of the uplinks to the edge node and enable auto-discovery on the connected uplink. Port pairing support duplicates the REP configuration on the paired uplink port.
- After connecting each device to the uplink, the process repeats to bring the REP segment in a daisy chain manner. Each new REP node joins the ring automatically by learning the REP segment ID from its connected node. In an REP open ring, the last device on the segment acts as an edge device with static REP configuration.

## REP segment ID auto-discovery limitations

- The only supported port-pairing is uplinks Gi1/0/25 - Gi1/0/26, and Gi1/0/27 - Gi1/0/28. The same pairing applies to Ten Gigabit Ethernet (Te) ports.
- If you configure a REP segment on a downlink port, the switch receives the segment ID from the upstream switch and connects the partner downlink port to the same segment. However, the switch does not pass the segment ID to its partner port. As a result, you must configure the partner port of the downlink pair manually.
- This feature does not support the insertion of an edge node into an existing segment. You must configure static or manual REP segment IDs on both the primary and secondary edge devices.
- When inserting a new switch between two existing segment switches, connect the interface of the new switch to the corresponding interfaces on the existing switches that transmit the same segment ID. If you

connect the interfaces incorrectly, the segment will fail. You must meet this requirement when removing a node between two others.

For example, if Gi1/0/1 of switch1 and Gi1/0/2 of switch2 are part of an existing segment, and you insert switch3 between them, ensure that the interfaces connect to Gi1/0/1 of switch1 and Gi1/0/2 of switch2. This approach includes switch3 in the same segment.

- If you configure REP automatically on an interface using the **rep segment auto** command, and later remove the REP configuration with the **no rep segment** or overwrite it with the **rep segment** command, you cannot configure REP automatically again by using the **rep segment auto** command. To restore automatic configuration, shut down the interface, bring it up, and enter the **rep segment** auto command again.
- REP segment ID auto-discovery depends on the CDP protocol. It does not support EtherChannel links.

# REP segments

A segment is a collection of ports that are connected to one another in a chain and configured with a segment ID.

- Each segment is defined by a unique segment ID.
- Ports within a segment are connected in a chain topology.
- Segments require the configuration of primary and secondary edge ports.

### Configuring REP segments and edge ports

To configure REP segments, you must set the REP administrative VLAN (or use the default VLAN 1) and add the desired ports to the segment in interface configuration mode.

Follow these configuration requirements and guidelines:

- Configure the REP administrative VLAN or use VLAN 1 by default.
- Add ports to the segment using interface configuration mode.
- Configure two edge ports in a segment. Assign one port as the primary edge port and the other as the secondary edge port, which is the default setting.
- Only one primary edge port should exist in a segment.
- If two ports are configured as primary edge ports, REP selects one to serve as the segment's primary edge port.
- Optionally, configure the location for segment topology change notices (STCNs) and VLAN load balancing.

# Default REP configurations

A default REP configuration is a network protocol setting that

- disables REP on all interfaces by default, with interfaces acting as regular segment ports unless specifically configured as edge ports,

- sets the initial conditions for VLANs and administrative VLANs (all VLANs blocked, administrative VLAN is VLAN 1, STCNs disabled when REP is enabled), and
- determines the behavior of advanced features, such as VLAN load balancing (manual preemption as default; delay timer disabled) and REP fast or REP ZTP (REP fast disabled; REP ZTP enabled globally and disabled at interface level).
- If VLAN load balancing is not configured, after manual preemption, the system blocks all VLANs on the primary edge port.
- REP fast is disabled by default.
- REP ZTP is enabled by default at the global level, but disabled at the interface level.

# Guidelines and limitations for REP configuration

Follow these guidelines when configuring REP:

- The IE9300 switch supports up to 8 REP segments or 3 REP fast segments starting from IOS-XE release 17.15.2. Earlier releases supported a maximum of 4 REP segments or 3 REP fast segments.
- We recommend starting with one port and then configuring contiguous ports to minimize both the number of segments and blocked ports.
- If more than two ports in a segment fail and no external neighbors are configured, a single port transitions to a forwarding state, maintaining connectivity for the data path during configuration.

  In the **show interfaces rep** command output, the Port Role for this port displays as 'Fail Logical Open', and the Port Role for the other failed port displays as **Fail No Ext Neighbor**. After external neighbors are configured for the failed ports, they transition through alternate port states; they eventually move to an open state or remain as the alternate port, as determined by the alternate port selection mechanism.
- REP ports must be Layer 2 IEEE 802.1Q or trunk ports.
- We recommend that you configure all trunk ports in the segment with the same set of allowed VLANs.
- Use caution when configuring REP over an SSH or Telnet connection. REP blocks all VLANs until another REP interface sends an unblock message. If you enable REP on the same interface used for the SSH or Telnet session, you may lose connectivity to the switch.
- You cannot run REP and STP on the same segment or interface.
- If you connect an STP network to a REP segment, ensure the connection is at the segment edge. Connecting STP to a non-edge location may cause a bridging loop, as STP does not operate on REP segments and all STP BPDUs are dropped at REP interfaces.
- If REP is enabled on two ports of a switch, both ports must be configured as either regular segment ports or edge ports. REP ports must meet these requirements:
  - Only two ports on a switch can be part of the same REP segment.
  - If only one port on a switch is configured in a segment, the port should be an edge port.
  - If two ports on a switch belong to the same segment, they must both be edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and a regular segment port cannot belong to the same segment.

    - If two ports on a switch belong to the same segment, and one is configured as an edge port and the other as a regular segment port (a misconfiguration), the edge port will be treated as a regular segment port.

- REP interfaces initially come up in a blocked state and remain blocked until it is safe to unblock. Monitor interface status to prevent unexpected connection losses.
- REP sends all LSL PDUs in untagged frames on the native VLAN. The BPA message sent to the Cisco multicast address is sent on the administration VLAN, which is VLAN 1 by default.
- You can configure the duration for which a REP interface remains active without receiving a hello from a neighbor. You can use the **rep lsl-age-timer** interface configuration command to set the time range from 120 ms to 10,000 ms. The LSL hello timer is then set to the age-timer value divided by three. In normal operation, three LSL hellos are sent before the age timer on the peer switch expires and checks for hello messages. Only use **rep lsl-age-timer** for non-REP fast copper Gigabit interfaces. All other interfaces do not benefit from **rep lsl-age-timer**.
    - EtherChannel port-channel interfaces do not support LSL age-timer values less than 1000 ms. If you attempt to configure a value below 1000 ms on a port channel, an error message will be displayed, and the command will be rejected.
    - **lsl-age-timer** interface-level command is intended to be used when normal link down detection will be too slow for convergence time.

      FastEthernet and fiber connections do not require the **lsl-age-timer**. Gigabit copper interfaces can use REP fast instead.

- REP ports cannot be configured as any of these port types:
    - Switched Port Analyzer (SPAN) destination port
    - Tunnel port
    - Access port
- REP is supported on EtherChannels, but not on individual ports within an EtherChannel.
- REP ring size is unlimited; however, rings with more than 20 nodes may experience slow convergence.

## Guidelines for REP fast configuration

Follow these guidelines when configuring REP fast:

- You must configure REP fast on both ends of the link in order for the feature to work.
- A REP segment can contain a mix of Gigabit fiber and Gigabit copper. The 50 ms requirement for convergence from a single failure can be achieved if Gigabit copper interfaces have REP fast.
- REP fast can be deployed within a REP segment where not all interfaces support REP fast; however, 50ms convergence may not be guaranteed in such cases.
- Be aware of these limitations:
    - A maximum of three REP segments can have REP fast enabled at the same time.
    - Beginning with release 26.1.1, MACsec can interoperate with both REP and REP fast. Before this release, MACsec interoperated only with REP fast.

- REP fast is not supported in a stacked environment.
- REP fast over EtherChannel is not supported.

## Guidelines for REP ZTP configuration

Follow these guidelines when configuring REP ZTP:

- Ensure that the PnP feature is present on Cisco Catalyst IE9300 Rugged series switches to enable REP ZTP functionality.
- Understand that REP behavior during the NO_NEIGHBOR state is modified beginning in Cisco IOS XE 17.14.1 and later. This change allows a DHCP request message to reach a DHCP server and unblock PnP provisioning of a new switch, with no impact to the REP state machine after PnP completion.
- Apply the changes in REP behavior during the NO_NEIGHBOR state only to REP ZTP in Cisco IOS XE 17.14.1 and later. If the PnP feature is not present, normal REP functionality operates as expected.
- The REP ZTP feature can coexist with the REP bpduleak/negotiated feature on fiber uplink ports.
- Do not use the REP ZTP feature on EtherChannel interfaces for day 0 on an upstream switch, as EtherChannel is not present on the downstream interface by default. REP ZTP operates only on physical interfaces.
- REP ZTP is supported on both copper (downlink) and fiber (uplink) interfaces.
- REP ZTP interoperates only with other IE switching products running IOS XE that claim REP ZTP support.

# Configure the REP administrative VLAN

When a link fails or a VLAN is blocked during load balancing, REP floods packets to a regular multicast address at the HFL. Flooding occurs throughout the entire network. It does not occur only within the REP segment. You can control message flooding by configuring an administrative VLAN.

**Before you begin**

Use these guidelines when configuring the REP administrative VLAN.

- If you do not configure an administrative VLAN, the default is VLAN 1.
- You can configure one admin VLAN on the switch for all segments.
- The administrative VLAN cannot be the RSPAN VLAN.

To configure the REP administrative VLAN, complete these steps.

**Procedure**

**Step 1** Use the **enable** command to enter privileged EXEC mode.

Enter your password if prompted.

**Step 2** Use the **configure terminal** command to enter global configuration mode.

**Step 3** Use the **rep admin vlan** *vlan-id* command to configure the administrative VLAN.

**Example:**

```
Switch(config)# rep admin vlan 2
```

Specifies the administrative VLAN. The range is from 2 to 4094.

**Step 4** (Optional) Use the **no rep admin vlan** command to reset the admin VLAN to the default (1).

**Step 5** Use the **end** command to exit global configuration mode.

**Step 6** (Optional) Use the **show interface** *[ interface-id ]* **rep detail** command to verify REP configuration on the interface.

**Example:**

```
Switch# show interface gigabitethernet1/0/1 rep detail
```

**Step 7** (Optional) Use the **copy running-config startup config** command to save your entries in the switch startup configuration file.

# Configure a REP interface

To configure REP, enable REP on each segment interface and identify the segment ID.

Perform this task to enable and configure REP on IW916x APs using the CLI.

**Before you begin**

Ensure the following prerequisites are met:

- You need interface IDs, segment IDs, and VLAN lists.

**Procedure**

**Step 1** Use the **interface** *interface-id* command to select the interface to configure.

**Example:**

```
Switch(config)#interface gigabitethernet1/0/1
```

Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface).

**Step 2** Use the **switchport mode trunk** command to configure the interface as a Layer 2 trunk port.

**Step 3** Use the **rep segment** *segment-id* [**edge** [**no-neighbor** | **primary**] | **preferred**] command to enable REP on the interface and identify segment parameters.

The segment ID range is from 1 to 1024.

**Example:**

```
Switch(config-if)# rep segment 10
```

**Note**
You must configure both a primary edge port and a secondary edge port on each segment.

These optional keywords are available:

- (Optional) **edge** : Configures the port as an edge port. Each segment has only two edge ports. Entering the keyword **edge** without the keyword **primary** configures the port as the secondary edge port.

  ```
  Switch(config-if)# rep segment 10 edge
  ```

- (Optional) **no-neighbor** : Configures a port with no external REP neighbors as an edge port. The port inherits all the properties of an edge port, and you can configure the properties the same way you do for an edge port.

  ```
  Switch(config-if)# rep segment 10 edge no-neighbor
  ```

- (Optional) **primary** : Configures the port as the primary edge port, the port on which you can configure VLAN load balancing.

  ```
  Switch(config-if)# rep segment 10 edge primary
  ```

  **Note**
  Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the keyword **primary** on both the switches, the configuration is valid. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by entering the **show rep topology** command in privileged EXEC mode.

- (Optional) **preferred** : Indicates that the port is the preferred alternate port or the preferred port for VLAN load balancing.

  ```
  Switch(config-if)# rep segment 10 preferred
  ```

  **Note**
  Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives the port a slight edge over equal contenders. The alternate port is usually a previously failed port.

**Step 4** (Optional) Use the **rep stcn** [**interface** *interface-id* |**segment** *id-list* | **stp**] command to configure STCNs as needed.

These keywords are available:

- **interface** *interface-id*: Designates a physical interface or port channel to receive STCNs.

  ```
  Switch(config-if)# rep stcn interface GigabitEthernet1/0/48
  ```

- **segment** *id-list* : Identifies one or more segments to receive STCNs. The range is from 1 to 1024.

  ```
  Switch(config-if)# rep stcn segment 10, 20
  ```

- **stp** : Sends STCNs to STP networks.

  ```
  Switch(config-if)# rep stcn stp
  ```

**Note**
Multiple Spanning Tree (MST) mode is required on edge no-neighbor nodes when **rep stcn stp** command is configured for sending STCNs to STP networks.

**Step 5** (Optional) Use the **rep block port** [**id** *port-id* | *neighbor-offset* | **preferred**] **vlan** [*vlan-list* | **all**] command to configure VLAN load balancing on the primary edge port.

**Example:**

```
Switch(config-if)# rep block port id 0009001818D68700 vlan 1-100
```

Identifies the REP alternate port in one of three ways ( **id** *port-id*, *neighbor_offset*, **preferred**), and configures the VLANs to be blocked on the alternate port.

These keywords are available to configure VLAN load balancing:

- **id** *port-id*: Identifies the alternate port by port ID. The port ID is automatically generated for each port in the segment. You can view interface port IDs by entering the **show interface** *type number* **rep** [**detail**] privileged EXEC command.
- *neighbor_offset*: Number to identify the alternate port as a downstream neighbor from an edge port. The range is from -256 to 256, with negative numbers indicating the downstream neighbor from the secondary edge port. A value of **0** is invalid. Enter **-1** to identify the secondary edge port as the alternate port.

  **Note**
  When you enter the **rep block port** command at the primary edge port (offset number 1), you cannot enter an offset value of 1 to identify an alternate port.

- **preferred** : Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing.
- **vlan** *vlan-list*: Blocks one VLAN or a range of VLANs.
- **vlan all**: Blocks all the VLANs.

**Note**
Enter this command only on the REP primary edge port.

**Step 6** (Optional) Use the **rep preempt delay** *seconds* command to set a pre-empt delay for VLAN load balancing.

**Example:**

```
Switch(config-if)#rep preempt delay 100
```

- Use this command if you want VLAN load balancing to be automatically triggered after a link failure and recovery.
- The time delay range is between 15 to 300 seconds. The default is manual pre-emption with no time delay.

**Note**
Enter this command only on the REP primary edge port.

**Step 7** (Optional) Use the **rep lsl-age-timer** *value* command to configure the REP interface aging timer.

**Example:**

```
Switch(config-if)#rep lsl-age-timer 2000
```

Configures a time (in milliseconds) for which the REP interface remains up without receiving a hello from a neighbor.

The range is from 120 to 10,000 ms in 40-ms increments. The default is 5000 ms (5 seconds).

**Note**
- EtherChannel port channel interfaces do not support LSL age-timer values that are less than 1000 ms.
- Ensure that both the ports on the link have the same LSL age configured in order to avoid link flaps.

**Step 8** Use the **end** command to exit global configuration mode and returns to privileged EXEC mode.

**Step 9** (Optional) Use the **show interface** [*interface-id*] **rep** [**detail**] command to displays the REP interface configuration.

**Example:**

```
Switch# show interface gigabitethernet1/0/1 rep detail
```

# Manually trigger VLAN load balancing on a segment

To manually trigger VLAN load balancing on a specified segment using the CLI, especially when no preemption delay is configured.

If you do not configure a preemption time delay using the **rep preempt delay** *seconds* interface configuration command on the primary edge port, VLAN load balancing must be triggered manually on the segment by default. Complete all other segment configurations before manually triggering VLAN load balancing. A confirmation message appears when you use the **rep preempt delay segment** *segment-id* command, as preemption can cause network disruption.

**Before you begin**

- Ensure you have completed all other segment configuration steps.
- Make sure you are at the device CLI with appropriate privileges.

**Procedure**

**Step 1** Use the **enable** command to enable the privileged EXEC mode.

Enter your password if prompted.

**Step 2** Use the **rep preempt segment** *segment-id* command to manually trigger VLAN load balancing on the segment.

**Example:**

```
Switch# rep preempt segment 100
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]
```

You need to confirm the command before it is executed.

**Step 3** (Optional) Use the **show rep topology segment** *segment-id* command to view the current REP topology information for the specified segment.

**Example:**

```
Switch# show rep topology segment 100
```

**Step 4** Use the **end** command to exit configuration mode and return to privileged EXEC mode.

# Configure SNMP Traps for REP

You can configure a switch to send REP-specific traps to notify the Simple Network Management Protocol (SNMP) server of link-operational status changes and port role changes.

**Procedure**

**Step 1** Use the **enable** command to enable privileged EXEC mode.

Enter your password if prompted.

**Step 2** Use the **configure terminal** command to enter global configuration mode to make changes to device settings.

**Step 3** Use the **snmp mib rep trap-rate** *value* command to enable the switch to send REP traps and sets the number of traps sent per second.

**Example:**

```
Switch(config)# snmp mib rep trap-rate 500
```

Enter the number of traps sent per second. The range is 0 to 1000. The default value is 0, which means no limit is imposed and a trap is sent at every occurrence.

**Step 4** Use the **end** command to return to privileged EXEC mode.

**Step 5** (Optional) Use the **show running-config** command to view the running configuration, which can be used to verify the REP trap configuration.

**Step 6** (Optional) Use the **copy running-config startup-config** command to save your entries in the switch startup configuration file.

# Configure REP ZTP

To configure REP ZTP, you enable or disable it at the global level and the interface level. The default states are:

- Global level: Enabled
- Interface level: Disabled

You must explicitly enable the feature at the interface level on the upstream device interface connected to the downstream device. When enabled, only that interface will receive notification from the downstream switch to block or unblock the PnP startup VLAN.



**Note** When applying configuration from DNAC or a PNP server, the user must explicitly add this CLI command to the configuration template to enable the feature.

**Procedure**

**Step 1** Use the **configure terminal** command to enter the global configuration mode.

**Step 2** Use the **rep ztp** command to globally enable the REP ZTP.

**Note**
Use the **no rep ztp** command to disable REP ZTP.

**Step 3** Use the **interface** *interface-name* command to enter interface configuration mode on the upstream device interface that is connected to the downstream device.

**Example:**

```
Switch(config)# interface GigabitEthernet1/0/1
```

**Step 4** Use the **rep ztp-enable** command to enable REP ZTP on the interface.

**Note**
Use the **no rep ztp-enable** command to disable REP ZTP on the interface.

The following example shows the minimum configuration required to enable the REP ZTP feature on the upstream device interface that is connected to a downstream device.

```
Switch#show running-config interface gigabitEthernet 1/0/1
Building configuration...
Current configuration : 93 bytes
!
interface GigabitEthernet1/0/1
switchport mode trunk
rep segment 100
rep ztp-enable
end
```

# Configure REP segment ID auto-discovery

Perform this task during new REP ring deployments, during ring expansions, or when you want to minimize manual configuration steps. Completing this process simplifies ring deployments and speeds up the work.

**Before you begin**

- Verify that your switch model and software version support REP segment ID auto-discovery. To confirm support, enter **rep ?** in global configuration mode and verify that **rep-auto-discovery** appears in the help output.
- Identify the devices to configure as edge nodes. These nodes require static configuration.
- Ensure that CDP is enabled on all devices.

Perform these steps to configure REP segment ID auto-discovery:

**Procedure**

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Step 2** Use the **rep autodisc** command to configure REP auto discovery.

**Note**
Use the **no rep autodisc** command to disable the REP segment ID.

**Step 3** Use the **interface** *interfacename interface-id* command to enter the interface configuration mode.

**Example:**

```
Switch(config)# interface GigabitEthernet1/0/1
```

**Step 4** Use the **rep segment auto** command to enable auto-discovery on an interface that participates in the REP ring.

**Note**
Use the **no rep segment** command to disable auto-discovery.

**Step 5** Use the **rep segment** *segment-id* **edge** command to configure static REP on edge nodes with static REP segment ID.

**Example:**

```
Switch(config-if)# rep segment 100 edge
```

**Step 6** (Optional) Use the **show interfaces rep detail** command to check the status of REP segment ID auto-discovery on the segment.

**Example:**

This example shows that the REP segment ID auto-discovery is globally enabled on a device.

```
Switch# show interfaces rep detail
REP Segment Id Auto Discovery Status: Enabled
```

This example shows that the REP segment ID auto-discovery is globally disabled on a device.

```
Switch# show interfaces rep detail
REP Segment Id Auto Discovery Status: Disabled
```

This example shows that the REP segment ID on the interface is configured automatically.

```
Switch# show interfaces rep detail
REP Segment Id Type: Auto
```

This example shows that the REP segment ID on the interface is configured manually.

```
Switch# show interfaces rep detail
REP Segment Id Type: Manual
```

# Preventive best practices

## Control-plane load governance

Ensure overall control-plane load is kept within safe limits to avoid interference with critical protocols such as REP, BFD, and PTP.

- Configure monitoring tools and SNMP polling intervals conservatively to prevent excessive CPU utilization.
- Account for concurrent CPU-intensive features, such as high-frequency SNMP polling, PTP traffic bursts, and BFD sessions, especially during topology changes or reconvergence events.
- Operate devices on stable and recommended software releases to benefit from validated fixes, performance improvements, and resiliency enhancements.

## PTP and topology change stabilization

- Reduce transient CPU spikes that timing and topology adjustments can cause.
- Allow sufficient stabilization time for PTP after topology changes to reduce short-term CPU utilization increases.
- Avoid overlapping PTP adjustments with REP reconvergence or other CPU-intensive events.

## REP design and operational planning

Design and operate REP with simplicity and predictability to minimize control-plane impact.

- Design REP rings only when operationally necessary. Avoid excessive, overlapping, or unnecessary rings that can increase reconvergence time and CPU load.
- Review and tune REP timing parameters, such as **rep preempt delay**, to align with resiliency goals and operational requirements.
- Plan configuration changes, maintenance windows, and REP topology modifications carefully to avoid multiple simultaneous control-plane events.

## CPU monitoring and diagnostics

Continuously monitor system health to detect and mitigate CPU stress early.

- Monitor CPU utilization trends, particularly during REP convergence, power events, and maintenance activities.
- Periodically review system logs and resource utilization for recurring or sustained CPUHOG events linked to REP or other control-plane processes.
- Enable and retain sufficient logging and diagnostic data to support effective troubleshooting during abnormal conditions.

## Recommended operational checks

Use these commands to monitor system state and collect diagnostic information.

- **show processes cpu sorted**
- **show platform resource**
- **show rep topology**
- **show logging**
- **show tech-support**

# Monitoring REP configurations

This topic provides examples of REP monitoring command output. The examples show configuration and status details for uplink and downlink ports as well as segment topology information.

This section provides example outputs for the **show interface** [ *interface-id* ] **rep** [ **detail** ] command. The output shows REP configuration and status on both uplink and downlink ports.

The **show interface** [ *interface-id* ] **rep** [ **detail** ] command output demonstrates the REP configuration and status on a uplink port.

```
 Device# show interfaces GigabitEthernet1/0/4 rep detail
GigabitEthernet1/0/4 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
```

```
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

The **show interface** [ *interface-id* ] **rep** [ **detail** ] command output demonstrates the REP configuration and status on a downlink port.

```
Device# show interface GigabitEthernet1/0/5 rep detail
GigabitEthernet1/0/5   REP enabled
Segment-id: 1 (Segment)
PortID: 019B380E4D9ACAC0
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 019B380E4D9ACAC0696B
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Disabled
Preempt Delay Timer: 100 sec
LSL Ageout Timer: 2000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: 09E9380E4D9ACAC0
Configured Load-balancing Block VLAN: 1-100
STCN Propagate to: segment 25
LSL PDU rx: 292, tx: 340
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

This section provides an example output for the **show rep topology** [ **segment** *segment-id* ] [**archive** ] [ **detail** ] command. The output displays REP topology information for all segments.

```
Device# show rep topology
REP Segment 1
BridgeName       PortName     Edge Role
---------------- ----------   ---- ----
10.64.106.63     Gi1/0/4      Pri  Open
10.64.106.228    Gi1/0/4           Open
10.64.106.228    Gi1/0/3           Open
10.64.106.67     Gi1/0/3           Open
10.64.106.67     Gi1/0/4           Alt
10.64.106.63     Gi1/0/4      Sec  Open
```

```
REP Segment 3
BridgeName       PortName     Edge Role
---------------- ----------   ---- ----
10.64.106.63     Gi1/011     Pri  Open
SVT_3400_2       Gi1/0/3           Open
SVT_3400_2       Gi1/0/4           Open
10.64.106.68     Gi1/0/2           Open
10.64.106.68     Gi1/0/1           Open
10.64.106.63     Gi1/0/2      Sec  Alt
```

# Check the REP ZTP status

Use the **show** command to identify the state of REP ZTP on an interface. In this example, REP ZTP is disabled on interface GigabitEthernet 1/0/1 and enabled on interface GigabitEthernet 1/0/2.

### Procedure

**Step 1** Use the **show interfaces rep detail** command in the privileged exec mode.

**Example:**

```
GigabitEthernet1/0/1 REP enabled
Segment-id: 100 (Segment)
PortID: 00016C13D5AC4320
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 00026C13D5AC43209DAB
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1

REP-ZTP Status: Disabled
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 382, tx: 297
HFL PDU rx: 0, tx: 0
BPA TLV rx: 1, tx: 19
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 95, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 95, tx: 95
GigabitEthernet1/0/2 REP enabled
Segment-id: 100 (Segment)
PortID: 00026C13D5AC4320
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 00026C13D5AC43209DAB
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Enabled
```

```
REP-ZTP PnP Status: Unknown
REP-ZTP PnP Vlan: 1
REP-ZTP Port Status: Blocked

REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 11, tx: 11
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

**Step 2** Use the **show interfaces rep detail** command to monitor the status of **REP ZTP**.

When the downstream device is booted up, it sends notification to the connected upstream switch interface, which unblocks the **pnp_startup_vlan** so the device can obtain a DHCP IP address and establish communication with the PNP server or DNAC. The show command indicates the status as Unblocked.

These syslogs on the upstream switch notify you about FWD and BLK of ports. There are no syslogs in the downstream switch as PnP takes control of the console and no syslogs can be printed on the console.

```
REP-6-ZTPPORTFWD: Interface GigabitEthernet1/0/2 moved to forwarding on ZTP notification
```

```
REP-6-ZTPPORTBLK: Interface GigabitEthernet1/0/2 moved to blocking on ZTP notification
```

**Example:**

```
Switch#show interfaces rep detail
GigabitEthernet1/0/1 REP enabled
Segment-id: 100 (Segment)
PortID: 00016C13D5AC4320
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 00026C13D5AC43209DAB
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 430, tx: 358
HFL PDU rx: 0, tx: 0
BPA TLV rx: 1, tx: 67
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 107, tx: 0
```

```
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 107, tx: 108

GigabitEthernet1/0/2 REP enabled
Segment-id: 100 (Segment)
PortID: 00026C13D5AC4320
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 00026C13D5AC43209DAB
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Enabled
REP-ZTP PnP Status: In-Progress
REP-ZTP PnP Vlan: 69
REP-ZTP Port Status: Unblocked
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 32, tx: 40
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

**Step 3** Use the **show platform hardware l2 stp** command to check the interface state of the PnP startup VLAN.

**Example:**

```
Switch#show platform hardware l2 stp asic-num 0 vlan-id 69 □[PnP Vlan]
------------------------STP TABLE START------------------------
---------------------------------------------------------------
VlanId:1 StpId:0 MemberPort:3 StpState:FORWARDING
VlanId:1 StpId:0 MemberPort:7 StpState:FORWARDING
VlanId:1 StpId:0 MemberPort:25 StpState:FORWARDING
---------------------------------------------------------------
------------------------STP TABLE END-------------------------
```

**Step 4** (Optional) Use these debug commands to troubleshoot REP ZTP.

- **debug rep lslsm** : This command helps you understand LSL state machine events in the NO_NEIGHBOR state.
- **debug rep packet** : Use this command to dump LSL packets with the REP ZTP LSL TLV to check the PnP status on the peer client node.

# PTP over REP

PTP over REP is a time synchronization solution that:

- combines Precision Time Protocol (PTP) with Resilient Ethernet Protocol (REP),

- provides accurate and predictable time synchronization in ring and linear Layer 2 topologies, and
- maintains timing continuity during link or node failures in industrial networks.

PTP over REP is essential for environments that require accurate timing for applications such as motion control, protection relays, and distributed control systems. It also ensures that network resiliency does not cause timing reconvergence events that disrupt these applications.

REP ensures rapid topology recovery, while PTP maintains synchronization accuracy across the restored topology.

### Use cases

Common PTP over REP use cases include:

- An industrial ring network that uses REP for fast failover and PTP to synchronize controllers and field devices.
- A linear REP topology that connects network nodes in industrial environments where precise time alignment is required for monitoring and protection applications.

# Guidelines for PTP over REP

- Each Boundary Clock (BC) introduces additional delay at every hop.
- Transparent Clock (TC) deployments minimize per-hop delay contribution. TCs are limited to a single VLAN.
- PTP over REP supports both standard REP and REP Fast. When using REP Fast, configure REP Fast on all ports in the ring. Do not mix standard REP and REP Fast within the same ring.

# PTP clock types profiles and their accuracy

***Table 5: PTP clock types, profiles, and their accuracy***

| Platforms | PTP clock type | PTP profile | PTP accuracy | Number of REP rings |
|---|---|---|---|---|
| Cisco Catalyst IE9300 Rugged Series Switch | • Boundary Clock<br>• Grandmaster Boundary Clock<br>• Transparent Clock | Default (IEEE 1588 v2), Power 2011/2017 | Boundary Clock (BC): ~200 ns per hop<br>Transparent Clock (TC): ~50 ns per hop | Up to 26 open REP segments |

| Platforms | PTP clock type | PTP profile | PTP accuracy | Number of REP rings |
|---|---|---|---|---|
| Cisco IE3500 Rugged Series Switch | • Boundary Clock<br>• Grandmaster Boundary Clock<br>• Transparent Clock | Default Profile (IEEE 1588 v2), Power Profile 2011/2017 | Boundary Clock (BC): ~200 ns per hop<br>Transparent Clock (TC): < 200 ns per hop | Up to 26 open REP segments or 3 REP Fast segments |

**Note**

- End-to-end accuracy depends on the cumulative delay introduced by the number of BCs and TCs in the network path.
- The stated PTP accuracy values do not apply when GLC-T copper SFP transceivers are used in the timing path because these transceivers can reduce PTP timing accuracy.

***Table 6: PTP over REP capabilities***

| Category | Support |
|---|---|
| PTP clocks | • Boundary Clock<br>• Grandmaster Clock<br>• Transparent Clock |
| PTP profiles | • Default (IEEE 1588 v2)<br>• Power Profile 2011/2017 (platform-dependent) |
| Media | • Copper ports<br>• SFP-based fiber ports |
| REP topology | • Ring topologies<br>• Linear topologies<br>• Up to 26 REP rings |
| VLAN behavior | • Boundary Clocks support multiple VLANs.<br>• Transparent Clocks support a single VLAN. |

# Configure PTP over REP

You can configure PTP over REP using either of the following profiles:

- Configure PTP over REP using default profile
- Configure PTP over REP using power profile

## Configure REP

Configures REP on switch interfaces to enable ring topology and PTP packet transport by setting the administrative VLAN and segment membership for ring ports.

### Procedure

**Step 1** Create and activate VLAN:

a) Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Switch# configure terminal
```

b) Use the **vlan** *vlan-id* command to create VLAN configuration on the switch, which serves as both the REP administrative VLAN and the PTP transport VLAN.

**Example:**

```
Switch(config)# vlan 100
```

c) (Optional) Use the **no shutdown** command in VLAN configuration mode to ensure that VLAN is administratively enabled.

**Example:**

```
Switch(config-vlan)# no shutdown
```

**Note**
This command applies to the Layer 2 VLAN and not an SVI. It helps clear an existing `lshut` state in a brownfield network.

The **lshut** status means that the VLAN is locally shut down.

d) Use the **exit** command to return to global configuration mode.

**Example:**

```
Switch(config-vlan)# exit
```

**Step 2** Configure REP on interface:

a) Use the **interface** *interface-id* command to configure the interface.

**Example:**

```
Switch(config)# interface GigabitEthernet1/3
```

b) Use the **switchport mode trunk** command on the interface to set the first ring-facing port to trunk mode, allowing VLAN-tagged traffic including PTP packets to pass through.

**Example:**

```
Switch(config-if)# switchport mode trunk
```

c) Use the **switchport trunk allowed vlan** *vlan-id* command to explicitly permit VLAN on the trunk, ensuring PTP messages are not blocked by VLAN filtering.

**Example:**

```
Switch(config-if)# switchport trunk allowed vlan 100
```

d) Use the **rep segment** *segment-id* command to add interface as a non-edge member, enabling it to participate in the resilient ring topology and carry PTP packets.

**Example:**

```
Switch(config-if)# rep segment 10
```

e) Use the **no shutdown** command to enable the interface.

**Example:**

```
Switch(config-if)# rep segment 10
```

f) Use the **exit** command to return to global configuration mode.

**Example:**

```
Switch(config-if)# exit
```

g) Use the **rep admin vlan** *vlan-id* command to configure VLAN as the REP administrative VLAN to ensure REP control messages and PTP packets share the same VLAN and are not filtered.

**Example:**

```
Switch(config)# rep admin vlan 100
```

Repeat step 2 to configure REP on the second interface.

**Step 3** (Optional) Use the **show rep topology** command to verify that the switch ports appear in REP segmen topology with `Open` state before proceeding with PTP configuration.

**Example:**

```
Switch# show rep topology
REP Segment 10

BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
RB1              Gi4/0/7    Pri  Open
Switch           Gi1/3           Open
Switch           Gi1/4           Open
RB2              Gi2/0/7         Open
RB2              Gi2/0/8         Alt
LANB-1           Gi1/4           Open
LANB-1           Gi1/3           Open
RB1              Gi4/0/8    Sec  Open
```

## Configure PTP over REP using power profile

Configure PTP over REP using the power profile to enable precise time synchronization across industrial ring topologies.

**Before you begin**

Ensure REP is configured.

### Procedure

**Step 1** Clear the existing PTP configuration.

a) Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Switch# configure terminal
```

b) Use the **no ptp profile** command to remove any existing PTP profile configuration before applying a new one.

**Example:**

```
Switch(config)# no ptp profile
```

c) Use the **no ptp mode** command to remove any existing PTP mode configuration on the switch.

**Example:**

```
Switch(config)# no ptp mode
```

d) Use the **no ptp domain** command to remove any existing PTP domain configuration on the switch.

**Example:**

```
Switch(config)# no ptp domain
```

**Step 2** Configure REP on an interface.

a) Use the **interface** *interface-id* command to configure the interface.

**Example:**

```
Switch(config)# interface GigabitEthernet1/3
```

b) Use the **rep segment** *segment-id* command to add the interface as a non-edge member, enabling it to participate in the resilient ring topology and carry PTP packets.

**Example:**

```
Switch(config-if)# rep segment 10
```

c) Use the **exit** command to return to global configuration mode.

**Example:**

```
Switch(config-if)# exit
```

Repeat step 2 to configure REP on the second interface.

**Step 3** Configure PTP power profile, mode, and domain.

a) Use the **ptp profile power** command to configure the power profile on the switch.

**Example:**

```
Switch(config)# ptp profile power
```

b) Use the **ptp mode p2ptransparent** command to configure the switch as a peer-to-peer Transparent Clock (TC) under the power profile.

**Example:**

```
Switch(config)# ptp mode p2ptransparent
```

c) Use the **ptp domain** *domain-number* command to assign the switch to PTP domain, ensuring it participates in the correct PTP synchronization domain.

**Example:**

```
Switch(config)# ptp domain 100
```

**Step 4** Use the **interface** *interface-id* command to configure the first REP ring-facing interface and enter interface configuration mode.

**Example:**

```
Switch(config)# interface GigabitEthernet1/3
```

**Step 5** Use the **ptp vlan** *vlan-id* command on the interface to bind PTP operation to VLAN on the first REP ring-facing interface.

**Example:**

```
Switch(config-if)# ptp vlan 100
```

**Step 6** Use the **exit** command to return to global configuration mode.

**Example:**

```
Switch(config-if)# exit
```

Repeat steps 4 to 6 to configure PTP VLAN on the other ring-facing interface.

**Step 7** Verify the REP configuration.

**Example:**

```
Switch# show rep topology
REP Segment 10

BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
RB1              Gi4/0/7    Pri  Open
Switch           Gi1/3           Open
Switch           Gi1/4           Open
RB2              Gi2/0/7         Open
RB2              Gi2/0/8         Alt
LANB-1           Gi1/4           Open
LANB-1           Gi1/3           Open
RB1              Gi4/0/8    Sec  Open
```

## Configure PTP over REP using default profile

Configure PTP over REP using the default profile to enable precise time synchronization across industrial ring topologies.

**Before you begin**

Ensure REP is configured.

**Procedure**

**Step 1** Use these commands to clear the existing PTP configuration:

a) Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Switch# configure terminal
```

b) Use the **no ptp profile** command to remove any existing PTP profile configuration before applying a new one.

**Example:**

```
Switch(config)# no ptp profile
```

c) Use the **no ptp mode** command to remove any existing PTP mode configuration on the switch.

**Example:**

```
Switch(config)# no ptp mode
```

d) Use the **no ptp domain** command to remove any existing PTP domain configuration on the switch.

**Example:**

```
Switch(config)# no ptp domain
```

**Step 2** Configure REP on an interface:

a) Use the **interface** *interface-id* command to select the interface and enter interface configuration mode.

**Example:**

```
Switch(config)# interface GigabitEthernet1/3
```

b) Use the **rep segment** *segment-id* command to add the interface as a nonedge member, enabling it to participate in the resilient ring topology and carry PTP packets.

**Example:**

```
Switch(config-if)# rep segment 10
```

c) Use the **exit** command to return to global configuration mode.

**Example:**

```
Switch(config-if)# exit
```

Repeat step 2 to configure REP on the second interface.

**Step 3** Configure PTP mode and domain:

a) Use the **ptp mode e2etransparent** command to configure the switch as an end-to-end Transparent Clock (TC).

**Example:**

```
Switch(config)# ptp mode e2etransparent
```

b) Use the **ptp domain** *domain-number* command to assign the switch to PTP domain, ensuring it participates in the correct PTP synchronization domain.

**Example:**

```
Switch(config)# ptp domain 100
```

c) Use the **end** command to return to privileged EXEC mode.

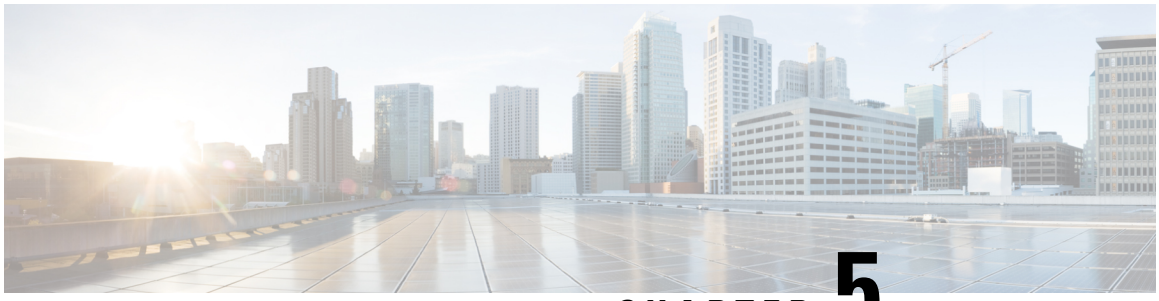
**Example:**

```
Switch(config)# end
```

**Step 4** (Optional) Use the **show rep topology** command to verify the REP configuration.

**Example:**

```
Switch# show rep topology
REP Segment 10
BridgeName   PortName   Edge   Role
------------ ---------- ----   ----
RB1          Gi4/0/7    Pri    Open
Switch       Gi1/3              Open
Switch       Gi1/4              Open
RB2          Gi2/0/7            Open
RB2          Gi2/0/8            Alt
LANB-1       Gi1/4              Open
LANB-1       Gi1/3              Open
RB1          Gi4/0/8    Sec    Open
```



CHAPTER 5

# FlexLink+

FlexLink+ provides enhanced redundancy and rapid failover for network links, ensuring continuous traffic flow in case of link failure.


- FlexLink+ redundancy functions, on page 91
- Guidelines and restrictions, on page 92
- Configure active port for Flex Link+, on page 92
- Configure standby port for FlexLink+, on page 93
- Configure VLAN load balancing on FlexLink+, on page 94
- Configure time for VLAN load balancing on FlexLink+, on page 95
- Configure manual preemption for VLAN load balancing on FlexLink+, on page 95
- Configure FlexLink+ topology change messages, on page 96


# FlexLink+ redundancy functions

FlexLink+ is a Layer 2 redundancy feature that

- provides a pair of interfaces where one acts as a backup to the other
- offers an alternative to the Spanning Tree Protocol (STP) for simple link redundancy, and
- supports switchover on both physical interfaces and EtherChannel bundles.

FlexLink+ provides redundancy by using one Layer 2 link as primary and another as backup. It can also improve bandwidth through VLAN load balancing, letting both links forward traffic at the same time for different VLANs while still maintaining redundancy.

In load balancing mode, both ports forward traffic for separate VLANs simultaneously, which boosts bandwidth and maintains redundancy.

*Table 7: Feature history*

| Feature name | Release information | Description |
|---|---|---|
| FlexLink+ | 26.2.1 | This feature provides link redundancy between Layer 2 interfaces without requiring Spanning Tree Protocol. It supports failover for active-standby configurations, VLAN load balancing across links, automatic or manual preemption, and physical interfaces or port channels.<br>FlexLink+ is ideal for industrial networks requiring simple, reliable uplink redundancy with minimal configuration complexity. |

# Guidelines and restrictions

## Guidelines

- Use the **spanning-tree portfast trunk** command on uplink interfaces connected to FlexLink+ ports to bypass STP listening and learning states.
- Enable either MSTP or Rapid PVST on upstream switches for networks that extend across a FlexLink+ node to prevent traffic blackholing. For more information abour configuring MSTP, refer Configuring Multiple Spanning-Tree Protocol and for more information about configuring Rapid PVST, refer Spanning-Tree Interoperability and Backward Compatibility.

## Restrictions

- FlexLink+ supports physical Layer 2 interfaces and EtherChannel.
- VLAN load balancing requires the edge port to terminate the segment.

# Configure active port for Flex Link+

Define the primary (active) interface in a FlexLink+ pair.

**Before you begin**

Configure the node connected to the FlexLink+ active link as the root bridge.

**Procedure**

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Switch# configure terminal
```

**Step 2** Use the **interface** *interface-id* command to enter interface configuration mode.

**Example:**

```
Switch(config)# interface GigabitEthernet1/0/1
```

**Step 3** Use the **switchport trunk allowed vlan** *vlan-list* command to configure the allowed VLANs on the interface.

**Example:**

```
Switch(config-if)# switchport trunk allowed vlan 10 20
```

**Step 4** Use the **switchport mode trunk** command to set the interface to trunk mode.

**Example:**

```
Switch(config-if)# switchport mode trunk
```

**Step 5** Use the **rep segment** *segment-id* **edge no-neighbor primary** command to define the port as the primary edge port.

**Example:**

```
Switch(config-if)# rep segment 2 edge no-neighbor primary
```

# Configure standby port for FlexLink+

Define the standby interface in a FlexLink+ pair.

**Procedure**

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Switch# configure terminal
```

**Step 2** Use the **interface** *interface-id* command to specify the interface.

**Example:**

```
Switch(config)# interface GigabitEthernet1/0/1
```

**Step 3** Use the **switchport trunk allowed vlan** *vlan-list* command to configure the allowed VLANs on the interface.

**Example:**

```
Switch(config-if)# switchport trunk allowed vlan 10 20
```

**Step 4** Use the **switchport mode trunk** command to set the interface to trunk mode.

**Example:**

```
Switch(config-if)# switchport mode trunk
```

**Step 5** Use the **rep segment** *segment-id* **edge no-neighbor preferred** command to define the port as the standby edge port.

**Example:**

```
Switch(config-if)# rep segment 2 edge no-neighbor preferred
```

The **preferred** keyword influences which port becomes the blocking port, but the system selects the actual blocking port according to the timing of link state changes, such as when a port comes up later.

# Configure VLAN load balancing on FlexLink+

This procedure enables traffic distribution across a FlexLink+ pair.

**Procedure**

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Switch# configure terminal
```

**Step 2** Use the **interface** *interface-id* command to enter interface configuration mode.

**Example:**

```
Switch(config)# interface GigabitEthernet1/0/1
```

**Step 3** Use the **rep block port** *port-number* **vlan** *vlan-id* command to define the VLANs that are blocked on the standby port.

**Example:**

```
Switch(config-if)# rep block port 2 vlan 1-50
```

This command blocks VLANs 1 to 50 on the standby port, which means these VLANs remain active on the primary port.

**Step 4** Use the **switchport mode trunk** command to set the interface to trunk mode.

**Example:**

```
Switch(config-if)# switchport mode trunk
```

**Step 5** Use the **exit** command to exit interface configuration mode.

**Example:**

```
Switch(config-if)# exit
```

**Step 6** Use the **interface** *interface-id* command to access the standby interface configuration.

**Example:**

```
Switch(config)# interface GigabitEthernet1/1
```

**Step 7** Use the **rep segment** *segment-id* **edge no-neighbor** command to confirm the standby interface role in the segment.

**Example:**

```
Switch(config)# rep segment 10 edge no-neighbor
```

# Configure time for VLAN load balancing on FlexLink+

You can configure the time to trigger VLAN load balancing automatically after a link recovers. For more information about preempt delay, see VLAN load balancing.

This configuration is valid on the primary edge port only.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Switch# configure terminal
```

**Step 2** Use the **interface** *interface-id* command to enter interface configuration mode.

**Example:**

```
Switch(config)# interface GigabitEthernet1/0/1
```

**Step 3** Use the **rep preempt delay** *seconds* command to configure the preemption delay time.

**Example:**

```
Switch(config-if)# rep preempt delay 100
```

The valid range for the delay value is 15 to 300 seconds.

# Configure manual preemption for VLAN load balancing on FlexLink+

Manual preemption defines the process for manually restoring the configured VLAN load balancing state on a segment.

Configure manual preemption as described in the following procedure. For more information about VLAN load balancing using manual preemption, see VLAN load balancing.

### Procedure

**Step 1** Use the **enable** command to enter privileged EXEC mode.

**Example:**

```
Switch> enable
```

**Step 2** Use the **rep preempt segment** *segment-id* command to manually trigger VLAN load balancing preemption for the specified segment.

**Example:**

```
Switch# rep preempt segment 10
```

Confirm the command when prompted to proceed with the preemption action.

# Configure FlexLink+ topology change messages

Notify upstream devices of topology changes within the FlexLink+ segment.

Configure FlexLink+ in a larger network domain to ensure traffic convergence.

**Procedure**

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Switch# configure terminal
```

**Step 2** Use the **interface** *interface-id* command to enter interface configuration mode.

**Example:**

```
Switch(config)# interface GigabitEthernet1/0/1
```

**Step 3** Use the **rep stcn stp** command to enable propagation of topology change notifications on the active interface.

**Example:**

```
Switch(config-if)# rep stcn stp
```

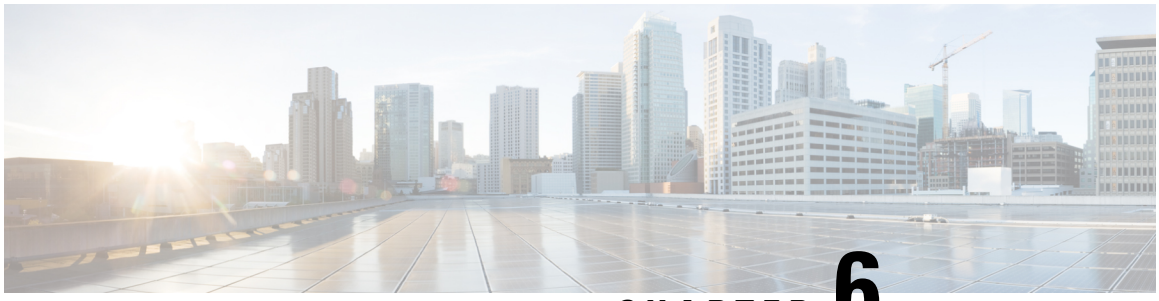
Configure the **rep stcn stp** command on the FlexLink+ interface to send topology change notifications to upstream STP, MSTP, and REP devices when a topology change occurs in the FlexLink+ segment. If you do not configure this command, upstream devices do not receive notifications about link failures or topology changes in the FlexLink+ segment, which can cause traffic blackholing.

**Note**
Enable this command on each interface configured for FlexLink+.

**Step 4** Use the **exit** command to exit interface configuration mode.

**Example:**

```
Switch(config-if)# exit
```



CHAPTER 6

# Media Redundancy Protocol


- Media Redundancy Protocol, on page 97
- MRP modes, on page 98
- MRP roles and states, on page 99
- Guidelines and limitations of MRP, on page 101
- MRP features in IE9300 stacks, on page 104
- Precision Time Protocol over MRP, on page 104
- Configure PTP over MRP, on page 105
- Configure the PROFINET MRP, on page 106
- Prerequisites to MRP CLI mode configuration, on page 109
- MRP CLI configuration parameters, on page 110
- Configure the Switch as MRA in MRP CLI mode, on page 110
- Configuration examples for MRP CLI mode, on page 112
- Examples of configuration verification commands and outputs, on page 113
- Media Redundancy Client, on page 115


# Media Redundancy Protocol

A MRP is a network protocol for industrial automation that ensures fast convergence in ring network topologies.

- Ensures fast convergence in ring network topologies for industrial automation
- Operates under the IEC standard 62439-2
- Supports recovery times of 30 ms, 200 ms, and 500 ms

### Supported switches and feature history for MRP

List of Cisco Catalyst IE9300 Rugged Series Switches that support MRP:

- IE-9310-26S2C-E and IE-9310-26S2C-A
- IE-9320-26S2C-E and IE-9320-26S2C-A
- IE-9320-22S2C4X-E and IE-9320-22S2C4X-A
- IE-9320-24T4X-E and IE-9320-24T4X-A
- IE-9320-24P4X-E and IE-9320-24P4X-A

- IE-9320-16P8U4X-E and IE-9320-16P8U4X-A
- IE-9320-24P4S-E and IE-9320-24P4S-A
- IE-9310-16P8S4X-E and IE-9310-16P8S4X-A

***Table 8: Feature History table***

| Feature | Release information | Feature description |
|---|---|---|
| Media Redundancy Client | 26.1.1 | This feature enables the configuration of Cisco switches as MRC within an MRP ring. This allows them to participate in network redundancy and respond to topology changes without acting as the ring manager. This approach enhances network resiliency and simplifies deployment. It also supports rapid failover and compliance with industrial certification requirements. |
| Enhanced ring convergence profiles for standalone IE9300 switches | Release 17.18.1 | From Cisco IOS-XE 17.18.1 onwards, 12 rings of 30ms is also supported on a standalone IE9300 switch. |
| PTP over MRP | Release 17.18.1 | From Cisco IOS-XE 17.18.1 onwards, PTP support over MRP is introduced. |
| MRP on an IE9300 Stack | Release 17.17.1 | From Cisco IOS-XE 17.17.1 onwards, stack support for MRP is introduced. |
| MRP | Release 17.13.1 | From Cisco IOS-XE 17.13.1 onwards, 12 rings of 200 ms or 500 ms convergence profiles are supported on a standalone IE9300 switch. |

# MRP modes

MRP modes are operating configurations that define how the switch interacts with the MRP network. Each mode has a distinct management interface and a specific compatibility with external frameworks.

- Only one MRP mode can be enabled at a time on the switch.
- Each mode offers a unique management interface and integration capability.

### Types of MRP modes and their characteristics

The switch supports two MRP modes, each with specific management and compatibility features.

- PROFINET MRP mode: Designed for integration with Siemens' Totally Integrated Automation (TIA) framework. This mode is primarily managed through the TIA framework and does not utilize the CLI or WebUI for MRP configuration. This mode is the default when the MRP is activated via the web interface or command line.
- MRP CLI mode: Managed using Cisco IOS XE CLI or WebUI. This mode is incompatible with Siemens TIA and does not support downloading MRP configurations from Siemens TIA.

# MRP roles and states

The roles and states of the MRP ring define how network redundancy is managed in a ring topology. They distinguish operational behaviors for preventing loops, managing failures, and ensuring recovery.

- MRP roles include MRA (default node role), MRM (manages the ring and coordinates recovery), and MRC (operates under MRM control).
- MRP ring port states are Disabled, Blocked, Forwarding, and Not Connected. Each state determines how frames are handled.
- MRP control frames (Test, TopoChange, LinkChange) are used for monitoring, failure detection, and recovery coordination.

### MRP roles, states, and protocol interoperation

MRP operates with defined roles and port states to manage network redundancy and recovery in ring topologies. MRP also interoperates with Spanning Tree Protocol (STP) to prevent loops and maintain network stability.

MRP node roles:

- MRA (Media Redundancy Automanager): Default for all nodes, uses a voting protocol to select one MRM based on priority; remaining nodes become MRCs.
- MRM (Media Redundancy Manager): Manages the ring, monitors status, blocks ports to prevent loops, and coordinates recovery during failures.
- MRC (Media Redundancy Client): Operates under MRM control, forwarding or blocking traffic as instructed.

MRP ring port states:

- Disabled: Ports drop all received frames.
- Blocked: Ports drop all frames except MRP control frames and some standard frames like LLDP.
- Forwarding: Ports forward all received frames.
- Not Connected: Ports are physically disconnected or down (distinct from Disabled, which is manually configured).

Network operation in normal (Ring-Closed) state:

- During normal operation, the network operates in a Ring-Closed state.

- One of the MRM's ring ports is blocked. The other forwards traffic to prevent loops.
- MRCs typically have both ports in the Forwarding state, resulting in a logical stub topology.

Network behavior during failures (Ring-Open state):

- When a failure occurs, the network transitions to a Ring-Open state.

  For example: If a link between two MRCs fails, both MRM ports switch to Forwarding, while MRCs adjacent to the failure have one port Disabled and the other Forwarding.

MRP control frames:

- Test Frames: Sent by the MRM to monitor ring status.
- TopoChange Frames: Sent by the MRM upon failure or recovery detection.
- LinkChange Frames: Sent by MRCs to the MRM during local port failure or recovery (Linkdown or Linkup events).

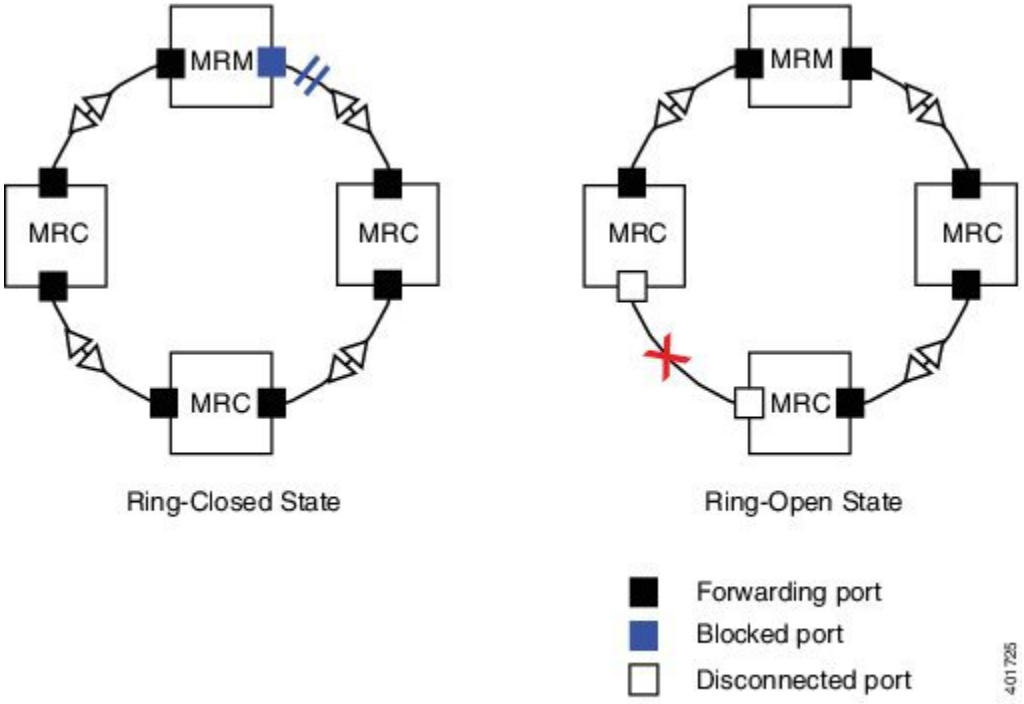
MRP-STP interoperation:

- MRP-STP interoperation enables MRP and STP to work together to maintain network stability and prevent broadcast loops.
- Interoperability is managed in MRP CLI mode; no additional CLI configuration is required for MRP and STP to interoperate.
- MRP works with STP to prevent broadcast loops caused by devices not participating in the MRP ring but accidentally connected to the network.
- STP Bridge Protocol Data Units (BPDUs) are not sent on MRP-enabled ports. When ports are unconfigured from the MRP ring, they are automatically added back to the STP network.

MRP recovery performance:

- MRP ensures efficient switchover during failures to avoid loss of Layer 2 Ethernet frames. This results in a logical stub topology.
- Recovery time profiles (for example: 200 ms) dictate the maximum recovery time during topology convergence.

*Figure 14: MRP ring states*




### MRP ring operation and recovery

The figure displays two rings: the Left and Right rings. In the Left Ring, the connection on the MRM is in a blocked state because no ports are disconnected. In the Right Ring, two MRC connections are in the disabled state because the link between them is broken, as marked by a red “x”.

# Guidelines and limitations of MRP

This section outlines MRP support, compatibility, port and ring configurations, convergence profiles, scalability, interface behavior, and access port setup.

## MRP support and compatibility

- Support for multiple MRP rings is available only through the CLI or WebUI.
- You cannot configure MRP on the port running these features: REP, STP, Flex Links, MACsec, Dot1x, or TrustSec.

## Ring and port configurations

- Each IE9300 node must include two interfaces as members of an MRP ring. Partial rings or ring segments are not supported.

- MRP ports cannot be configured as SPAN destination ports, private VLAN ports, tunnel ports, or on EtherChannels (or individual ports in EtherChannels).
- Each MRP ring has one Admin VLAN by default. You can override this using a CLI command. To prevent traffic flooding, the Admin VLAN must be unique for each ring on the same device. VLANs only include interfaces from a single MRP ring.

## Convergence profiles and scalability

- The switch supports up to 12 rings in standalone IE9300 switch. Each ring uses standard convergence profiles of 30 ms, 200 ms, or 500 ms.
- Each ring can support up to 50 MRCs.

## MRP interface behavior

- MRP interfaces start in a forwarding state and remain in this state until they receive notification to block. The ring state transitions to **Ring-Closed** during normal operation.

## Access port configuration

- To configure MRP interfaces as access ports, assign them to the appropriate VLAN using the **switchport mode access** and **switchport access vlan x** commands.

## Guidelines and limitations for MRP CLI mode

This section focuses on key configuration requirements, such as ensuring interface mode consistency, handling VLAN mismatches, reconfiguring rings, and supported convergence profiles.

- After using the CLI to configure the MRP ring, you must attach it to a pair of ports that support MRP.
- Both MRP ports must have the same interface mode, either access or trunk.
- To change the MRP ring configuration or to switch the interface mode of the ring ports between access and trunk, you must delete the existing ring configuration and recreate it with the desired settings.
- Access VLAN matching:
  - When both MRP ports are in access mode, their access VLANs must match.
  - If the configured MRP VLAN does not match the ports' access VLAN, the MRP VLAN is automatically updated to match the access VLAN of the MRP ports.
- VLAN mismatch error handling:
  - If the ports in an MRP ring do not belong to the same access VLAN during ring creation, or if the VLAN of one port changes after ring creation, MRP ring operation is suspended.
  - A system error message is displayed:

    ```
    ERROR% The ring 1 ports don't belong to the same access VLAN. The MRP ring will not
     function until the issue has been fixed.
    ```

  - To resolve this, ensure that both ring ports have the same access VLAN.

# Guidelines and limitations to MRA

MRA is a temporary administrative role in Cisco Catalyst IE9300 Rugged Series Switches that facilitates the selection of the MRM through a voting protocol during the startup phase of a MRP ring. After the voting process, the MRA transitions to either the MRM or MRC role.

MRA can be activated through the CLI. For configuration details, see the section MRP CLI configuration parameters, on page 110 in this configuration guide.

- MRA is not an operational role. It is used specifically at device startup to facilitate the MRM selection process.
- All nodes begin as MRAs at power-up. After the MRM is selected, the remaining MRAs automatically transition to the MRC role.
- Manual configuration of an MRM and MRA in the same ring is not supported.
- MRAs use a voting protocol based on a configured **priority** value to select the MRM. They sends **MRP_Test** frames on both ring ports.

  Manual configuration of an MRC role is not allowed; the role is automatically determined after the voting process.
- MRAs compare their own priority with the **priority** values in the received **MRP_Test** frames:
  - If the MRA's priority is higher, it sends an **MRP_TestMgrNAck** (negative acknowledgment) frame with the remote manager's MAC address.
  - If the MRA receives an **MRP_TestMgrNAck** containing its own MAC address, it transitions to the MRC role.
- Once the MRM is selected, the remaining MRAs transition to the MRC role. **MRP_TestPropagate** frames are sent to inform other MRAs in the client role about the role change and the new higher-priority MRM.

  These frames ensure that clients monitor the higher-priority manager and remain in the client role if the manager's role changes.

# Guidelines and limitations to PROFINET MRP mode

Before configuring the Cisco switch with PROFINET MRP through Siemens TIA or STEP7, ensure the following:

- The PROFINET MRP feature does not support the MRC role.
- Use the TIA portal to configure or modify the MRA role.
- Avoid using the CLI for configuration when TIA is in use. MRP CLI mode and PROFINET MRP mode are mutually exclusive.
- If the switch is connected to the PROFINET PLC, the output of **show profinet status | include Connected** should appear **Yes** . If it shows **No** , the switch is not connected to the PROFINET PLC.
- Ensure that the GSD file version matches the Cisco IOS release to avoid compatibility issues. Refer to the PROFINET Protocol Configuration Guide for detailed configuration instructions.

# MRP features in IE9300 stacks

MRP features in IE9300 stacks are network protocol capabilities that

- enable Media Redundancy Protocol across stacked Cisco IE9300 switches,
- support up to 4-member stacks (starting in Cisco IOS-XE 17.17.1), and
- enhance system stability and integration, with specific differences in support for modes such as PROFINET.

### Supported configurations and benefits

The functionality and behavior of MRP remain consistent in both standalone and stacked configurations, with MRP stack setups supporting up to 4 members. For more information on Switch Stacks, see Managing Switch Stacks .

Key benefits of deploying MRP in a stacked IE9300 setup include:

- Supports up to 16 rings with 200 ms and 500 ms convergence profiles in IE9300 stack setups. The 30ms convergence profile is not supported in IE9300 stack setups.
- Reduces the risk of single points of failure by ensuring the system stays operational, even if a stack member or the active switch fails.
- Provides seamless integration and reliability across the network.
- The stack setup offers greater port density, enabling the accommodation of more devices without compromising performance.

# Precision Time Protocol over MRP

PTP over MRP enables PTP time synchronization across networks that use MRP. This feature was introduced in IOS XE 17.18.1.

- PTP is a time synchronization protocol for distributed network nodes.
- PTP over MRP is supported according to IEC standard 62439-2. This support enables fast convergence in ring network topologies for Industrial Automation networks.
- The system is compatible with these configurations and features:
  - IE9300-Manager (up to 12 rings, each with 20 nodes over 20 km),
  - networks using QoS (COS 6 / DSCP EF 46),
  - copper and SFP ports, and
  - the system provides a time error deviation of less than 10 microseconds at 50% link utilization during an MRP ring break.

### Supported configurations for PTP over MRP

The table lists the supported configurations for PTP over MRP.

*Table 9: PTP over MRP supported configurations*

| Device | PTP clock | PTP profile | MRP mode | MRP convergence |
|---|---|---|---|---|
| **IE9300** | Boundary/Grand Master Boundary (GMC-BC) | Default (IEEE 1588 v2) | Manager | • 200ms<br>• 500ms |

# Configure PTP over MRP

Use this task to configure PTP over MRP.

**Before you begin**

**Note** For more information on configuring PTP over MRP, see Timing and Synchronization Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Step 2** Use the **ptp clock boundary domain** *domain_number* **profile** *profile-type-name* command to enable the PTP boundary mode.

**Example:**

```
Switch(config)#ptp clock boundary domain 44  profile default
```

**Step 3** (Optional) Use the **dscp** *dscp_value* **message** [ **event** | **general** ] command in BC mode to set the IP Differentiated Services Code Point (DSCP) value for messages.

**Example:**

```
Switch(config-ptp-clk)#ip dscp 43 message
```

**Note**

- *dscp_value*—a number from 0 to 63,
- **message event**—configures the DSCP value for event messages., with a default value of 59,
- **message general**—configures the DSCP value for general messages, with a default value of 47.

**Step 4** Use the **end** command to save the configuration and exit the privileged EXEC mode.

The PTP is configured with DSCP values for messages over MRP.

### What to do next

You can configure Quality of Service (QoS) settings.

# Configure the PROFINET MRP

This task guides you through configuring PROFINET MRP to ensure proper network operation and redundancy.

**Before you begin**

Disconnect an MRP Ethernet port from the ring (open ring) to discover all neighboring devices by using the LLDP protocol. Complete this step before you deploy PROFINET MRP to the network. This method helps prevent unnecessary flooding if you encounter configuration issues.

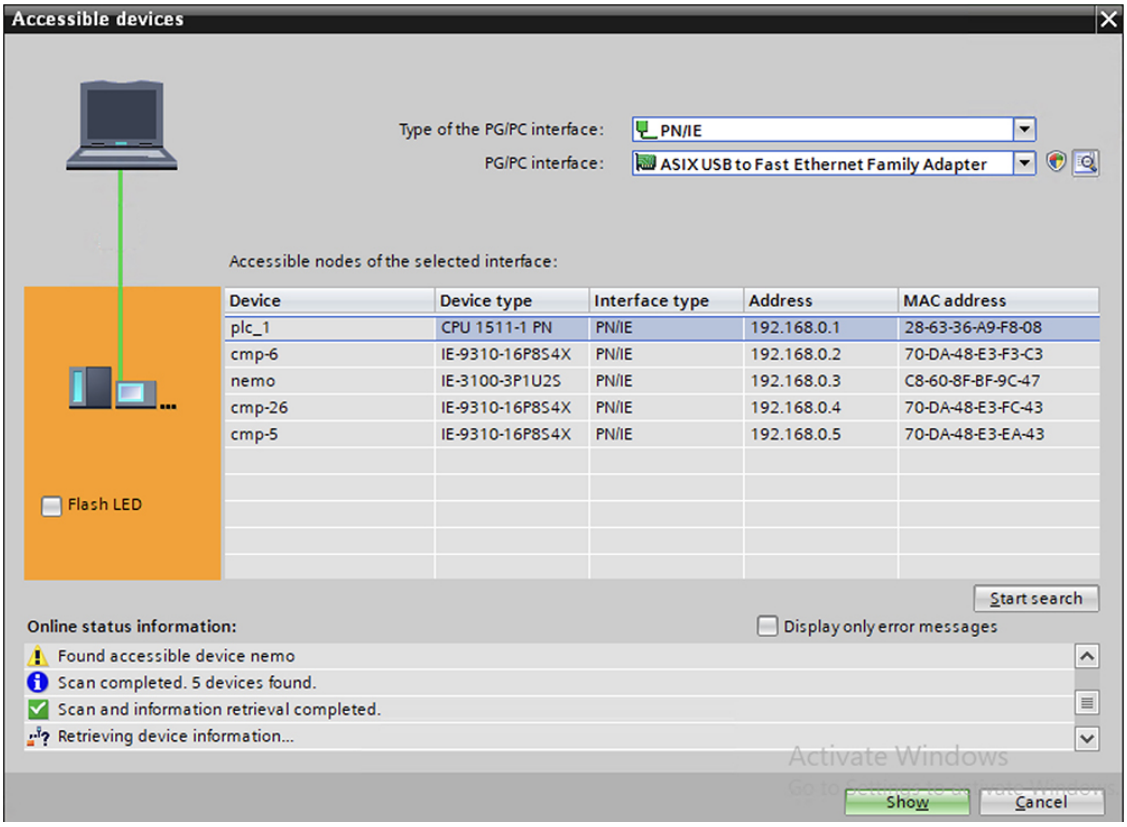
- Use the **show lldp neighbor** command to confirm all neighbor devices are correctly discovered before continuing with PROFINET MRP setup.
- Check that the PROFINET status shows **connected-state**.

### Procedure

**Step 1** Access the PROFINET Device Discovery (DCP) window.

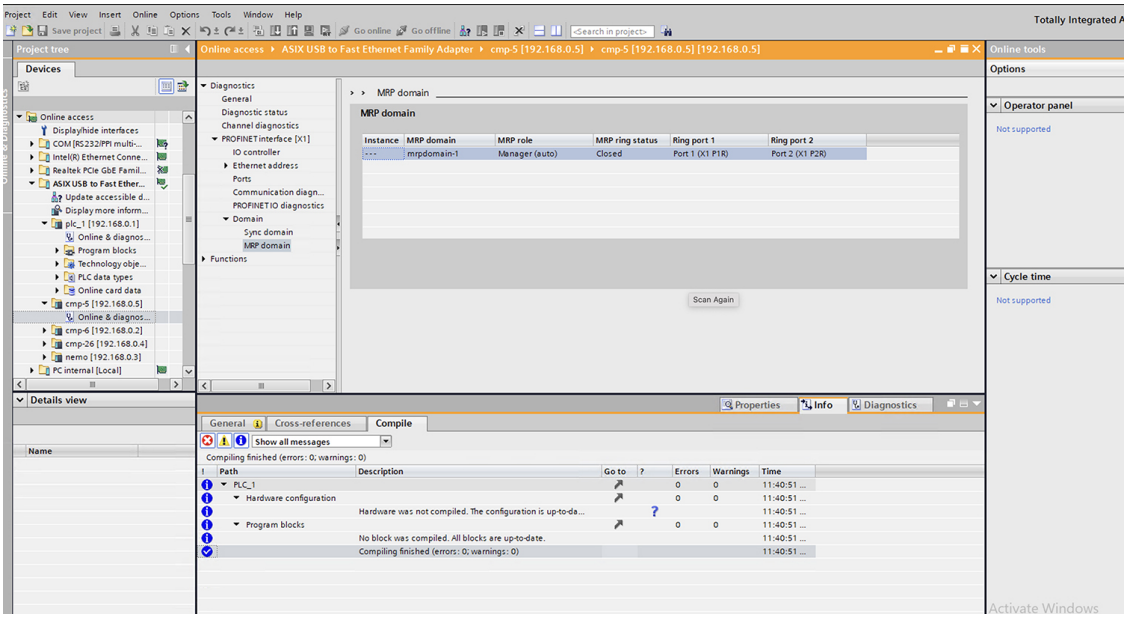
Open the PROFINET DCP window to identify and manage devices in the network.

*Figure 15: DCP window before configuring MRP*



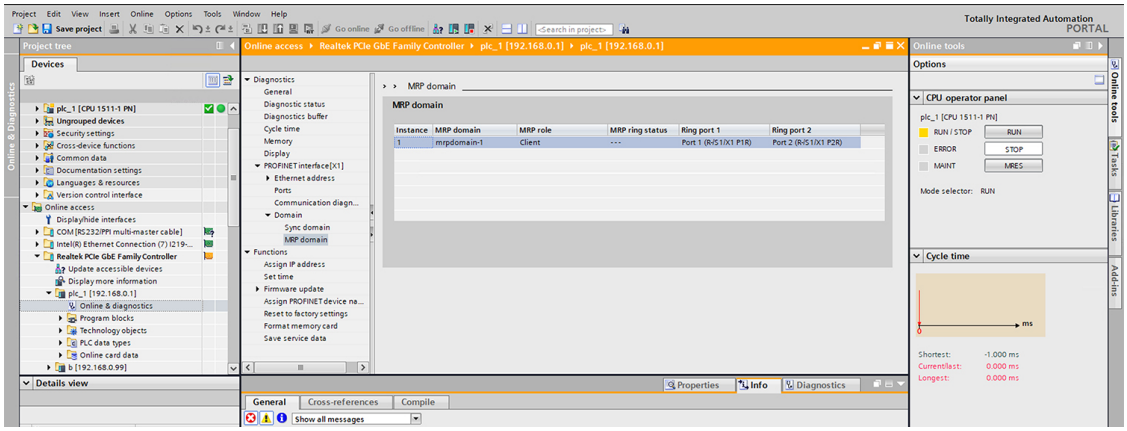

**Step 2** Assign PROFINET MRP manager role and domain name on the device.

*Figure 16: PROFINET MRP manager role and MRP domain name*



**Step 3** Define the PROFINET MRP client and MRP domain name on client devices.

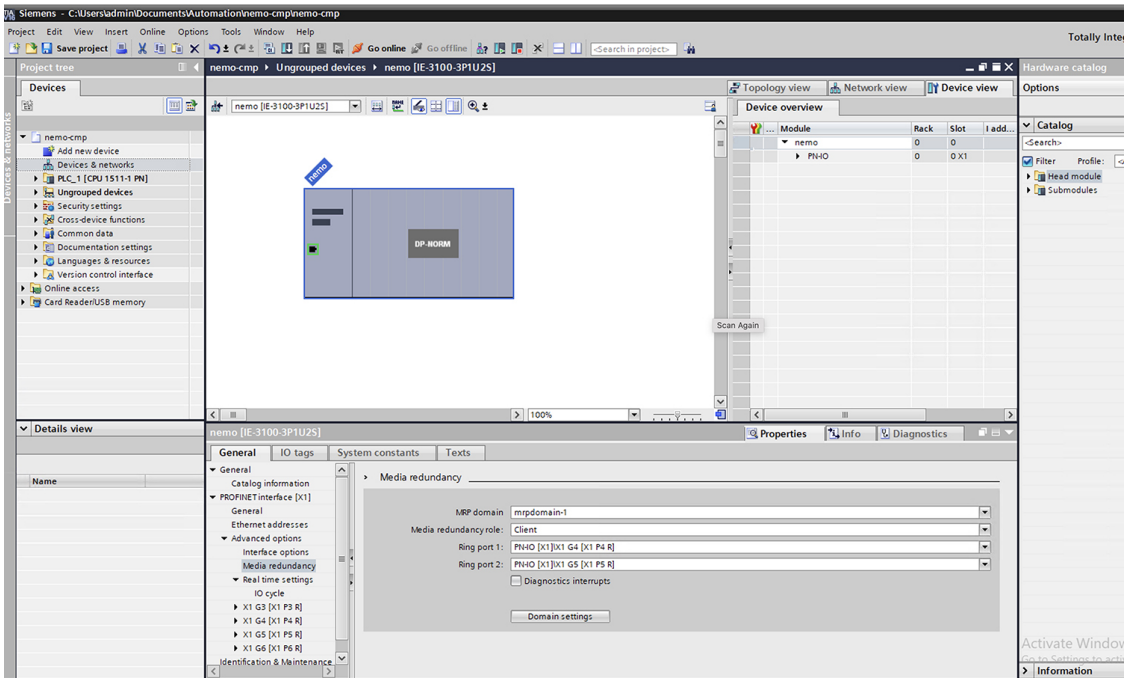
***Figure 17: PROFINET MRP and MRP domain on client***




**Step 4** If you use MRA mode, configure all devices and domain details.

**Step 5** Configure the PROFINET MRP interfaces on each device in the ring.

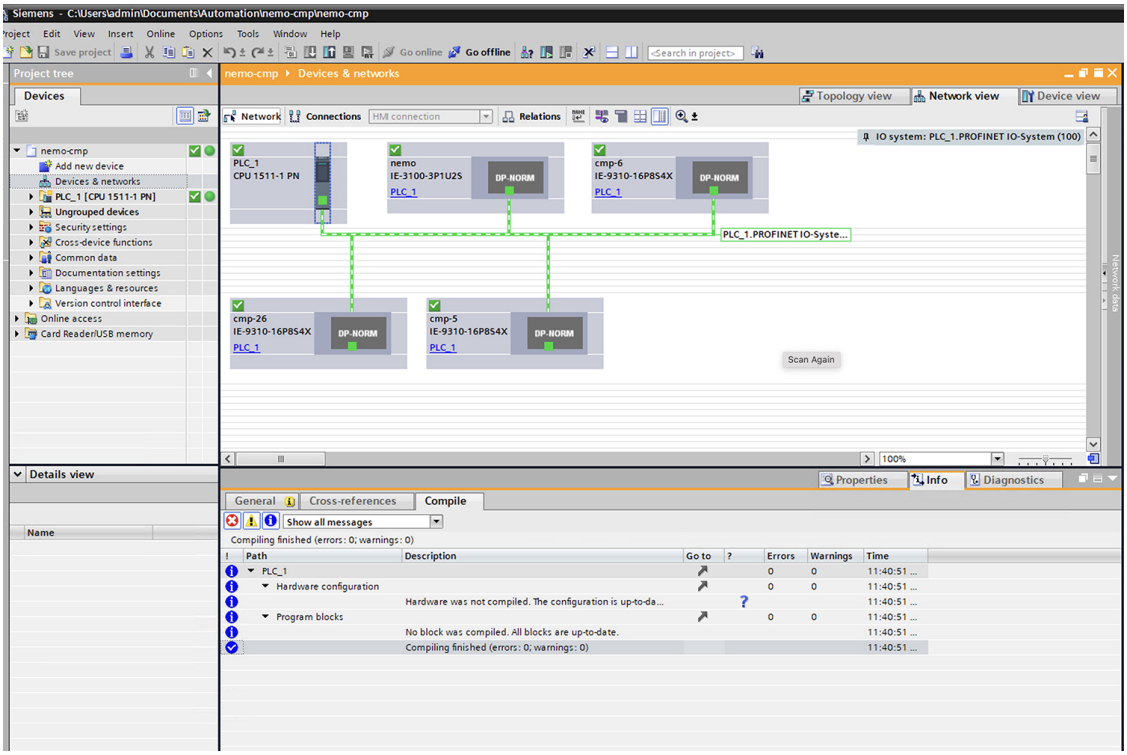
***Figure 18: PROFINET MRP interfaces***




**Step 6** Compile the configuration, and then download it to the PLC device.

**Step 7** Verify that all devices are connected and the MRP ring is closed.

*Figure 19: PROFINET MRP network configuration diagram*




# Prerequisites to MRP CLI mode configuration

To prevent network storms when configuring or unconfiguring the MRP feature in a physical ring topology, follow these steps:

- Ensure that one physical connection between two nodes in each ring remains open.
- Issue the **shut** command on the connecting interfaces or physically disconnect the cable.
- After completing the configuration of all MRMs, issue the **no shut** command on the port or reconnect the cable between the nodes.
- MRP CLI is disabled by default.

  The default mode is **PROFINET MRP**

  The default VLAN is **VLAN 1**
- If using a non-default VLAN for MRP, create the VLAN before assigning it to **MRP Ring 1**.

# MRP CLI configuration parameters

The MRP CLI configuration parameters are a category for configuring the MRP on a network device. These optional parameters help provide both redundancy and resiliency in network communication.

- domain-id: A unique identifier that represents the MRP ring and ensures correct recognition and communication within the ring.
- domain-name: This is a logical name assigned to the MRP domain ID to make management and identification easier.
- profile: This setting defines the timing parameter (default 200 ms), which controls how quickly the ring responds to topology changes.
- vlan-id: This is the VLAN used for transmitting MRP frames, which separates MRP traffic from other network data.

### Key components of MRP CLI configuration

The main components of MRP CLI configuration include node setup and ring count limits.

- Node setup: Configure the device as an MRA node and associate it with two MRP ports.
- Ring count limits:
  - Up to 16 rings can be configured in a stack setup.
  - Up to 12 rings can be configured on a standalone node.

# Configure the Switch as MRA in MRP CLI mode

To configure a switch as an MRA in MRP CLI mode, ensure proper ring and interface configurations for redundancy. MRP CLI mode is the default mode.

**Before you begin**

- Ensure the switch is connected and accessible via CLI.
- If the device is connected to a PLC module, select the option **no device in the ring** for MRP.

**Procedure**

**Step 1** Use the **configure termninal** command to enable MRP on the switch.

Use the **mrp ring** *mrp_id* command to configure the MRP ring with the specified ring ID.

**Example:**

```
Switch(config-mrp)# mrp ring 1
```

**Step 2** Use the **mode auto-manager** command to set the switch to auto-manage mode.

**Step 3** (Optional) Use the **profile** *value* command to configure the recovery profile.

Choose a value for maximum recovery time: 30, 200, or 500 ms. Default: 200 ms.

**Example:**

```
Switch(config-mrp-auto-manager)# profile 30
```

**Step 4** (Optional) Use the **priority** *value* command to configure the MRA priority.

Set a priority within 36864–61440. The default is 40960.

**Example:**

```
Switch(config-mrp-auto-manager)# priority 40955
```

**Step 5** (Optional) Use the **vlan-id** *vlan* command to configure the VLAN ID.

Use within 1–4094, default is 1.

**Example:**

```
Switch(config-mrp-auto-manager)# vlan-id 2025
```

**Step 6** (Optional for single MRP ring) Use the **domain-name** *name* command to configure the domain name.

Provide a name that can be up to 32 characters long.

**Example:**

```
Switch(config-mrp-auto-manager)# domain-name Cisco MRP Ring 1
```

**Step 7** (Optional for single MRP ring) Use the **domain-id** *value* command to configure the domain ID.

*value* is a UUID string of 32 hexadecimal digits in five groups separated by hyphens.

**domain-id** for MRP ring 1 is FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFE (by default).

**Example:**

```
Switch(config-mrp-auto-manager)# domain-id FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFE
```

Assign a unique domain ID to each ring:

- The default domain ID for ring 1 is FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFE.
- The default domain ID for ring 2 is FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFD.

The domain ID as FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF should be avoided.

**Step 8** (Optional) Use the **interval** *value* command to set the Interval.

Specify the interval options in milliseconds:

- 3 : Default interval for 30 ms recovery profile.
- 20 : Default interval for 200 ms recovery profile.
- 50 : Default interval for 500 ms recovery profile.

**Note**

The WebUI does not show the interval field for MRP.

**Example:**

```
Switch(config-mrp-auto-manager)# interval 3
```

**Step 9** Use the **end** command to exit from global configuration mode.

# Configure the ring ports and modes for MRP

Configure the ring ports and modes for MRP on network switches.

**Procedure**

**Step 1** Use the **configure terminal** command to configure the interface mode.

**Step 2** Use the **interface** *ID* to configure the ring ports and modes.

**Example:**

```
Switch(config)# interface GigabitEthernet1/0/22
```

**Step 3** Use the **switchport mode** { **access** | **trunk** } command to configure the interface mode.

**Example:**

For default VLAN ID 1 :

```
Switch(config-if)# switchport mode access
```

For other VLAN IDs:

```
Switch(config-if)# switchport mode access VLAN <ID>
```

**Step 4** Use the **mrp ring 1** command to associate the interface to the MRP ring.

**Step 5** Use the **end** command to return to the global configuration mode.

**Step 6** To configure multiple rings, repeat steps 1 to 4 for each additional ring.

# Configuration examples for MRP CLI mode

This section provides a configuration example for MRP auto-manager.

This section demonstrates how to configure auto-manager for MRP CLI mode.

```
Switch# configure terminal
Switch# no profinet mrp
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# mrp ring 1
Switch(config-mrp)# mode auto-manager
```

```
Switch(config-mrp-auto-manager)# domain-id FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFE
Switch(config-mrp-auto-manager)# priority 40960
Switch(config-mrp-auto-manager)# end
```

This section demonstrates how to configure interface mode for MRP CLI mode.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface GigabitEthernet1/0/22
Switch(config-if)# switchport mode trunk
Switch(config-if)# mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown all
interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/0/21
Switch(config-if)# switchport mode trunk
Switch(config-if)# mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown all
interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)# exit
```

# Examples of configuration verification commands and outputs

A verification procedure is a systematic process that

- confirms whether a configuration has been applied as intended,
- detects discrepancies between the expected and actual system state, and
- ensures that operational objectives are met after changes or deployments.

### MRP CLI Mode Configuration Verification

Verify the MRP CLI mode configuration:

```
Switch# show  mrp ring  1
MRP ring 1
Profile : 30 ms
Mode : Auto-Manager
Priority : 40955
Operational Mode: Manager
From : CLI
License : Not Applicable
Gateway :
Status : Disabled
Best Manager :
MAC Address : 70:DA:48:3B:B3:95
Priority : 40955
Network Topology: Ring
Network Status : CLOSED

Port1:
MAC Address : 70:DA:48:3B:B3:96
Interface : Tw1/0/22
Status : Forwarding

Port2:
MAC Address : 70:DA:48:3B:B3:95
Interface : Tw1/0/21
Status : Blocked
```

```
VLAN ID : 2025
Domain Name : Cisco MRP Ring 1
Domain ID : FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFE
Topology Change Request Interval : 0ms
Topology Change Repeat Count : 3
Short Test Frame Interval : 1ms
Default Test Frame Interval : 3ms
Operational Test Frame Interval : 3ms
Test Monitoring Interval Count : 3
Test Monitoring Extended Interval Count : N/A
```

### MRP CLI mode configuration summary

This section presents the summary of the MRP CLI mode configuration.

```
Switch# show  platform mrp summary
MRP ring Summary
Total number of rings configured    : 1
Total number of rings Closed        : 1
Total number of rings Open          : 0
Total number of rings Idle          : 0
Total number of rings Undefined     : 0
Ring instance 1
status       : CLOSED
port 1       : Tw1/0/21, SECONDARY
port 2       : Tw1/0/22, PRIMARY
```

### PROFINET MRP mode configuration verification

Verify the PROFINET MRP mode configuration:

```
Switch# show profinet mrp ring 1
MRP ring 1
Mode : Client
From : Profinet
License : Not Applicable
Gateway :
Status : Disabled
Best Manager :
MAC Address : 28:63:36:A9:F8:08
Priority : 40960
Network Topology : Ring
Network Status : CLOSED

PNPORT 0:(126/53540)
MAC Address : 70:DA:48:E4:86:01
Interface : Gi1/0/1
Status : Forwarding

PNPORT 0:(126/53540)
MAC Address : 70:DA:48:E4:86:10
Interface : Gi1/0/16
Status : Forwarding

VLAN ID : 1
Domain Name : mrpdomain-1
Domain ID : C3D687FE789E3A1ACDBE5BFCBBC27B6
Link Down Timer Interval : 20 ms
Link Up Timer Interval : 20 ms
Link Change (Up or Down) count : 4
```

# Media Redundancy Client

Media Redundancy Client (MRC) is a network redundancy capability that

- enables Cisco switches to participate as client nodes in a MRP ring
- allows devices to react to ring topology changes and redundancy management controlled by an MRP manager.
- provides rapid recovery from link or node failures by quickly unblocking ports to maintain connectivity.

### MRC reference information

MRP supports seamless redundancy and fault tolerance, which are critical for industrial automation. It enables industrial switches to join existing MRP rings, ensuring high network availability. For example, switches can be added to a plant floor MRP ring and configured as clients to participate in redundancy without managing the ring.

In an MRP ring network, a designated MRM actively monitors the ring's health. All other switches act as Media Ring Clients (MRCs) and listen for instructions from the MRM. When a link or node fails, the MRM detects the issue. It then coordinates recovery by instructing all MRCs to update their forwarding tables and reroute traffic to avoid the failure.

Starting with Cisco IOS XE release 26.1.1, MRC mode is supported.

There are two modes to configure a node in an MRP ring:

- Auto-manager mode: The node participates in the manager election process. The node with the lowest priority becomes the manager (MRA-M), and the others become clients (MRA-C).
- Client mode (MRC): The node does not participate in the manager election process and always remains a client. This mode is essential for networks requiring Process Field Net (PROFINET) certification, which mandates client mode.

## MRC mode functionality

- MRC forwards the test frames.
- MRC responds to Media Redundancy Manager's (MRM's) instructions.
- MRCs do not supervise the ring.
- An MRP ring should consist of at least one MRM to achieve redundancy, as MRCs alone do not provide redundancy.

## Configure MRC

You can set up a switch to operate in MRC mode within an MRP ring for increased network redundancy.

Use this task when you need a switch to join an MRP ring as a client node, not as a manager.

Perform these steps to configure MRC.

### Procedure

**Step 1** Use the **configure terminal** command to enter configuration mode.

**Step 2** Use the **mrp ring** *ring_number* command to configure MRP for the specified ring ID.

**Example:**

```
Switch(config)# mrp ring 1
```

**Step 3** Use the **mode client** command to enable client mode for the ring.

**Example:**

```
Switch(config-mrp-ring)# mode client
```

The MRC mode ensures that the switch does not participate in the ring manager election.

**Step 4** Use the **exit** command to exit from the configuration mode and return to EXEC mode.

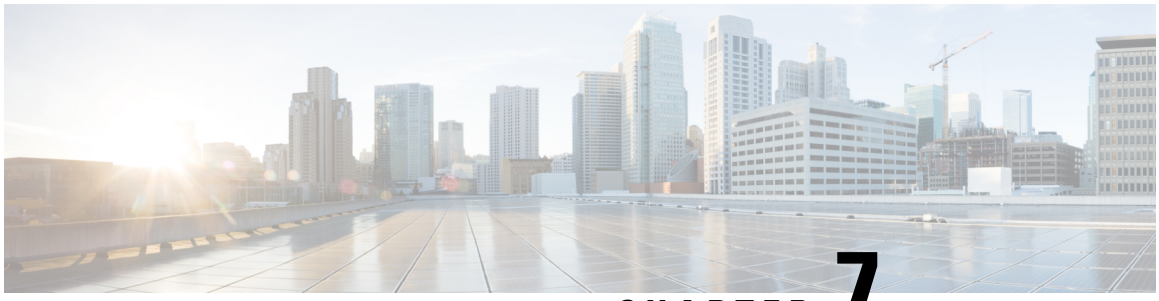
**Example:**

```
Switch(config-mrp-ring)# exit
```

**Step 5** (Optional) Use the **show mrp ring 1** command to monitor the MRP ring 1 details.

**Example:**

```
Switch# show mrp ring 1
MRP ring 1
Mode : Client
From : CLI
License : Not Applicable
Gateway :
Status : Disabled
Best Manager :
MAC Address : AA:BB:CC:DD:EE:01
Priority : 36864
Network Topology: Ring
Network Status : CLOSED
Port1: Port2:
MAC Address :AA:BB:CC:DD:EE:02 MAC Address : AA:BB:CC:DD:EE:03
Interface :Gi1/5 Interface :Gi1/7
Status :Forwarding Status :Forwarding
VLAN ID : 10
Domain Name : Cisco MRP Ring 1
Domain ID : FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFE
Link Down Timer Interval : 20 ms
Link Up Timer Interval : 20 ms
Link Change (Up or Down) count : 4
```



CHAPTER 7

# High-availability Seamless Redundancy


- Feature History, on page 117
- High-availability Seamless Redundancy, on page 117
- Guidelines for configuring HSR on IE9300 Series switches, on page 132
- Default settings, on page 136
- Configure an HSR ring, on page 137
- Enable HSR alarms, on page 139
- Clear all node table and VDAN table dynamic entries, on page 139
- HSR verification commands, on page 140
- Configuration examples, on page 143
- Related documents for the IE9300 Series, on page 147


## Feature History

This topic provides the release and feature information for High-Availability Seamless Redundancy (HSR)—HSR-SAN (Single RedBox mode).

***Table 10: Feature History Table***

| Feature Name | Release | Feature Information |
|---|---|---|
| **High-Availability Seamless Redundancy (HSR)—HSR-SAN (Single RedBox mode)** | Cisco IOS XE 17.13.1 | Initial support for Cisco Catalyst IE9300 Rugged Series Switches |

## High-availability Seamless Redundancy

High-availability Seamless Redundancy (HSR) is a network protocol defined in IEC 62439-3-2016 that provides seamless redundancy in ring topologies by sending traffic in both directions and using protocol-specific information to eliminate duplicate packets.

- HSR operates in a ring topology, with Port-A sending traffic counterclockwise and Port-B sending traffic clockwise.

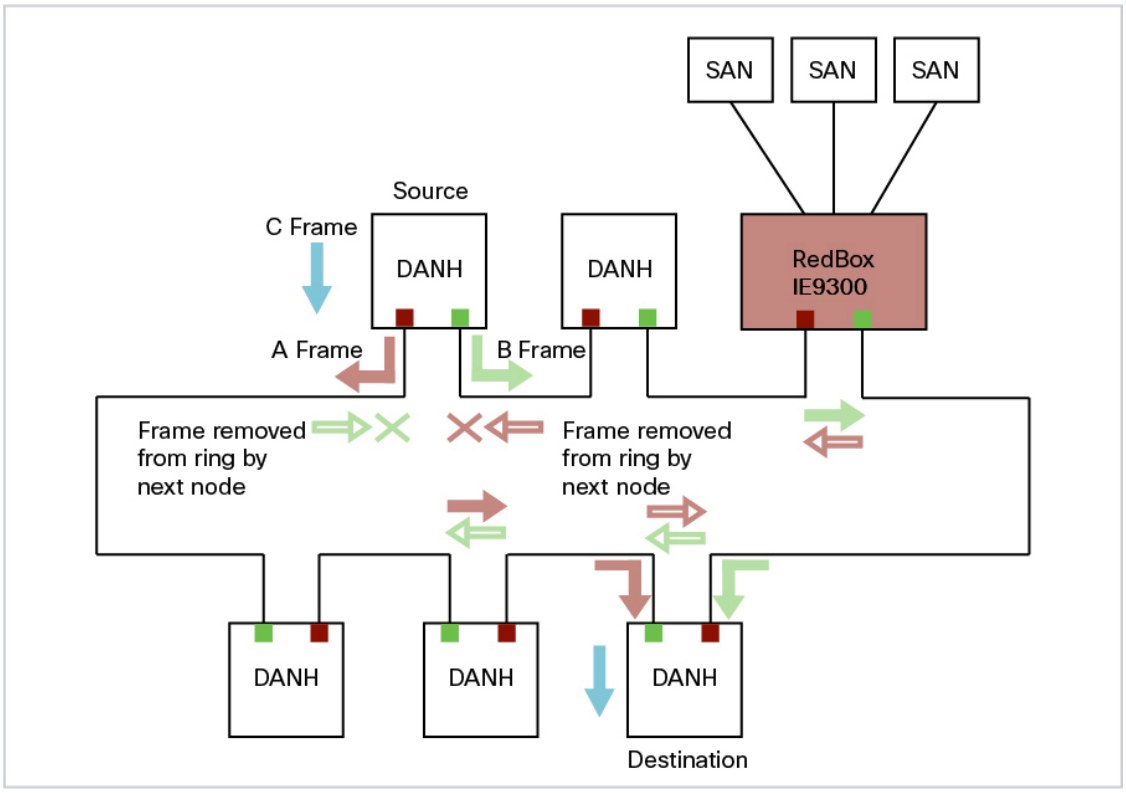
- The HSR packet format includes a header (HSR header) containing a sequence number to identify duplicate frames.
- HSR is similar to Parallel Redundancy Protocol (PRP), but differs in topology and packet format; PRP uses a redundancy control trailer (RCT) instead of a header.

### HSR protocol operation and device support

**Note** HSR is supported on specific Cisco Catalyst IE9300 Rugged Series Switches SKUs. For information about supported SKUs, refer to the Guidelines and Limitations section in this guide. The term *switch* in this document refers to a Cisco Catalyst IE9300 Rugged Series Switch unless otherwise noted.

1. In this release, the switch supports only an HSR Singly Attached Node (SAN) and only one HSR instance.
2. You can create only one HSR instance or one PRP instance. If you have created a PRP instance, no HSR instance can be created.
3. Non-switching nodes with two interfaces attached to the HSR ring are referred to as Doubly Attached Nodes implementing HSR (DANHs).
4. Singly Attached Nodes (SANs) connect to the HSR ring through a device called a RedBox (Redundancy Box).
5. The RedBox acts as a DANH for any traffic when it is the source or the destination. The switch implements RedBox functionality using Gigabit Ethernet port connections to the HSR ring.
6. The following figure shows an example of an HSR ring as described in IEC 62439-3. In this example, the RedBox is an Cisco Catalyst IE9300 Rugged Series Switch.

*Figure 20: Example of HSR ring carrying unicast traffic*




7. Devices that do not support HSR must not connect directly to the HSR ring. Examples include laptops and printers. All HSR-capable devices must process the HSR header on received ring packets. They must also add the HSR header to packets sent into the ring.
8. Non-HSR devices connect to the HSR ring through a RedBox. As shown in the figure, the RedBox has two ports on the DANH side. Non-HSR SAN devices connect to the upstream switch ports.
9. The RedBox generates supervision frames for these devices. This makes them appear as DANH devices on the ring. Because the RedBox emulates these as DANH, they are called Virtual Doubly Attached Nodes (VDAN).

# Loop avoidance mechanisms

Loop avoidance is a mechanism in HSR rings that prevents data frames from circulating endlessly, ensuring efficient use of network bandwidth and avoiding network loops.

- Each node forwards frames from one HSR port to the other, but the RedBox does not retransmit frames already sent in the same direction.
- Unicast packets destined for nodes inside the ring are consumed by the destination node and not forwarded further.
- Packets that complete a loop are detected and dropped by the originating node to prevent looping.

Loop avoidance in HSR rings is achieved through specific forwarding and dropping behaviors for unicast and multicast packets.

- Unicast packet with destination inside the ring: When the unicast packet reaches the destination node, the packet is consumed by the respective node and is not forwarded.
- Unicast packet with destination not inside the ring: This packet does not have a destination node in the ring, so every node forwards it until it returns to the originating node. Each node tracks the packets it sends and their direction. When the originating node recognizes that the packet has completed a loop, it drops the packet.
- Multicast packet: Each node forwards a multicast packet, as there can be more than one recipient. As a result, the multicast packet always returns to the originating node. Every node checks whether it has already forwarded the packet through its outgoing interface. When the packet returns to the originating node, the node identifies it as already forwarded and drops it instead of forwarding it again.

# HSR RedBox operation modes

The HSR RedBox enables connectivity between SAN devices and HSR rings. It can also bridge HSR and PRP networks or connect two HSR rings, depending on its mode of operation.

- HSR-SAN mode connects SAN devices to an HSR ring and represents SAN devices as VDANs on the ring.
- HSR-PRP mode bridges HSR and PRP networks by converting frames between the two protocols.
- HSR-HSR mode connects two HSR rings using a QuadBox device, associating switch ports with each ring.

### Supported HSR RedBox modes

The HSR RedBox can operate in several modes. Each mode defines how packets are handled in different network scenarios.

- **HSR-SAN** : The most basic mode, where the RedBox connects SAN devices to an HSR ring. No other PRP or HSR network is involved. Traffic on the upstream switch port does not have HSR/PRP tags, and the RedBox represents the SAN device as a VDAN in the ring.
- **HSR-PRP** : Used to bridge HSR and PRP networks. The RedBox extracts data from the PRP frame and generates the HSR frame, and performs the reverse operation for packets in the opposite direction. More than one PRP network can be bridged to one HSR ring and vice versa.
- **HSR-HSR** : Connects two HSR rings through a QuadBox device. Two ports on the switch are associated with one HSR ring, and the other two ports are associated with the second HSR ring. The remaining ports on the switch are shut down.

**Note** In this release, the switch supports HSR-SAN mode only.

### HSR RedBox in HSR-SAN mode

In HSR-SAN mode, the RedBox connects SAN devices to an HSR ring, and the RedBox represents each SAN device as a VDAN on the ring. No HSR or PRP tags are present on the upstream switch port traffic.

# HSR SAN mode in RedBox ring topology

HSR SAN mode is a configuration in which the RedBox inserts the HSR tag for the host within a ring topology. The RedBox also manages forwarding of ring traffic, applying specific rules for handling frames, duplicates, and unique destinations.

In HSR SAN mode, packets are handled in these ways:

- A source DANH sends a frame passed from its upper layers (C frame). It prefixes the frame with an HSR tag to identify frame duplicates and sends the frame over each port (A frame and B frame).
- A destination DANH receives two identical frames from each port within a certain interval. The destination DANH removes the HSR tag of the first frame before passing it to its upper layers and discards any duplicate.
- Each node in the HSR ring forwards frames received from one port to the other port of the HSR pair. However, specific exceptions apply:
  - The received frame returns to the originating node in the ring.
  - The frame is a unicast frame with a destination MAC address of a node upstream of the receiving node.
  - The node had already sent the same frame in the same direction. This rule prevents a frame from spinning in the ring in an infinite loop.

# CDP and LLDP for HSR

HSR supports the Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP). CDP and LLDP are Layer 2 neighbor discovery protocols. Both CDP and LLDP can provide information about nodes directly connected to the device. They also provide additional information, including the local and remote interface names and device names.

When CDP or LLDP is enabled, you can use the CDP or LLDP information to find the adjacent nodes on an HSR ring and their status. You can use the neighbor information from each node to determine the complete HSR network topology. Additionally, you can debug and locate ring faults.

CDP and LLDP are configured on physical interfaces only.

For more information, see Configuring an HSR Ring and Verifying Configuration.

# HSR alarms

- HSR alarms are generated by an HSR RedBox when one or both physical ring ports/links are down.

- Partial Ring Fault occurs when one ring port or link is down. Packets can still be sent using the redundant path, but user intervention is required.
- Full Ring Fault occurs when both ring ports or links are down. This major fault requires immediate attention and can trigger an external hardware alarm relay.

### HSR alarm types, notifications, and event representation

HSR rings can generate partial and full ring fault alarms, each with specific notification mechanisms and system representations.

- Syslog: Generated when the alarm is raised or cleared.
- SNMP Notification: Sent when the alarm is raised or cleared.
- Relay output: External relay contacts are asserted or de-asserted in response to the alarm. Relays are activated by major faults only.

This table lists the HSR events and their representations.

***Table 11: HSR Events and Representations***

| Event Number | Event Description | System Log (Level) | Alert/Alarm Log | Alarm LED and Output relay |
|---|---|---|---|---|
| **1** | Ring goes from UP to DOWN state. | 2 | 2 | Major Alarm/Assert |
| **2** | Ring goes from DOWN to UP state. | 6 | 6 | De-assert |
| **3** | One ring port goes DOWN. The other ring port and the ring itself are UP. | 3 | 3 | |
| **4** | Both ring ports are UP again. | 6 | 6 | |

**Note** See Enable HSR alarms, on page 139 for steps to configure HSR alarms.

You can view currently active alarms using the **show facility alarm status** command. The following example shows alarm status for minor and major HSR alarms:

```
Switch# show facility-alarm status
Source          Severity    Description                     Relay   Time
Switch            MINOR    34 HSR ring is partially down       MAJ    Oct 24 2017 10:16:10

-------
Switch# show facility-alarm status
Source          Severity    Description                   Relay     Time
Switch            MAJOR    33 HSR ring is down              MAJ      Oct 24 2017 10:17:07
```

### HSR alarm syslog examples

The following examples show the syslog entries that are generated for each HSR alarm event assertion and clear event (if configured):

- Syslog generated on occurrence of Partial fault:

```
Oct 24 11:07:13.952 IST: %HSR_ALARM-3-HSR_PARTIALFAULT: The HSR ring in now in PARTIAL
 FAULT state
```

- Syslog generated when the Partial fault is cleared:

```
Oct 24 11:07:38.032 IST: %HSR_ALARM-3-HSR_PARTIALFAULT: The HSR ring in now in PARTIAL
 FAULT state - event cleared
```

- Syslog generated on occurrence of Full fault:

```
Oct 24 11:07:38.036 IST: %HSR_ALARM-2-HSR_RINGFAULT: The HSR ring in now in FAULT state
```

- Syslog generated when the Full fault is cleared:

```
Oct 24 11:08:19.082 IST: %HSR_ALARM-2-HSR_RINGFAULT: The HSR ring in now in FAULT state
 - event cleared
```

# PTP over HSR

PTP over HSR is a network synchronization capability that allows PTP packets to bypass standard HSR duplicate or discard logic to maintain timing accuracy across redundant paths.

PTP over HSR:

- Supports the PTP Power profile on Cisco Catalyst IE9300 Rugged, IE3500 Rugged Series Switches.
- Utilizes a designated time recipient port for synchronization while maintaining a passive port for redundancy.
- Operates automatically without requiring additional interface-specific PTP configuration.

### PTP over HSR operational details

The PTP grandmaster in an HSR network can be a RedBox, a VDAN, a SAN, or a DANH. Because the PTP 1588 standard does not account for clocks synchronized over redundant, simultaneously active paths, HSR handles PTP packets differently than other traffic types.

## Supported PTP profiles and modes

This reference provides the HSR support matrix for PTP profiles, clock modes, and RedBox types as defined by IEC 62439-3.

PTP over HSR is supported only for the PTP Power Profile. For unsupported PTP profiles, PTP traffic flows over HSR port-A only.

*Table 12: HSR support for PTP profiles*

| PTP Profile | Clock Mode | Supported | HSR RedBox Type as per IEC 62439-3 |
|---|---|---|---|
| Power Profile | Boundary Clock (BC) | Yes | HSR RedBox as doubly attached BC (DABC) with P2P |
| | P2P Transparent Clock (TC) | Yes | HSR RedBox as doubly attached TC (DATC) with P2P |
| | Grandmaster Clock (GMC)-BC | No | Not applicable |
| | Forward | No | Not applicable |
| Default Profile | BC | No | Not applicable |
| | End-to-End (E2E) TC | No | Not applicable |

## Operating HSR RedBox as Doubly Attached BC (DABC) with P2P

This section describes the operation of PTP over HSR using an example where RedBox Primary and RedBox Secondary are configured to run in Power Profile as Boundary Clocks that use the Peer-to-Peer delay measurement mechanism.

### Summary

Assume for this example that SAN-1 is the GMC. All the clocks are configured to run Peer-to-Peer Delay measurement and the peer delay is regularly calculated and maintained on every link shown in the figure. The BMCA on RedBox Primary determines the port to SAN-1 to be connected to the time source. The PTP protocol running on RedBox Primary will forward Sync and Follow_Up messages on ports RedBox Primary A and B.

On RedBox Secondary, the regular BMCA operation determines RedBox Secondary port A to be time recipient and RedBox Secondary port B to be `PASSIVE`. However, with the knowledge that ports RedBox Secondary A and B are part of the same HSR ring, RedBox Secondary port B is forced into `PASSIVE_SLAVE` state and RedBox Secondary port A becomes active for PTP.

RedBox Secondary port A works as a regular time recipient port. It uses the Sync and Follow_Up messages along with their correction field to calculate the delay and offset from time source and synchronize the local clock.

RedBox Secondary port B, which is in `PASSIVE_SLAVE` state operates in this way:

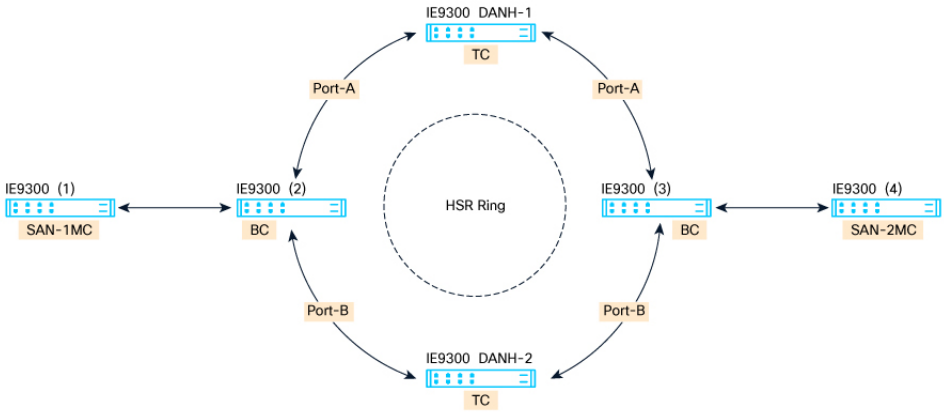
Just like RedBox Secondary port A, it maintains the delay and offset from time source, but does not perform any operation on the local clock. Having all the synchronization information available enables it to seamlessly take over as the new time recipient in case RedBox Secondary port A loses communication with the GMC.

The given image uses these device mappings:

- SAN-1MC: IE9300 (1)
- RedBox Primary: IE9300 (2)

- RedBox Secondary: IE9300 (3)
- SAN-2MC: IE9300 (4)
- DANH-1: IE9300 configured as a Transparent Clock
- DANH-2: IE9300 configured as a Transparent Clock

### Workflow




These stages describe the PTP operation and synchronization logic for RedBox Primary (IE9300 (2)) and RedBox Secondary (IE9300 (3)).

1. RedBox Primary (IE9300 (2)) performs BMCA to identify the time source and distribute synchronization messages.
   - BMCA identifies the port connected to SAN-1MC (IE9300 (1)) as the time-receiver port.
   - Sync and Follow_Up messages are forwarded through RedBox Primary Port A toward DANH-1 and through RedBox Primary Port B toward DANH-2.
2. RedBox Secondary (IE9300 (3)) manages its port states to maintain synchronization and redundancy.
   - RedBox Secondary Port A, connected to DANH-1, functions as the active time-receiver port.
   - RedBox Secondary Port B, connected to DANH-2, remains in the `PASSIVE_SLAVE` state while maintaining synchronization information for failover.

### Result

The local clock on RedBox Secondary (IE9300 (3)) is synchronized using the correction field in the Sync and Follow_Up messages. If RedBox Secondary Port A loses communication with the GMC, RedBox Secondary Port B can take over as the active time-receiver port.

## Configure HSR RedBox as DABC with P2P

Configure the PTP power profile on SAN, RedBox, and DANH nodes in an HSR doubly attached boundary clock topology with P2P delay measurement.

This procedure applies to resilient industrial Ethernet deployments that use SAN or RedBox boundary clocks and DANH transparent clocks. These clocks must synchronize with the same grandmaster while maintaining redundancy and accurate peer-delay measurements.

### Procedure

**Step 1** Use the **configure terminal** command to enter global configuration mode.

**Example:**

```
Switch# configure terminal
```

**Step 2** Use the **interface range** *interface-id* command to create the HSR ring interface and assign the ports to the HSR ring.

**Example:**

```
Switch(config)# interface range GigabitEthernet 1/0/21-22
```

**Note**
Select the pair that matches the physical ring connections in your deployment. Both interfaces in the selected pair must use the same settings and VLAN configuration. Configure these settings before assigning the interfaces to the HSR ring.

For channel and interface details, see HSR-Ring 1

**Step 3** Use the **hsr-ring** *ring-id* command to create an HSR ring.

**Example:**

```
Switch(config-if-range)# hsr-ring 1
```

**Step 4** Use the **no shutdown** command to turn on the HSR interface.

**Example:**

```
Switch(config-if-range)# no shutdown
```

For more details on the HSR ring configuration, see HSR Ring Configuration

**Step 5** Use the **exit** command to return to global configuration mode.

**Example:**

```
Switch(config-if-range)# exit
```

**Step 6** Configure PTP

a) Use the **ptp clock boundary domain** *domain-number* **profile power** command to configure the boundary type PTP clock, which stops the PTP session from the grandmaster clock and acts as a PTP server or client clock downstream.

**Example:**

```
Switch(config)# ptp clock boundary domain 0 profile power
```

b) Use the **allow-without-tlv** command to permit PTP message processing without TLVs.

**Example:**

```
Switch(config-ptp-clk)# allow-without-tlv
```

c) Use the **clock-port** *port-name* command to define a new clock port for ethernet multicast interface Gi1/0/21.

**Example:**

```
Switch(config-ptp-clk)# clock-port dyn1
```

d) Use the **transport ethernet multicast interface** *interface-id* command to specify the transport method for clocking traffic.

**Example:**

```
Switch(config-ptp-port)# transport ethernet multicast interface Gi1/0/21
```

e) Use the **clock-port** *port-name* command to define a new clock port for ethernet multicast interface Gi1/0/22.

**Example:**

```
Switch(config-ptp-clk)# clock-port dyn2
```

f) Use the **transport ethernet multicast interface** *interface-id* command to specify the transport method for clocking traffic.

**Example:**

```
Switch(config-ptp-port)# transport ethernet multicast interface Gi1/0/22
```

g) (Optional) Use the **vlan** *vlan-id* command to configure VLAN for tagged packets.

**Example:**

```
Switch(config-ptp-port)# vlan 100
```

**Step 7** Configure Configure DANH-1 as a TC

In this example, DANH-1 is an IE9300 switch configured as a TC. The PTP commands apply to supported switches. HSR interface assignments are platform-specific so you can use the supported interface pair for your switch model.

a) Use the **configure terminal** command to enter global configuration mode of the switch that operates as DANH-1.

**Example:**

```
DANH-1# configure terminal
```

b) Use the **ptp clock transparent domain** *domain-number* **profile power** command to configure the device as a Transparent Clock, which accounts for packet residence time to maintain PTP synchronization accuracy without terminating the PTP session.

**Example:**

```
DANH-1(config)# ptp clock transparent domain 0 profile power
```

c) Use the **allow-without-tlv** command to permit PTP message processing without TLVs.

**Example:**

```
DANH-1(config)# allow-without-tlv
```

See Step 8a to 8c to configure DANH-2.

See Verification commands to verify the configuration.

**Note**
When RedBox Primary and RedBox Secondary are configured for HSR, Boundary Clock (BC) must be enabled on both the HSR-capable ring ports and the ports connected to SANH devices.

# HSR RedBox as Doubly Attached TC (DATC) with P2P

This process assumes SAN-1 functions as the Grandmaster Clock (GMC). All clocks are configured to run Peer-to-Peer Delay measurement, with peer delay regularly calculated and maintained on every link.

### Summary

These components participate in the synchronization process:

- RedBox Primary: Performs BMCA to determine the time source connection and forwards Sync and Follow_Up messages.
- RedBox Secondary: Operates with one port as the time recipient and the other as a passive slave to ensure seamless failover.

### Workflow

These stages describe the operational behavior of the RedBox devices during PTP synchronization.

1. RedBox Primary determines the time source and manages message forwarding.
   - The BMCA on RedBox Primary identifies the port connected to SAN-1 as the time source.
   - RedBox Primary forwards all Sync and Follow_Up messages received on port C out of ports A and B.
2. RedBox Secondary manages port roles to maintain synchronization and redundancy.

| When | And | Then | And |
|---|---|---|---|
| Port A receives Sync/Follow_Up | Active state | Calculate delay and offset | Forward messages out of port C |
| Port B receives Sync/Follow_Up | Passive state | Maintain delay and offset | Drop messages |

### Result

The network maintains synchronization information, allowing port B to seamlessly take over as the time recipient if port A loses communication with the GMC.

# Configure HSR RedBox as DATC with P2P

Configure PTP power profile and clock modes across SAN, RedBox, and DANH nodes to establish deterministic time synchronization in an HSR DATC topology using P2P delay measurement.

This procedure applies to resilient industrial Ethernet deployments where SAN or RedBox TCs and DANH TCs must converge to the same grandmaster with redundancy and accurate peer-delay timing.

### Procedure

**Step 1** To configure SAN-1, SAN-2, RedBox with PTP, see PTP configuration.

**Step 2** Use the **interface range** *interface-id* command to create the HSR ring interface and assign ports to the HSR ring.

**Example:**

```
Switch(config)# interface range GigabitEthernet 1/0/21-22
```

For channel and interface details, see HSR-Ring 1 .

**Step 3** Use the **hsr-ring** *ring-id* command to create HSR ring.

**Example:**

```
Switch(config-if-range)# hsr-ring 1
```

**Step 4** Use the **no shutdown** command to turn on the HSR interface.

**Example:**

```
Switch(config-if-range)# no shutdown
Swotch(config-if-range)# exit
```

For more details on the HSR ring configuration, see HSR Ring Configuration.

**Step 5** Configure DANH-1 as a TC

In this example, DANH-1 is an IE9300 switch configured as a TC. The PTP commands also apply to supported switches. HSR interface assignments are platform-specific so you can use the supported interface pair for your switch model.

a) Use the **configure terminal** command to enter global configuration mode of the switch that operates as DANH-1.

**Example:**

```
DANH-1# configure terminal
```

b) Use the **ptp clock transparent domain** *domain-number* **profile power** command to configure the device as a TC, which accounts for packet residence time to maintain PTP synchronization accuracy without terminating the PTP session.

**Example:**

```
DANH-1(config)# ptp clock transparent domain 0 profile power
```

c) Use the **allow-without-tlv** command to permit PTP message processing without TLVs.

**Example:**

```
DANH-1(config)# allow-without-tlv
```

See Step 5a to 5c to configure TC for DANH-2, RedBox Primary, and RedBox Secondary.

See Verification commands to verify the configuration.

**Note**
On each RedBox, verify that PTP is enabled on both HSR ring interfaces and on the interfaces connected to singly attached nodes (SANs). Apply the same PTP settings to both HSR ring interfaces to support uninterrupted synchronization if the active timing path changes.

# HSR Uplink Redundancy Enhancement

The HSR Uplink Redundancy Enhancement feature is a network capability that allows two separate interfaces to connect upstream from the HSR ring through two separate HSR RedBoxes, ensuring there is no single point of failure when exiting the HSR ring.

- Enables flexible network designs with dual uplinks for redundancy.
- Supports high availability protocols such as HSRP, VRRP, and REP.
- Prevents next-hop split-brain conditions and reduces failover times.

### HSR Uplink Redundancy Enhancement reference information

The HSR Uplink Redundancy Enhancement feature allows two separate interfaces to connect upstream from the HSR ring through two separate HSR RedBoxes. This design ensures there is no single point of failure exiting the HSR ring. Protocols such as HSRP, VRRP, and REP can leverage this feature to improve high availability. Prior to this enhancement, using these protocols on redundant uplinks could result in issues like next-hop split-brain conditions or slow REP failover times.

To implement HSR Uplink Redundancy, confirm that the **fpgamode-DualUplinkEnhancement** feature is enabled. The feature provides connectivity to a dual router (HSRP) on the distribution layer.

1. Verify the status of the feature using the following command:

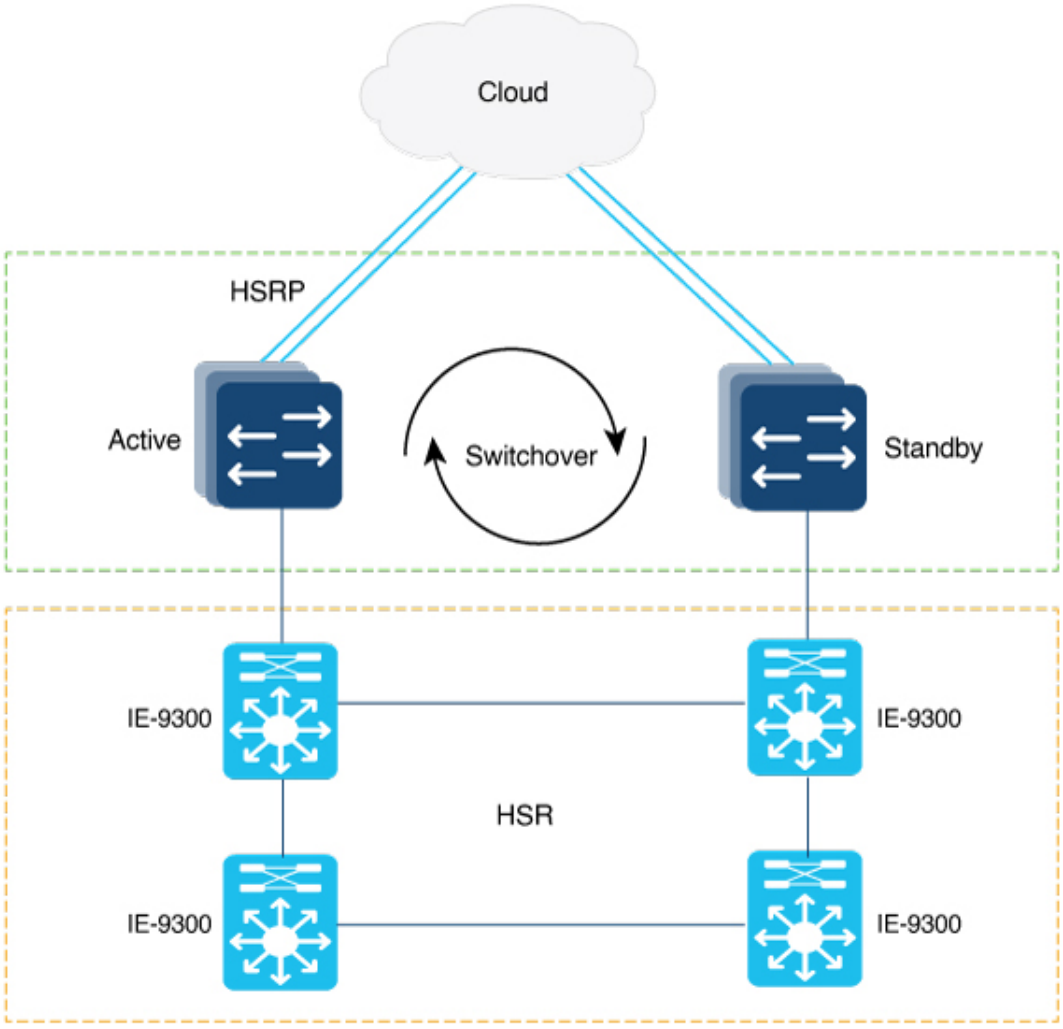
```
Switch# show hsr ring 1 detail | include fpgamode
fpgamode-DualUplinkEnhancement: Enabled
```

2. If the output shows *fpgamode-DualUplinkEnhancement* : *Disabled* , enable the feature with the following commands:

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#  hsr-ring 1 fpgamode-DualUplinkEnhancement
Switch(config)# end
```

A diagram shows an example network with HSR and HSRP that allows uplink next-hop gateway redundancy out of the HSR ring.

*Figure 21: Example of network redundancy using HSRP*




This example HSRP configuration applies to the two distribution switches Active and Standby depicted in the diagram. In this configuration, HSRP is configured in a Switch Virtual Interface (SVI).

```
Active# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Active(config)# interface vlan 10
Active(config-if)# ip address 30.30.30.2 255.255.255.0
Active(config-if)# standby 1 ip 30.30.30.1
Active(config-if)# standby 1 priority 120
Active(config-if)# end

Standby# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Standby(config)# interface Vlan10
Standby(config-if)# ip address 30.30.30.4 255.255.255.0
Standby(config-if)# standby 1 ip 30.30.30.1
Standby(config-if)# end
Active# show standby
Vlan10 - Group 1
```

```
State is Active
8 state changes, last state change 00:03:55
Track object 1 (unknown)
Virtual IP address is 30.30.30.1
Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 200 msec, hold time 750 msec
Next hello sent in 0.176 secs
Preemption enabled, delay min 5 secs, reload 5 secs, sync 5 secs
Active router is local
Standby router is 30.30.30.4, priority 100 (expires in 0.656 sec)
Priority 120 (configured 120)
Group name is "hsrp-Vl10-1" (default)
FLAGS: 0/1
Active# show standby brief
P indicates configured to preempt.
|
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        1    120 P Active  local           30.30.30.4      30.30.30.1
Standby# show standby
Vlan10 - Group 1
State is Standby
13 state changes, last state change 00:04:17
Track object 1 (unknown)
Virtual IP address is 30.30.30.1
Active virtual MAC address is 0000.0c07.ac01 (MAC Not In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 200 msec, hold time 750 msec
Next hello sent in 0.064 secs
Preemption enabled, delay min 5 secs, reload 5 secs, sync 5 secs
Active router is 30.30.30.2, priority 120 (expires in 0.816 sec)
Standby router is local
Priority 100 (default 100)
Group name is "hsrp-Vl10-1" (default)
FLAGS: 0/1
Standby# show standby brief
P indicates configured to preempt.
|
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        1    100 P Standby 30.30.30.2      local           30.30.30.1
```

### HSR Uplink Redundancy Enhancement example

This example demonstrates a network using HSR and HSRP to provide uplink next-hop gateway redundancy out of the HSR ring, with configuration steps for both Active and Standby distribution switches.

# Guidelines for configuring HSR on IE9300 Series switches

When configuring HSR and related modes on IE9300 Series switches, follow these guidelines and limitations:

HSR-SAN is supported on the following Cisco Catalyst IE9300 Rugged Series Switches:

- IE-9310-16P8S4X-E and IE-9310-16P8S4X-A
- IE-9320-26S2C-E and IE-9320-26S2C-A
- IE-9320-22S2C4X-E and IE-9320-22S2C4X-A

The interfaces supported for the HSR ring on IE-9310-16P8S4X-E and IE-9310-16P8S4X-A are listed in the table.

***Table 13: Channel and interface details***

| Channel | Interface |
|---|---|
| HSR-Ring 1 | Gi1/0/1-2 or Gi1/0/9-10 |

The interfaces supported for HSR ring on IE-9320-26S2C-E , IE-9320-26S2C-A , IE-9320-22S2C4X-E , and IE-9320-22S2C4X-A are:

***Table 14: Channel and interface details***

| Channel | Interface |
|---|---|
| HSR-Ring 1 | Gi1/0/21-22 or Gi1/0/23-24 |

1. Deployment, instance, and licensing restrictions

   HSR is supported only in a standalone deployment; there is no support for HSR for stacked switches. Only one HSR instance is supported. The switch supports only one HSR or one PRP instance. If a PRP instance has been created, you cannot create an HSR instance. The HSR feature requires the Network Essentials license. The HSR feature is not enabled by default. You must configure the HSR rings explicitly. HSR is disabled automatically if the required firmware image is not available on the system.

2. Interface assignment and ring mode restrictions

   Physical interfaces are predefined for the rings and ports in HSR-SAN, HSR-PRP, and HSR-HSR modes and cannot be changed. The table lists port assignments for each HSR mode. Ring 1 and Ring 2 support configuration in HSR-SAN mode. On the IE 4000 in HSR-PRP Dual RedBox mode, three ports participate in the HSR-PRP network. Only Ring 2 can be configured in this mode.

3. Port settings and compatibility requirements

   After including a port in a ring, you cannot change its media-type, speed, or duplex settings. Set these options before assigning ring membership. It is important for all interfaces in an HSR ring to have the same speed and duplex settings. Apply those settings before configuring ring membership. Both ports of one ring must be of same speed and type (that is, both can be SFPs or both can be copper). VLAN configuration such as trunk and access mode must be the same on both the ports participating in the ring. If you change the mode of HSR interfaces from access to trunk or trunk to access after configuring the ring, flap the HSR ring.

4. Node scale, ring limits, and port support

   The recommended maximum number of nodes in the node table is 512. Nodes include all DANH and VDAN devices connected to the ring. This number is not a strict limit. Adding more entries may increase duplicate packets for end devices. The maximum number of nodes in the HSR ring is 50. HSR ring ports can only be configured in L2 mode. HSR is supported on following port types:

   - 100 mbps, Full Duplex. Half duplex is not supported
   - 1000 mbps, Full Duplex. Half duplex is not supported
   - HSR is not supported on the uplink ports

5. Mutually exclusive protocols and unsupported features

   The following protocols and features are mutually exclusive with HSR on the same port: PRP, EtherChannels, Link Aggregation Control Protocol (LACP), Port Aggregation Protocol (PAgP), and REP. MACsec, HSR, and PRP are not allowed together. PTP over HSR is not supported. STP is not supported on the HSR ring. By default, all modes of Spanning Tree Protocol (STP) will be disabled on the ring ports. Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) are not supported on HSR. SPAN and RSPAN should not be used to monitor the traffic on an HSR ring. In addition, traffic that has been monitored using RSPAN should not be transferred over an HSR ring.

6. MTU and operational behavior

   HSR supports an MTU size of up to 1998 bytes of Ethernet payload. After an interface is added in the HSR ring, only the primary interface counters are updated. You should not need to configure and check the status of individual physical interfaces after they are added to the HSR ring.

7. Port shutdown restriction

   Once a port is part of ring, the port cannot be shut down. For example, if Gi1/0/23 and Gi1/0/24 are part of an HSR ring and you try to shut down Gi1/0/23 or Gi1/0/24, the operation will not be permitted:

   ```
   Switch(config)# <userinput>interface range gi1/0/23-24</userinput>
   Switch(config-if-range)#<userinput>shutdown</userinput>
    %Interface GigabitEthernet1/0/23 is configured in a HSR ring shutdown not permitted!
   Switch(config-if-range)#
   ```

   You can perform a shutdown of the HSR ring. For example:

   ```
   <userinput>Switch# conf t</userinput>
   Switch(config)#<userinput>int hs1</userinput>
   Switch(config-if-range)#<userinput>shut</userinput>
   ```

8. VLAN mismatch behavior

   VLAN configuration such as trunk and access mode must be the same on both the ports participating in the ring. For example, if Gi1/0/24 and Gi1/0/23 in an HSR ring are in trunk mode and you attempt to change the mode of one port to access, the ports in the ring will not be bundled:

   ```
   Switch(config)# <userinput>interface range gi1/0/23-24</userinput>
   Switch(config-if-range)# <userinput>switchport mode  access</userinput>
   Jul 27 22:00:27.809 IST: %EC-5-CANNOT_BUNDLE2: Gi1/0/23 is not compatible with Gi1/0/24
    and will be suspended (trunk mode of Gi1/0/23 is access, Gi1/0/24 is dynamic)
   ```

9. MAC flap prevention during HSR ring configuration

   Configuring an HSR ring on two ports of a switch causes MAC flaps on other switches without the HSR configuration. Shut down the newly created HSR ring on the switch, configure the ring on all switches, and then re-enable the rings one at a time. For example, if there are four switches in the ring, disable the HSR ring interfaces on each switch:

   ```
   Switch1(config)# <userinput>interface range gi1/0/21-22</userinput>
   Switch1(config-if-range)# <userinput>shutdown</userinput>
   Switch1(config-if-range)# <userinput>hsr-ring 1</userinput>
   Creating a HSR-ring interface hs1
   Switch1(config-if-range)# <userinput>int hs1</userinput>
   Switch1(config-if-range)# <userinput>shutdown</userinput>
   Switch1(config-if-range)# <userinput>end</userinput>
   ```

   After all four switches are configured with the ring, re-enable the HSR ports on each switch:

   ```
   Switch1# <userinput>conf t</userinput>
   Enter configuration commands, one per line. End with CNTL/Z.
   Switch1(config)# <userinput>interface range gi1/0/21-22</userinput>
   ```

```
Switch1(config-if-range)# <userinput>int hs1</userinput>
Switch1(config-if-range)# <userinput>no shutdown</userinput>
Switch1(config-if-range)# <userinput>end</userinput>
Switch1#
```

This process prevents temporary MAC flapping during HSR ring configuration in member switches.

## HSR-PRP dual RedBox mode

1. Adhere to these restrictions when configuring HSR-PRP Dual RedBox mode to ensure correct operation and avoid loss of connectivity or configuration.
2. Because three ports participate in the HSR-PRP network, only HSR ring 2 can be configured in HSR-PRP mode.
3. Interface assignment is fixed and cannot be changed. Refer to the table above for the assigned interfaces in HSR-PRP mode.
4. When HSR-PRP Dual RedBox mode is configured and enabled, all other ports apart from the 3 HSR-PRP ports are shut down and any feature running on any of these ports will not be functional. You will be warned about this mode change.
5. When HSR-PRP RedBox is active, all other interfaces that are not part of the RedBox remain in the shutdown state and are unusable as long as the RedBox mode is active.
6. Management of the switch through Device Manager is still possible with an in-band SVI interface reachable over the HSR Ring or PRP network. However, there will be loss of connection for a period of time when RedBox mode is enabled or disabled and the device reconfigures itself. Therefore, we highly recommend that you use a console connection when switching into or out of HSR-PRP mode.
7. When HSR-PRP mode is disabled, all physical interfaces will return to their default configuration (that is, configuration on non-RedBox physical ports will be lost).
8. In HSR-PRP mode, by design PRP/HSR channel 1 (gi1/0/21-22) operates in "PRP/HSR disabled" mode. Frames coming into these two ports are passed through to the hardware for switching to the HSR-PRP enabled channel 2. Because channel 1 is not used for PRP or HSR in HSR-PRP mode, the `show prp channel 1 detail` command displays "Protocol = Disabled" even though the Port state displays "Inuse".
9. In HSR-PRP Dual RedBox mode, during reload of the HSR-PRP switch when the traffic is in progress, MAC flaps occur once per source MAC address in the switch that is reloaded and also on the PRP device that is transmitting the traffic. Therefore, if there are 512 different source MAC addresses, then MAC flaps are observed 512 times (once per source MAC address). Also some duplicate packets are seen after this event.

## HSR-HSR QuadBox mode

To ensure correct operation and avoid loss of connectivity or configuration when configuring HSR-HSR QuadBox mode, please adhere to the following restrictions:

1. Interface and Port Assignment: Interface assignment is fixed and cannot be changed. When HSR-HSR QuadBox mode is enabled, all ports other than the four designated HSR-HSR ports are shut down; any features running on those ports will not be functional, and all interfaces not part of the RedBox remain unusable.
2. Management Recommendations: While management via Device Manager is possible using an in-band SVI interface, a connection loss will occur during mode transitions. It is highly recommended to use a console connection when enabling or disabling HSR-HSR mode.

3. Configuration Reset: When HSR-HSR mode is disabled, all physical interfaces will return to their default configuration, meaning any previous configuration on non-QuadBox physical ports will be lost.
4. MAC Address and Packet Handling: To prevent MAC address flapping caused by redundant packets arriving on different rings, MAC address learning is disabled. Because all other ports are shut down, unnecessary flooding of packets does not occur.
5. Topology Consistency: When the topology includes more than one QuadBox, the VLAN and multicast filter configurations must match on all QuadBoxes.
6. Access and MTU Restrictions: Switch port mode access is restricted, the MTU size is fixed at 2020 and cannot be altered, and MAC address table learning for VLANs 1-4094 is disabled.
7. Feature and Command Limitations: PTP is disabled by default (due to no FPGA support). Additionally, `show` and `clear` commands for Node/VDAN tables, `HSR ring proxyNodeTableForgetTime`, `HSR ring nodeforgetTime`, and the creation of independent HSR ring interfaces are restricted in the HSR-HSR profile.
8. Multicast Filter Behavior: Multicast filters are designed to drop only Multicast MACDA; filters set as Unicast MAC addresses will not result in any packet drops.

# Default settings

This topic provides a reference for the default settings and parameters used in HSR ring configurations.

***Table 15: HSR ring parameters***

| Parameter | Description | Range | Default Value |
|---|---|---|---|
| entryForgetTime | Time for clearing an inactive entry from duplicate discard table. | 0-65535 | 400 ms |
| fpgamode-DualUplinkEnhancement | Sets the FPGA register to filter source MAC addresses. | enable or disable | enable |
| nodeForgetTime | Clears an inactive entry from the node table after a set time interval. | 0-65535 | 60000 ms |
| nodeRebootInterval | Specifies when the RedBox starts sending supervision frames after bootup. | 0-65535 | 500 ms |
| pauseFrameTime | Specifies the interval between HSR pause frames. | 0-65535 | 25 ms |

| Parameter | Description | Range | Default Value |
|---|---|---|---|
| proxyNodeTableForgetTime | Clears an inactive entry from the proxy node table or vdan table after a set interval. | 0-65535 | 60000 ms |
| supervisionFrameLifeCheckInterval | Specifies the life check interval for supervision frames. | 0-65535 | 1600 ms |
| supervisionFrameOption | | | |
| mac-da | Specifies the last bytes of the destination MAC address for supervision frames (01:15:4E:00:01:00). The final pair, '00,' is replaced by the value of this parameter. | 1-255 MAC DA last eight bits option value | No default |
| vlan-cfi | Enables the Canonical Format Indicator (CFI) for the VLAN-tagged frame. | enable or disable | disable |
| vlan-cos | Sets the Class of Service (COS) value in the VLAN tag of the supervision frame. | 0-7 | 0 |
| vlan-id | Specifies the VLAN tag for the supervision frame. | 0-4095 | 0 |
| vlan-tagged | Specifies the VLAN tagging option. | enable or disable | disable |
| supervisionFrameRedboxMacaddress | Specifies the RedBox MAC address included in supervision frames. | 48-bit RedBox MAC address | The interface HSR ring MAC address |
| supervisionFrameTime | Specifies the interval between supervision frames. | 0-65535 | 3 ms |

# Configure an HSR ring

Follow these steps to configure an HSR ring:

**Before you begin**

- Read and understand the Guidelines for configuring HSR on IE9300 Series switches, on page 132 section of this chapter.
- Ensure the member interfaces of an HSR ring are not part of redundancy protocols such as FlexLinks, EtherChannel, or REP before configuring the HSR ring.

### Procedure

**Step 1** (Optional) Use the **cdp run** command to globally enable CDP to provide information about HSR ring nodes.

**Step 2** (Optional) Use the **lldp run** command to globally enable LLDP to provide information about HSR ring nodes.

**Step 3** Use the **interface range** *range* command to enter interface configuration mode and disable PTP on the ports to be assigned to the HSR ring.

**Example:**

```
Switch(config)# interface range gi1/0/21-22
Switch(config-if-range)# no ptp enable
```

**Step 4** (Optional) Use the **cdp enable** command to enable CDP on the ports to be assigned to the HSR ring.

**Step 5** (Optional) Use the **lldp transmit** command to enable LLDP on the ports to be assigned to the HSR ring.

**Example:**

```
Switch(config-if-range)# lldp transmit
Switch(config-if-range)# lldp receive
```

**Step 6** Use the **shutdown** command to shut down the ports before configuring the HSR ring.

**Step 7** Use the **interface range** *range* command to create the HSR ring interface and assign the ports to the HSR ring.

**Example:**

```
Switch(config)# interface range gigabitEthernet 1/0/21-22
Switch(config-if-range)# hsr-ring 1
```

**Step 8** (Optional) If required, use the **hsr** *hsr-id* **supervisionFrameLifeCheckInterval** *interval range* command configure HSR ring optional parameters. Refer to the Default Settings section for descriptions of parameters, ranges, and default values.

**Example:**

```
Switch(config-range)# hsr 1 supervisionFrameLifeCheckInterval 10000
```

**Step 9** use the **no shutdown** command to turn on the HSR interface.

**Example:**

```
Switch(config-if-range)# no shutdown
Switch(config-if-range)# end
```

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface range gigabitEthernet 1/0/21-22
Switch(config-if-range)# no ptp enable
Switch(config-if-range)# shutdown
Switch(config-if-range)# hsr-ring 1
Switch(config-if-range)# hsr-ring 1 supervisionFrameLifeCheckInterval 10000
```

```
Switch(config-if-range)# no shutdown
Switch(config-if-range)# end
```

# Enable HSR alarms

Enable or disable alarms and actions for HSR at the facility level. You cannot selectively enable partial or full faults. All alarms for a given facility are either enabled or disabled.

See HSR alarms, on page 121 for details about HSR alarms.

Use this procedure to enable alarms for HSR and configure related notification and logging options.

**Before you begin**

Ensure you have access to the device and the appropriate privileges to configure alarm facilities.

**Procedure**

**Step 1** Use the **configure terminal** command to enter the global configuration mode.

**Step 2** Use the **alarm facility hsr enable** command to enable the HSR alarm facility.

**Note**
Use the **no alarm facility hsr enable** command to disable HSR alarms.

**Step 3** (Optional) Use the **alarm facility hsr notifies** command to enable SNMP notification for HSR alarms.

**Step 4** (Optional) Use the **alarm facility hsr relay major** command to associate HSR alarms with the Major Relay.

**Step 5** (Optional) Use the **alarm facility hsr syslog** command to send HSR alarms to a syslog server.

**Step 6** (Optional) Use the **logging alarm informational** command to enable logging of informational HSR alarm messages.

**Step 7** Use the **logging alarm informational** command to exit global configuration mode.

HSR alarms are enabled and configured as required. You can verify the status using the **show facility-alarm status** command.

# Clear all node table and VDAN table dynamic entries

**Procedure**

**Step 1** Use the **clear hsr node-table** command to clear all dynamic entries in the node table.

**Step 2** Use the **clear hsr vdan-table** command to clear all dynamic entries in the VDAN table.

# HSR verification commands

A HSR verification feature is a diagnostic capability on Cisco switches that

- enables users to confirm the correct configuration and operation of HSR rings,
- provides access to relevant commands and their output for troubleshooting, and
- supports interpretation of filtering, statistics, and neighbor discovery information.

### Command reference for verifying HSR configuration

This table lists the primary commands used to verify HSR ring configuration and their purposes.

*Table 16: HSR verification commands*

| Command | Purpose |
|---|---|
| **show hsr ring 1 [ detail ]** | Shows configuration details for the specified HSR ring. |
| **show hsr statistics { egressPacketStatistics \| ingressPacketStatistics \| nodeTableStatistics \| pauseFrameStatistics}** | Shows statistics for HSR components.<br>**Note**<br>To clear HSR statistics information, use the command **clear hsr statistics**. |
| **show hsr node-table** | Shows HSR node table. |
| **show hsr vdan-table** | Shows HSR Virtual Doubly Attached Node (VDAN) table.<br>**Note**<br>The VDAN table and Proxy node table are the same. |
| **show cdp neighbors** | Shows CDP neighbor information for an HSR ring. |
| **show lldp neighbors** | Shows LLDP neighbor information for an HSR ring. |

### Verifying HSR ocnfiguration and neighbor information

These examples show how to use verification commands and interpret their output for HSR rings, multicast/VLAN filtering, and neighbor discovery.

```
 Switch# show hsr ring detail
HSR-ring listing:
--------------------
HSR-ring: HS1
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2       Maxports = 2
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-hsr
```

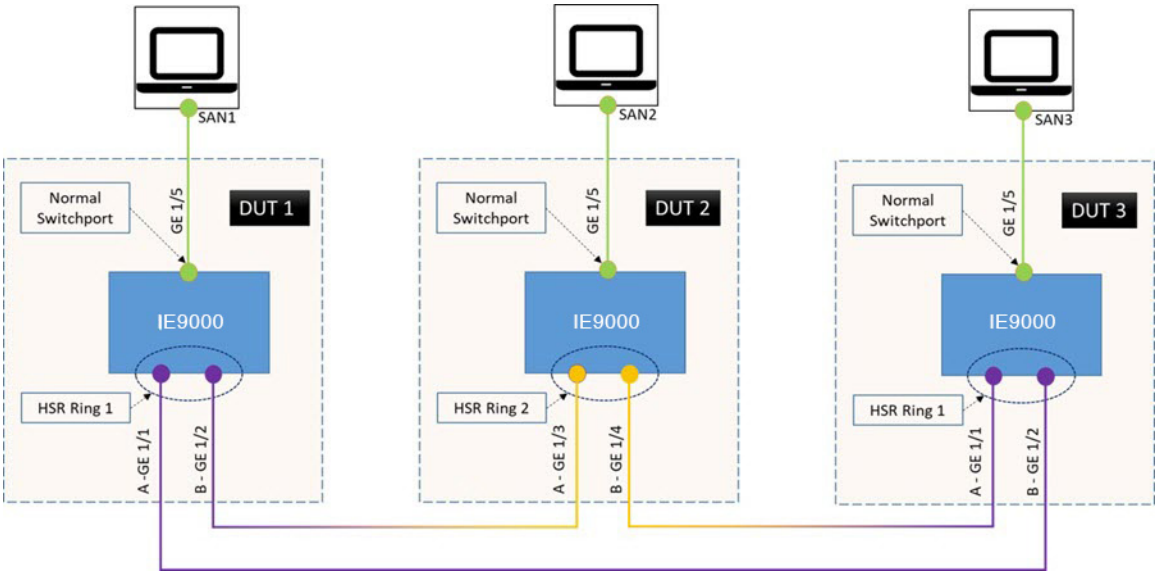
```
Ports in the ring:
1) Port: Gi1/1
Logical slot/port = 1/1      Port state = Inuse
Protocol = Enabled
2) Port: Gi1/2
Logical slot/port = 1/2      Port state = Inuse
Protocol = Enabled
Ring Parameters:
 Redbox MacAddr: 70db.984a.5040
 Node Forget Time: 60000 ms
 Node Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option: 0
 Supervision Frame CFI option: 0
 Supervision Frame VLAN Tag option: Disabled
 Supervision Frame MacDa: 0x00
 Supervision Frame VLAN id: 0
 Supervision Frame Time: 3 ms
 Life Check Interval: 1600 ms
 Pause Time: 25 ms
 fpgamode-DualUplinkEnhancement: Enabled
HSR-ring: HS2
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2       Maxports = 2
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-hsr
Ports in the ring:
1) Port: Gi1/3
Logical slot/port = 1/3      Port state = Inuse
Protocol = Enabled
2) Port: Gi1/4
Logical slot/port = 1/4      Port state = Inuse
Protocol = Enabled
Ring Parameters:
 Redbox MacAddr: 70db.984a.5040
 Node Forget Time: 60000 ms
 Node Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option: 0
 Supervision Frame CFI option: 0
 Supervision Frame VLAN Tag option: Disabled
 Supervision Frame MacDa: 0x00
 Supervision Frame VLAN id: 0
 Supervision Frame Time: 3 ms
 Life Check Interval: 1600 ms
 Pause Time: 25 ms
 fpgamode-DualUplinkEnhancement: Enabled
Switch#
```

```
Switch# show hsr ring multicast-filter
HSR-ring listing:
--------------------
HSR-ring: HS1
---------------
Filter No.  Address         Mask
================================================
2           0000.0100.0a00 ffff.ffff.ffff
HSR-ring: HS2
---------------
Filter No.  Address         Mask
================================================
```

```
5           0000.0100.0b00 0000.0000.0000

Switch# show hsr ring allowed-vlan
HSR-ring listing:
--------------------
HSR-ring: HS1
---------------
Vlan allowed list
----------------------
0-4094
HSR-ring: HS2
---------------
Vlan allowed list
----------------------
0-4094
Switch# show hsr ring multicast-filter-drop
HSR-ring listing:
--------------------
HSR-ring: HS1
---------------
Multicast filter drop count: 0
HSR-ring: HS2
---------------
Multicast filter drop count: 0
Switch# show hsr ring allowed-vlan
HSR-ring listing:
--------------------
HSR-ring: HS1
---------------
Vlan allowed list
----------------------
0-4094
HSR-ring: HS2
---------------
Vlan allowed list
----------------------
0-4094
Switch#
```

This example shows how to check CDP neighbor information for an HSR ring. In this example, there are three switches, and CDP is enabled on all three.




```
DUT 2# sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
DUT 1            Gig 1/3           160              S I   IE-4000-8 Gig 1/2
DUT 3            Fas 1/4           163              S I   IE-4000-8 Gig 1/1
Total cdp entries displayed : 2
```

This example shows how to check LLDP neighbor information for an HSR ring. This example uses the same topology as the previous figure. LLDP is enabled on all three switches.

```
DUT 2# sh lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
DUT 1               Gi1/3          120        B               port-002
DUT 3               Gi1/4          120        B               port-001
Total entries displayed: 2
```

# Configuration examples

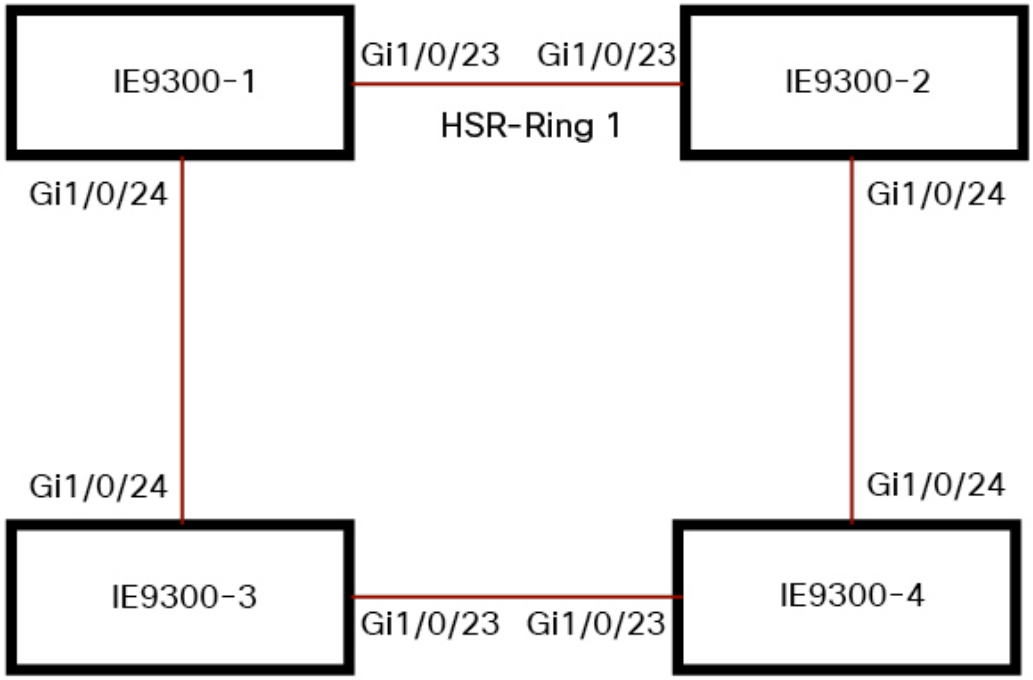
A configuration example is a documentation asset that

- illustrates recommended command-line sequences for configuring features on Cisco IE9300 and S5400 switches,
- includes sample outputs to verify successful configuration for both HSR-SAN and HSR-PRP scenarios, and
- supports users by providing step-by-step command demonstrations for practical reference.

### HSR-SAN

This example shows the configuration of an HSR ring (Ring 1) using Gi1/0/23 and Gi1/0/24 ports between four devices.

***Figure 22: HSR ring configuration with four devices***




```
IE9300-1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IE9300-1(config)# interface range gi1/0/23-24
IE9300-1(config-if-range)# shutdown
IE9300-1(config-if-range)# hsr-ring 1
IE9300-1(config-if-range)# no shutdown
IE9300-1(config-if-range)# end
IE9300-1#
IE9300-2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IE9300-2(config)# interface range gi1/0/23-24
IE9300-2(config-if-range)# shutdown
IE9300-2(config-if-range)# hsr-ring 1
IE9300-2(config-if-range)# no shutdown
IE9300-2(config-if-range)# end
IE9300-2#
IE9300-3# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IE9300-3(config)# interface range gi1/0/23-24
IE9300-3(config-if-range)# shutdown
IE9300-3(config-if-range)# hsr-ring 1
IE9300-3(config-if-range)# no shutdown
IE9300-3(config-if-range)# end
IE9300-3#
IE9300-4# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
IE9300-4(config)# interface range gi1/0/23-24
IE9300-4(config-if-range)# shutdown
IE9300-4(config-if-range)# hsr-ring 1
IE9300-4(config-if-range)# no shutdown
IE9300-4(config-if-range)# end
IE9300-4#
IE9300-1# sh hsr ring 1 detail
HSR-ring: HS1
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2       Maxports = 2
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-san
Ports in the ring:
  1) Port: Gi1/0/23
   Logical slot/port = 1/3      Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/0/24
   Logical slot/port = 1/4      Port state = Inuse
        Protocol = Enabled
Ring Parameters:
 Redbox MacAddr: f454.3365.8a84
 Node Forget Time: 60000 ms
 Node Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option: 0
 Supervision Frame CFI option: 0
 Supervision Frame VLAN Tag option: Disabled
 Supervision Frame MacDa: 0x00
 Supervision Frame VLAN id: 0
 Supervision Frame Time: 3 ms
 Life Check Interval: 2000 ms
 Pause Time: 25 ms
IE9300-2# show hsr ring 1 detail
HSR-ring: HS1
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2       Maxports = 2
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-san
Ports in the ring:
  1) Port: Gi1/0/23
   Logical slot/port = 1/3      Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/0/24
   Logical slot/port = 1/4      Port state = Inuse
        Protocol = Enabled
Ring Parameters:
 Redbox MacAddr: 34c0.f958.ee83
 Node Forget Time: 60000 ms
 Node Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option: 0
 Supervision Frame CFI option: 0
 Supervision Frame VLAN Tag option: Disabled
 Supervision Frame MacDa: 0x00
 Supervision Frame VLAN id: 0
 Supervision Frame Time: 3 ms
 Life Check Interval: 2000 ms
 Pause Time: 25 ms
```

```
IE9300-4# sh hsr ring 1 de
HSR-ring: HS1
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2       Maxports = 2
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-san
Ports in the ring:
  1) Port: Gi1/0/23
   Logical slot/port = 1/3      Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/0/24
   Logical slot/port = 1/4      Port state = Inuse
        Protocol = Enabled
Ring Parameters:
 Redbox MacAddr: f454.3312.5104
 Node Forget Time: 60000 ms
 Node Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option: 0
 Supervision Frame CFI option: 0
 Supervision Frame VLAN Tag option: Disabled
 Supervision Frame MacDa: 0x00
 Supervision Frame VLAN id: 0
 Supervision Frame Time: 3 ms
 Life Check Interval: 2000 ms
 Pause Time: 25 ms
IE9300-3# sh hsr ring 1 detail
HSR-ring: HS1
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2       Maxports = 2
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-san
Ports in the ring:
  1) Port: Gi1/0/23
   Logical slot/port = 1/3      Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/0/24
   Logical slot/port = 1/4      Port state = Inuse
        Protocol = Enabled
Ring Parameters:
 Redbox MacAddr: f454.335c.4684
 Node Forget Time: 60000 ms
 Node Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option: 0
 Supervision Frame CFI option: 0
 Supervision Frame VLAN Tag option: Disabled
 Supervision Frame MacDa: 0x00
 Supervision Frame VLAN id: 0
 Supervision Frame Time: 3 ms
 Life Check Interval: 2000 ms
 Pause Time: 25 ms
```

# Related documents for the IE9300 Series

This section provides references to related documentation and standards for the IE9300 Series and industrial communication networks.

- Cisco Catalyst IE9300 Rugged Series Switch documentation.
- IEC 62439-3 is an international standard titled 'Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).