Redundancy Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches

First Published: 2022-04-26

Last Modified: 2024-04-05

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

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

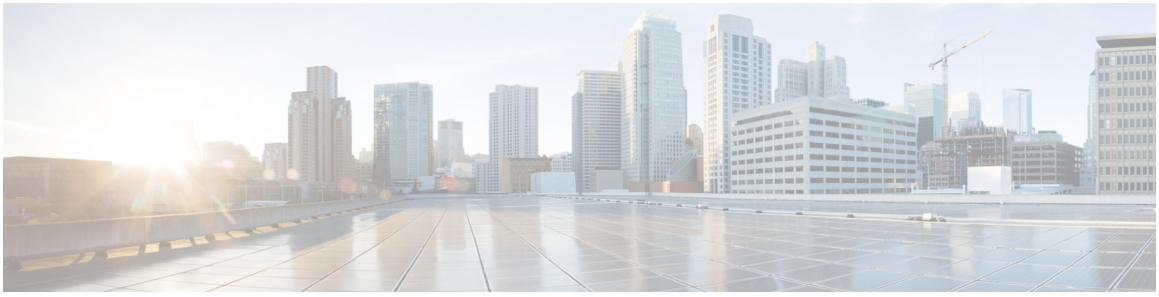
Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

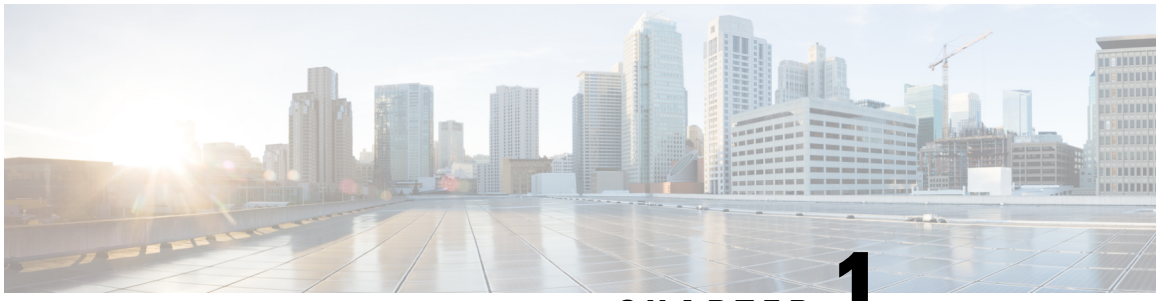
To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Bias Free Language

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.



CONTENTS



CHAPTER 1

Parallel Redundancy Protocol

Information About PRP

Parallel Redundancy Protocol (PRP) is defined in the International Standard IEC 62439-3. PRP is designed to provide hitless redundancy (zero recovery time after failures) in Ethernet networks.

Note PRP is supported on several Cisco Catalyst IE9300 Rugged Series Switches: IE-9320-26S2C-Eand IE-9320-26S2C-A beginning with Cisco IOS XE Cupertino 17,7,1, and IE-9320-22S2C4X-E, and IE-9320-22S2C4X-A beginning with Cisco IOX XE Dublin 17.12.1.

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). These schemes for redundancy can take between a few milliseconds to a few seconds for the network to recover and traffic to flow again.

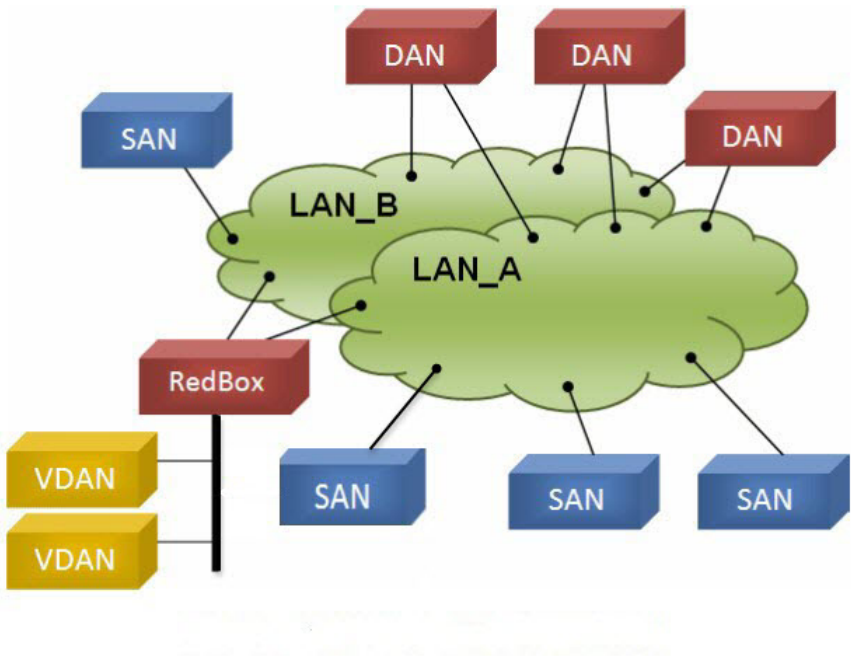
PRP uses a different scheme, where the end nodes implement redundancy (instead of network elements) by connecting two network interfaces to two independent, disjointed, parallel networks (LAN-A and LAN-B). Each of these Dually Attached Nodes (DANs) then have redundant paths to all other DANs in the network.

The DAN sends two packets simultaneously through its two network interfaces to the destination node. A redundancy control trailer (RCT), which includes a sequence number, is added to each frame to help 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 zero recovery time is required.

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

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 on behalf of its VDANs.

Figure 1: PRP Redundant Network



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 the Switch

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

PRP or HSR on a IE9300 Stack

The Parallel Redundancy Protocol (PRP) offers significant advantages in facilitating redundancy with zero downtime. High-availability Seamless Redundancy (HSR) is similar to PRP but is designed to work in a ring topology. While the initial implementation was limited to standalone switches, recent advancements have enabled PRP or HSR to be utilized in stacked configurations.

Benefits of PRP or HSR on a IE9300 Stack

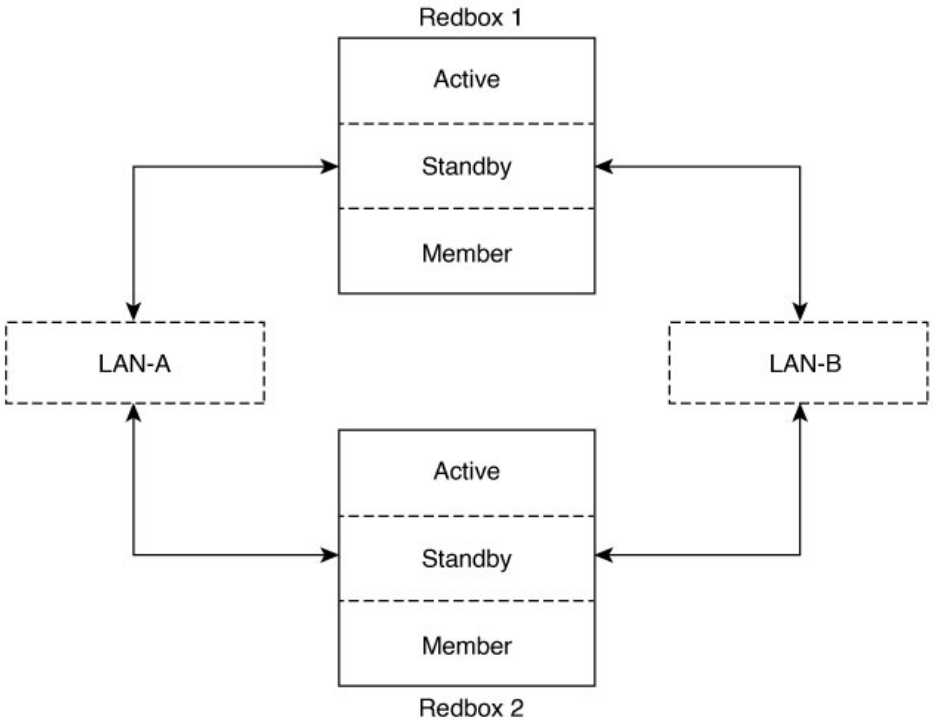
Deploying PRP or HSR in a stacked setup introduces a node level redundancy within the network.

- This enhancement mitigates the risk of single points of failure.
- Ensures the system remains operational even if a stack member or the active switch fails.
- The functionality and behavior of PRP and HSR remain consistent in both standalone and stacked configurations.
- Provides seamless integration and reliability across the network.

For more information on Switch Stacks, see Managing Switch Stacks.

Note There are no changes to the functionality or behavior of PRP and HSR when implemented in a IE9300 stack compared to their standalone configurations.

The following illustration displays a IE9300 stack as a RedBox.



Note A maximum of four-member stack can be configured with PRP or HSR as RedBox.

Guidelines and Limitations

The following guidelines and limitations apply:

- You can create any one of the following configurations:
  - HSR: Maximum of two rings

    or
  - PRP: Maximum of two channels

    or
  - One HSR ring and one PRP channel
- PRP and HSR are supported on IE-9320-26S2C and IE-9320-22S2C4X only.
- PRP and HSR on IE9300 stack is supported only if both the active and standby switches are FPGA-based SKUs.
- Both ports of a channel and a ring must be on the same slot, that is, the primary and secondary interfaces must be on the same switch member.
- When PRP or HSR is configured on the active unit and the switch goes down, it remains unavailable until the switch is restored.

Active-Standby Synchronization Mechanism Post-Switchover

Synchronization of the PRP or HSR to a redundant standby, supportis both incremental and bulk synchronization updates.

The behavior of PRP channel or HSR ring when a switch goes down, is as follows:

- If the channel or ring is configured on the standby switch, it will synchronize with the previous states of the channel or ring from the last active configuration.
- If the channel or ring is configured on the active switch, it will transition to a down state due to the slot being inactive. Once the slot is reactivated, the volatile FPGA will be reprogrammed with the previously configured values.

PRP Channels

PRP channel or channel group is a logical interface that aggregates two Gigabit Ethernet interfaces (access, trunk, or routed) into a single link. In the channel group, the lower numbered Gigabit Ethernet member port is the primary port and connects to LAN-A. The higher numbered port is the secondary port and connects to LAN-B.

The PRP channel remains up as long as at least one of these member ports remains up and sends traffic. When both member ports are down, the channel is down. The total number of supported PRP channel groups is 2

per switch. The interfaces that you can use for each group on each switch series are fixed, as shown in the following table.

PRP Channel Number	IE9300 Series
PRP Channel 1	Gi1/0/21 (LAN-A) and Gi1/0/22 (LAN-B)
PRP Channel 2	Gi1/0/23 (LAN-A) and Gi1/0/24 (LAN-B)

Mixed Traffic and Supervision Frames

Traffic egressing the RedBox PRP channel group can be mixed, that is, destined to either SANs (connected only on either LAN-A or LAN-B) or DANs. To avoid duplication of packets for SANs, the switch learns source MAC addresses from received supervision frames for DAN entries and source MAC addresses from non-PRP (regular traffic) frames for SAN entries and maintains these addresses in the node table. When forwarding packets out the PRP channel to SAN MAC addresses, the switch looks up the entry and determines which LAN to send to rather than duplicating the packet.

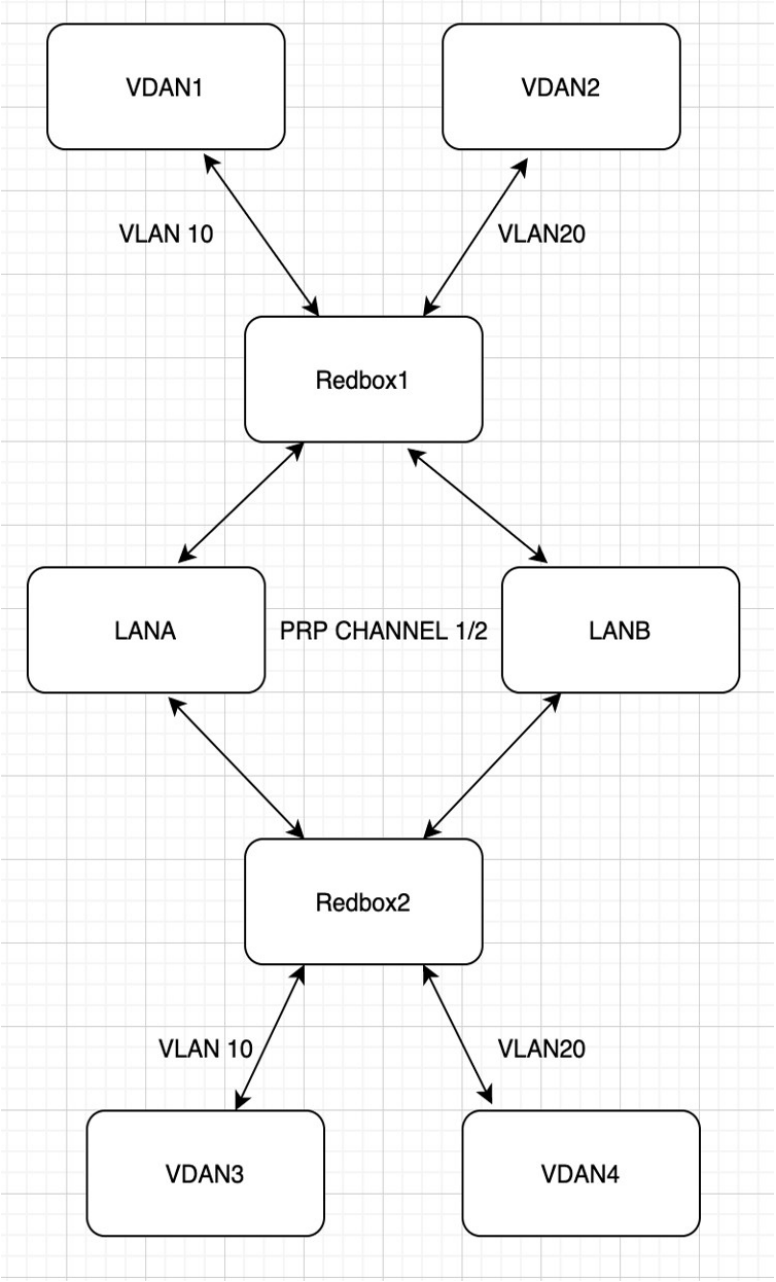
A RedBox with VDANs needs to send supervision frames on behalf of those VDANs. For traffic coming in on all other ports and going out PRP channel ports, the switch learns source MAC addresses, adds them to the VDAN table, and starts sending supervision frames for these addresses. Learned VDAN entries are subject to aging.

You can add static entries to the node and VDAN tables as described in x. You can also display the node and VDAN tables and clear entries. See y and z.

VLAN Tag 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.

In the example configuration 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.



See Configuring PRP Channel with Supervision Frame VLAN Tagging, on page 17 for configuration information.

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, and IE-9320-22S2C4X-E 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 the following conditions are met:

- The Network Advantage license is required to use TrustSec.
- Configure TrustSec on each interface first, before it is part of the PRP channel.
- The TrustSec configuration on both PRP channel interfaces must be the same to allow inline tagging and propagation with LAN-A and LAN-B as expected.

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

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** <>.

Valid Configuration

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
```

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
```

Invalid Configuration

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 lists **show** commands that you can use when configuring TrustSec on PRP member interfaces and examples of some command outputs:

- **show cts interface summary**
- **show cts pacs**
- **show cts interface <>**
- **show cts role-based counters**
- **show prp channel detail**
- **show prp statistics ingressPacketStatistics**
- **show prp statistics egressPacketStatistics**

The following example show the output of the **show cts interface summary** command:

```
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 1F577DC7E176855650F2F5609418AC60006009C000301002BBB79441FEE97B0E0B339B9036F9C7100000001364C8D
1A000093A8054BC5FA1780A24E23B60A4BFF46AF47A317EE20391BFCA6F0CAABA7F66393F05799A3B0EAB602B54749DCF7225A45FDDB1349A81977D857B9C3
```

```
1959A2B54CFC4505CD903D84394E69E5795D31543BB575FB8D51A6FA021FB5E6A0C296F8CA213183776880735167141125D38973D9BF2A66792E3AD1C0A05C3
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.
```

The following example shows the output of the **show cts role-based counters** command:

```
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
```

The following example shows the output of the **show prp channel detail** command:

```
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
```

The following example shows the output of the **show prp statistics ingressPacketStatistics** command:

```
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
```

The following example shows the output of the **show prp statistics egressPacketStatistics** command:

```
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
```

TrustSec Debugging Commands

This section lists **debug** commands that you can use when troubleshooting TrustSec on PRP member interfaces.

- **debug prp errors**
- **debug prp events**
- **debug prp detail**
- **debug cts error**
- **debug cts aaa**
- **debug cts all**

Prerequisites

- IE-9320-26S2C-A, IE-9320-26S2C-E, IE-9320-22S2C4X-A, or IE-9320-22S2C4X-E switch
- Network Essentials or Network Advantage License

- Cisco IOS XE 17.7.1 or greater for two-channel PRP support

Guidelines and Limitations

Guidelines

- Because PRP DANs and RedBoxes add a 6-byte PRP trailer to the packet, 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 as follows: **system mtu 1506**.
- To configure supervision frame VLAN tagging, you must configure interfaces in trunk mode.

Note 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 system displays this message:

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

- A PRP channel must have two active ports that are configured within a channel to remain active and maintain redundancy.
- Both interfaces within a channel group must have the same configuration.
- For Layer 3, you must configure the IP address on the PRP channel interface.
- UDLD must be disabled on interfaces where PRP is enabled, especially if the interfaces have media-type sfp.
- 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 converge time in PRP LAN-A and LAN-B.
- 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.
- For Cisco Catalyst IE9300 Rugged Series Switches, use the **int Gi1/0/23** or **int Gi1/0/24**, as shown in the following example:

```
switch(config)#int Gi1/0/23
switch(config-if)#shut
%Interface GigabitEthernet1/0/23 is configured in PRP-channel group, shutdown not
permitted!
```

- PRP functionality can be managed using the CIP protocol. The following CIP commands for PRP are available on:

- show cip object prp <*0-2*>
- show cip object nodetable <*0-2*>

Limitations

- PRP is supported only on IE-9320-26S2C-A, IE-9320-26S2C-E, IE-9320-22S2C4X-AIE-9320-22S2C4X-E switches.
- PRP traffic load cannot exceed 90 percent bandwidth of the Gigabit Ethernet interface channels.
- Load-balancing is not supported.
- 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.

  The following example shows output for Cisco Catalyst IE9300 Rugged Series Switches:

  .

  ```
  show prp channel 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 = 1/21 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
  ```

- 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.

  The following example shows the output for the **show prp channel** command:

  ```
  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 = 1/23 Port state = Inuse
 Protocol = Enabled
  2) Port: Gi1/0/24
   Logical slot/port = 1/24 Port state = Inuse
 Protocol = Enabled
```

Node and VDAN Tables

- The switch supports up to 512 (SAN+DANP) entries in the node table.
- The maximum static Node/VDAN count is 16.
- 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 will temporarily treat the unlearned node as a DAN and duplicate the egress packets until an ingress packet or supervision frame is received from the node to populate an entry into 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.

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 4.

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 4.
- Review the Prerequisites, on page 11 and Guidelines and Limitations, on page 12.
- 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.

SUMMARY STEPS

1. Enter global configuration mode:
2. Assign two Gigabit Ethernet interfaces to the PRP channel group. For channel 1, enter:
3. (Optional) For Layer 2 traffic, enter **switchport**. (Default):
4. (Optional) Set a nontrunking, nontagged single VLAN Layer 2 (access) interface:

5. (Optional) Create a VLAN for the Gigabit Ethernet interfaces:
6. (Optional) Disable Precision Time Protocol (PTP) on the switch:
7. Disable loop detection for the redundancy channel:
8. Disable UDLD for the redundancy channel:
9. Enter subinterface mode and create a PRP channel group:
10. Bring up the PRP channel:
11. Specify the PRP interface and enter interface mode:
12. Configure bpdufilter on the prp-channel interface:
13. (Optional) Configure LAN-A/B ports to quickly get to FORWARD mode:

DETAILED STEPS

Procedure

Step 1 Enter global configuration mode:

configure terminal

Step 2 Assign two Gigabit Ethernet interfaces to the PRP channel group. For channel 1, enter:

interface range GigabitEthernet1/1/0/21-22

For channel 2, enter:

interface range GigabitEthernet21/0/23-24

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 3 (Optional) For Layer 2 traffic, enter **switchport**. (Default):

switchport

Note For Layer 3 traffic, enter **no switchport**.

Step 4 (Optional) Set a nontrunking, nontagged single VLAN Layer 2 (access) interface:

switchport mode access

Step 5 (Optional) Create a VLAN for the Gigabit Ethernet interfaces:

switchport access vlan <*value*>

Note This step is required only for Layer 2 traffic.

Step 6 (Optional) Disable Precision Time Protocol (PTP) on the switch:

no ptp enable

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

Step 7 Disable loop detection for the redundancy channel:

no keepalive

Step 8 Disable UDLD for the redundancy channel:

udld port disable

Step 9 Enter subinterface mode and create a PRP channel group:

prp-channel-group *prp-channel group*

prp-channel group: Value of 1 or 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 10 Bring up the PRP channel:

no shutdown

Step 11 Specify the PRP interface and enter interface mode:

interface prp-channel *prp-channel-number*

prp-channel-number: Value of 1 or 2

Step 12 Configure bpdufilter on the prp-channel interface:

spanning-tree bpdufilter enable

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 13 (Optional) Configure LAN-A/B ports to quickly get to FORWARD mode:

spanning-tree portfast edge trunk

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

The following 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
```

Configuring PRP Channel with Supervision Frame VLAN Tagging

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

Before you begin

- Review the specific interfaces supported for each switch type, as described in PRP Channels, on page 4.
- Review the Prerequisites, on page 11 and Guidelines and Limitations, on page 12.
- 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.

SUMMARY STEPS

1. Enter global configuration mode:
2. Assign two Gigabit Ethernet interfaces to the PRP channel group. For channel 1, enter:
3. Configure the PRP interface for trunk administrative mode, to allow the interface to carry traffic for more than one VLAN.
4. Specify the allowed VLANS for the trunk interface:
5. (Optional) Disable Precision Time Protocol (PTP) on the switch:
6. Disable loop detection for the redundancy channel:

7. Disable UDLD for the redundancy channel:
8. Enter sub-interface mode and create a PRP channel group:
9. Bring up the PRP channel:
10. Specify the PRP interface and enter interface mode:
11. Configure bpdufilter on the prp-channel interface:
12. Set the VLAN ID to be used in VLAN tags for supervision frames:
13. (Optional) Configure the Class of Service (COS) value to be set in the VLAN tag of the Supervision frame:
14. Enable VLAN tagging on the interface:
15. (Optional) Configure LAN-A/B ports to quickly get to FORWARD mode:

DETAILED STEPS

Procedure

Step 1 Enter global configuration mode:

configure terminal

Step 2 Assign two Gigabit Ethernet interfaces to the PRP channel group. For channel 1, enter:

interface range {**{GigabitEthernet1/0/21-22}**

For channel 2, enter:

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. So, 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 3 Configure the PRP interface for trunk administrative mode, to allow the interface to carry traffic for more than one VLAN.

switchport mode trunk

Step 4 Specify the allowed VLANS for the trunk interface:

switchport trunk allowed vlan *value*

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

Step 5 (Optional) Disable Precision Time Protocol (PTP) on the switch:

no ptp enable

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

Step 6 Disable loop detection for the redundancy channel:

no keepalive

Step 7 Disable UDLD for the redundancy channel:

udld port disable

Step 8 Enter sub-interface mode and create a PRP channel group:

prp-channel-group *prp-channel group*

prp-channel group: Value of 1 or 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 9 Bring up the PRP channel:

no shutdown

Step 10 Specify the PRP interface and enter interface mode:

interface prp-channel *prp-channel-number*

prp-channel-number: Value of 1 or 2

Step 11 Configure bpdufilter on the prp-channel interface:

spanning-tree bpdufilter enable

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

Step 12 Set the VLAN ID to be used in VLAN tags for supervision frames:

prp channel-group *prp-channel-number* **supervisionFrameOption vlan-id** *value*

prp-channel-number: Value of 1 or 2

value: VLAN number from 0 to 4095

Step 13 (Optional) Configure the Class of Service (COS) value to be set in the VLAN tag of the Supervision frame:

prp channel-group *prp-channel-number* **supervisionFrameOption vlan-cos** *value*

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

Step 14 Enable VLAN tagging on the interface:

prp channel-group *prp-channel-number* **supervisionFrameOption vlan-tagged** *value*

prp-channel-number: Value of 1 or 2

Step 15 (Optional) Configure LAN-A/B ports to quickly get to FORWARD mode:

spanning-tree portfast edge trunk

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.

Example

```
REDBOX1# configure terminal
REDBOX1(config)#int range GigabitEthernet1/0/21-22
REDBOX1(config-if)#switchport mode trunk
REDBOX1(config-if)#switchport trunk allowed vlan 10,20
REDBOX1(config-if)# no ptp enable
REDBOX1(config-if)# no keepalive
REDBOX1(config-if)# udld port disable
REDBOX1(config-if)# no shutdown
REDBOX1(config-if)# prp-channel-group 1
REDBOX1(config-if)# exit
REDBOX1(config)#prp channel-group 1 supervisionFrameOption vlan-tagged
REDBOX1(config)#prp channel-group 1 supervisionFrameOption vlan-id 10
REDBOX1(config)# spanning-tree bpdufilter enable
REDBOX1(config-if)#spanning-tree portfast edge trunk
```

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.

SUMMARY STEPS

1. Enter global configuration mode:
2. 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):
3. Specify the MAC address to add to the VDAN table:

DETAILED STEPS

Procedure

Step 1 Enter global configuration mode:

configure terminal

Example:

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

Step 2 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 *prp-channel group* **nodeTableMacaddress** *mac-address* {dan | lan-a | lan-b}

prp-channel group: Value of 1 or 2

mac-address: MAC address of the node

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

Step 3 Specify the MAC address to add to the VDAN table:

prp channel-group *prp-channel group* **vdanTableMacaddress** *mac-address*

prp-channel group: Value of 1 or 2

mac-address: MAC address of the node or VDAN

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

Clearing All Node Table and VDAN Table Dynamic Entries

SUMMARY STEPS

1. Clear all dynamic entries in the node table by entering the following command:
2. Clear all dynamic entries in the VDAN table by entering the following command:

DETAILED STEPS

Procedure

Step 1 Clear all dynamic entries in the node table by entering the following command:

clear prp node-table [**channel-group** *group*]

Step 2 Clear all dynamic entries in the VDAN table by entering the following command:

clear prp vdan-table [**channel-group** *group*]

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** command shown in Add Static Entries to the Node and VDAN Tables, on page 20.

Disabling the PRP Channel and Group

SUMMARY STEPS

1. Enter global configuration mode:
2. Disable the PRP channel:
3. Exit interface mode:

DETAILED STEPS

Procedure

Step 1 Enter global configuration mode:

configure terminal

Step 2 Disable the PRP channel:

no interface prp-channel *prp-channel-number*

prp-channel number: Value of 1 or 2

Step 3 Exit interface mode:

exit

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 so that errors and warnings become syslogs. Doing so enables you to turn the syslogs into Simple Network Management Protocol (SNMP) traps for proper alerting and maintenance.

The following errors and warnings can be configured to become syslogs:

- 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

The parameters in the procedure list are captured from the output of the CLI command **sh prp statistics ingressPacketStatistics**.

You use CLI commands to configure the interval that syslogs are generated, from 60 seconds to 84,400 seconds. The default is 300 seconds. See the section Configure the PRP Logging Interval, on page 23 in this guide 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 is 300 seconds; however, you can choose a value from 60 seconds to 84,400 seconds.

Before you begin

Procedure

At the configuration prompt, enter the following command: **prp logging-interval** ***interval_in_seconds***

To choose the default interval of 300 seconds, do not enter a value. Enter one only to specify a logging inteval other than the 300-second default.

Example:

```
cl_2011#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cl_2011(config)#prp logging-interval 120
```

The switch generates syslogs from the PRP errors and warnings listed in the section Errors and Warnings as Syslog Messages , on page 22.

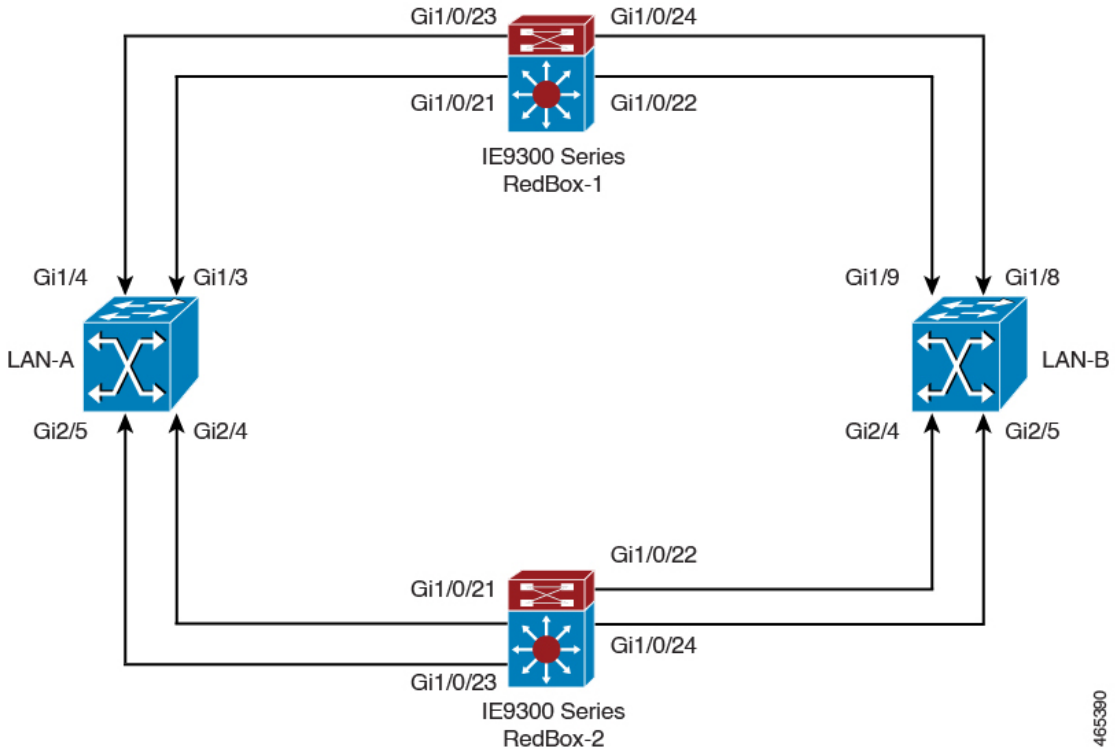
Example

The following text shows sample output resulting from the 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
```

Configuration Examples

The following 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.



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.

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
 shutdown
!
interface GigabitEthernet1/4
 switchport access vlan 25
 switchport mode access
!
interface GigabitEthernet1/5
 switchport access vlan 35
 switchport mode access
!
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 25
 switchport mode access
!
interface GigabitEthernet2/5
 switchport access vlan 35
 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
 shutdown
!
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
 no ptp enable
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
```

```
interface GigabitEthernet1/0/24
switchport access vlan 25
no ptp enable
prp-channel-group 2
spanning-tree bpdufilter enable

!
interface AppGigabitEthernet1/1
!
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 GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!

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 GigabitEthernet1/5
!
interface GigabitEthernet1/6
 description **** tftp connection ****
 switchport access vlan 100
 switchport mode access
 shutdown
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
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 AppGigabitEthernet1/1
!
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
!
!
!
```

VLAN Tagging Example

The following 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 Configuration

This section lists commands that you can use to verify PRP configuration and examples of those commands.

Command	Purpose
show prp channel {**1** | **2** [**detail** | **status** | **summary**] | **detail** | **status** | **summary**}	Displays configuration details for a specified PRP channel.
show prp control {**VdanTableInfo** | **ptpLanOption** | **ptpProfile** | **supervisionFrameLifeCheckInterval** | **supervisionFrameOption** | **supervisionFrameRedboxMacaddress** | **supervisionFrameTime**}	Displays PRP control information, VDAN table, and supervision frame information.
show prp node-table [**channel-group** <**group**> | **detail**]	Displays PRP node table.
show prp statistics {**egressPacketStatistics** | **ingressPacketStatistics** | **nodeTableStatistics** | **pauseFrameStatistics** | **ptpPacketStatistics**}	Displays statistics for PRP components.
show prp vdan-table [**channel-group** <**group**> | **detail**]	Displays PRP VDAN table.
show interface prp-channel {**1** | **2**}	Displays information about PRP member interfaces.

Note The **show interface G1/0/21** or **show interface G1/0/22** command should not be used to read PRP statistics if these interfaces are PRP channel members because the counter information can be misleading. Use the **show interface prp-channel** [**1** | **2**] command instead.

The following example shows the output for **show prp channel** 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
```

The following 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
```

The following example shows output for the **show prp control supervisionFrameOption** command with and without VLAN tagging added to the PRP channel. A `VLAN value` field of 1 means that VLAN tagging is enabled, and a value of 0 means that VLAN tagging is disabled.

```
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
PRP channel-group 2 Super Frame Option
  COS value is 0
  CFI value is 0
  VLAN value is 0
  MacDA value is 0
  VLAN id value is 0

REDBOX1#
```

The following example shows the command to determine if the switch has been configured so that errors and warnings to become syslogs:

```
switch #sh prp control logging-interval
 PRP syslog logging interval is not configured
```

The following example shows the command for configuring the logging interval to the default, 300 seconds.

```
switch #conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
switch(config)#prp logging-interval
switch(config)#do sh prp control logging-interval
 PRP syslog logging interval is 300 in seconds
```

The following example shows the command for configuring the logging interval to 600 seconds.

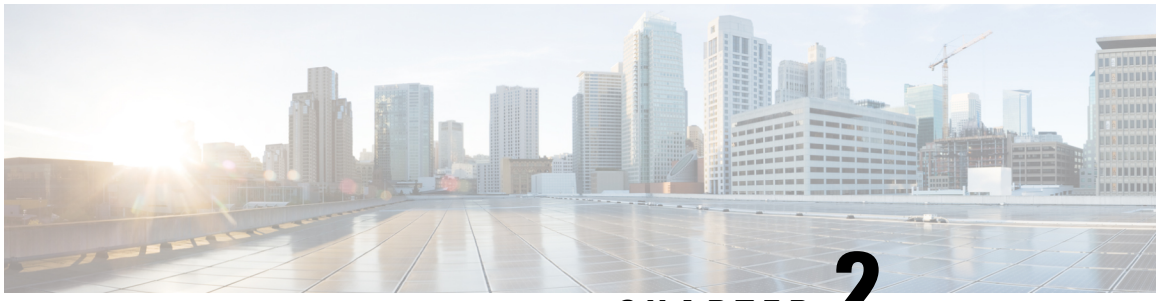
```
switch(config)#prp logging-interval 600
 PRP syslog logging interval is 600 in seconds

switch(config)#
```

Related Documents

Additional documentation—including Release Notes, installation instructions, and configuration guides—is available on the Cisco Catalyst IE9300 Rugged Series Switches page on cisco.com.

Feature History

Release	Feature Name	Feature Information
Cisco IOS XE Dublin 17.12.1	Parallel Redundancy Protocol	This feature became available on Cisco Catalyst IE9300 Rugged Series Switches IE-9320-22S2C4X-A and IE-9320-22S2C4X-E.
	PTP over PRP	This feature became available on Cisco Catalyst IE9300 Rugged Series Switches IE-9320-22S2C4X-A and IE-9320-22S2C4X-E.
Cisco IOS XE Cupertino 17.9.1	PTP over PRP	This feature became available on Cisco Catalyst IE9300 Rugged Series Switches IE-9320-26S2C-A and IE-9320-26S2C-E.
Cisco IOS XE Cupertino 17.7.1	Parallel Redundancy Protocol	This feature became available on Cisco Catalyst IE9300 Rugged Series Switches IE-9320-26S2C-A and IE-9320-26S2C-E.



CHAPTER 2

PTP over PRP

PTP over PRP

Precision Time Protocol (PTP) can operate over Parallel Redundancy Protocol (PRP) on Cisco Catalyst IE9300 Rugged Series Switches. The feature is supported on IE-9320-26S2C-A and IE-9320-26S2C-E switches beginning with Cisco IOS XE Cupertino 17.9.1. It is supported on IE-9320-22S2C4X-A, and IE-9320-22S2C4X-E switches beginning with Cisco IOS XE Dublin 17.12.1.

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

The PRP method of achieving redundancy by parallel transmission over two independent paths does not work for PTP as it does for other traffic. The delay that a frame experiences is not the same in the two LANs, and 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 not obliged to forward the RCT, which is a message part that comes after the payload.

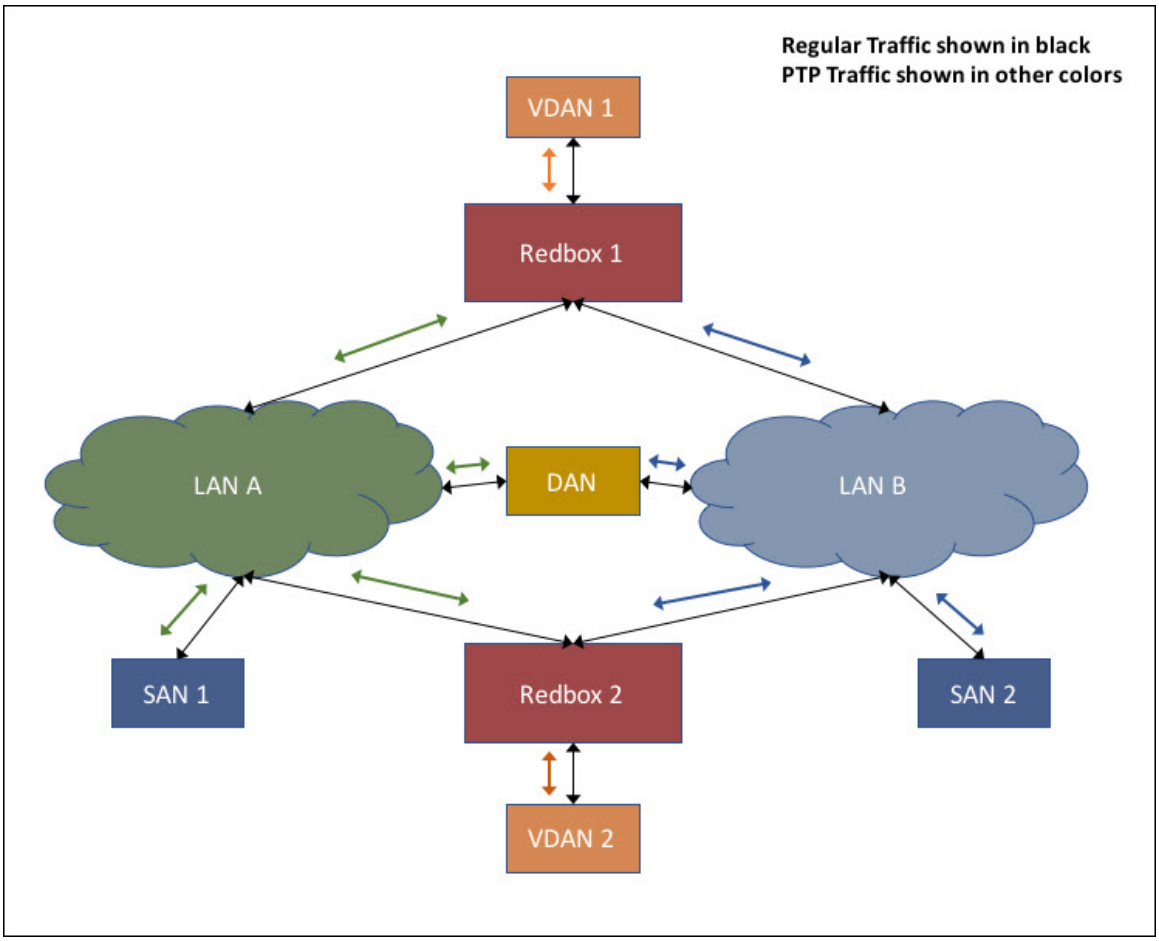
Before support of PTP over LAN-A and LAN-B, PTP traffic was allowed only on LAN-A to avoid the issues with PTP and parallel transmission described earlier. However, if LAN-A went down, PTP synchronization was lost. To enable PTP to leverage the benefit of redundancy offered by the underlying PRP infrastructure, 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.

PTP over PRP Packet Flow

The following figure illustrates the operation of PTP over PRP.

Figure 2: 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 of the ports (referred to as time recipient) is used to synchronize the local clock (VDAN 2 in the figure). While the LAN-A port is the time recipient, the LAN-A port's virtual clock is used to synchronize VDAN-2. The other PRP port, LAN-B, is referred to as PASSIVE. The LAN-B port's virtual clock is still synchronized to the same GMC, but is not used to 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.

Due to the change, VDAN 2 may experience an instantaneous shift in its clock due to the offset between the LAN-A port's virtual clock and the LAN-B port's virtual clock. The magnitude of the shift should only be a few microseconds at the most, because both clocks are synchronized to the same GMC. The shift also occurs when the LAN-A port comes back 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 the following:

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

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

PTP over PRP does not require configuration beyond how you would normally configure PTP and PRP separately, and there is no user interface added for this feature. The difference is that before the PTP over PRP feature, PTP worked over LAN-A only; now it works over both LANs. Before implementing PTP over PRP, refer to Guidelines and Limitations.

The high-level workflow to implement PTP over PRP in your network is as follows:

1. Refer to the section PRP 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, following the procedure for the PTP profile determined in step 1.
3. Configure PRP as described in 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.

Supported PTP Profiles and Clock Modes

The following 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

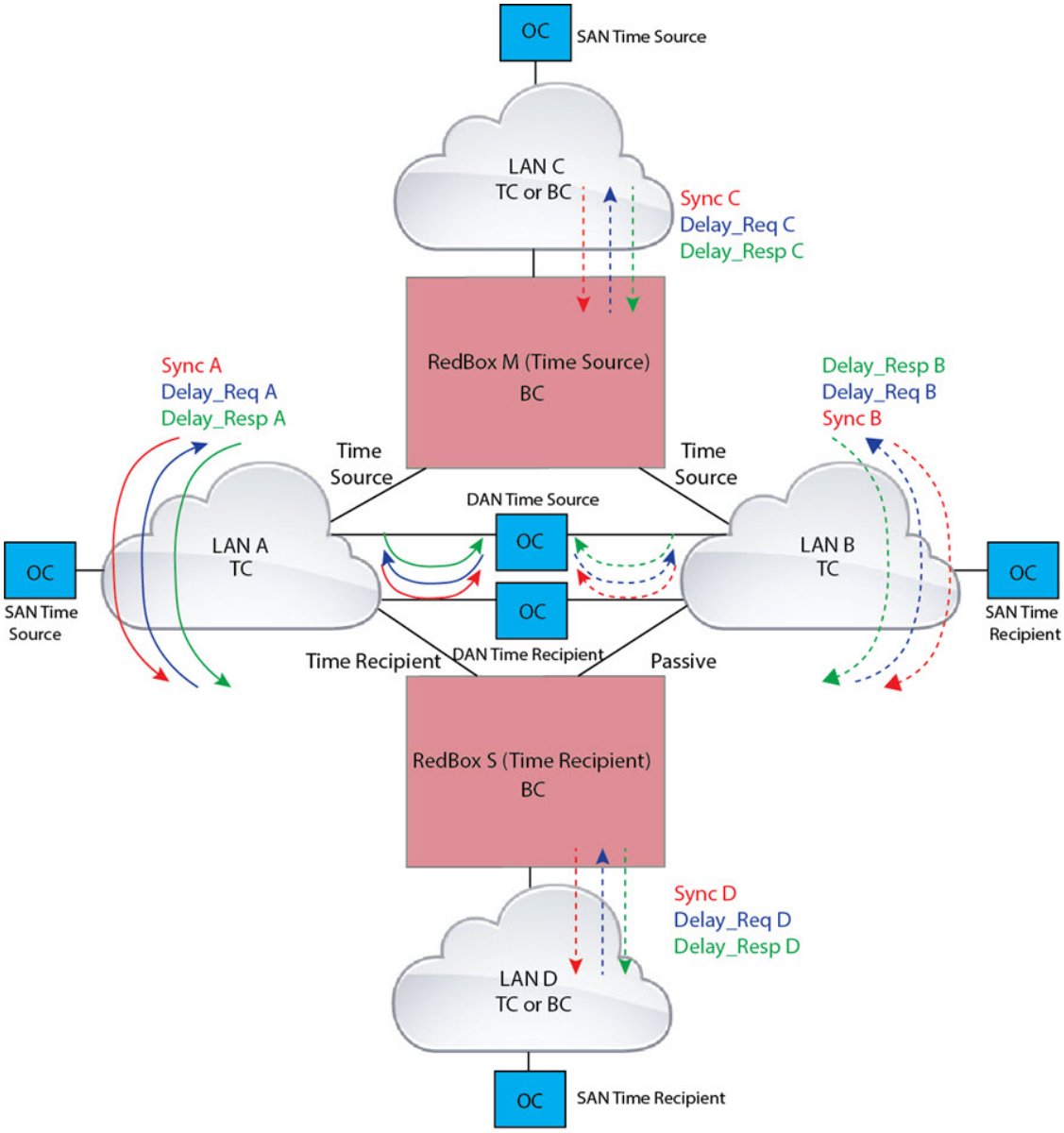
PRP RedBox Types

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 a Doubly Attached BC (DABC) with E2E

In the configuration shown below, two RedBoxes (for example, M and S) are configured as Boundary Clocks (BCs) that use the End-to-End delay measurement mechanism and IEEE1588v2 Default Profile. The Best Master Clock Algorithm (BMCA) on RedBox M determines port A and port B to be connected to the time source. The PTP protocol running on Redbox M treats both ports A and B individually as time source ports and sends out Sync and Follow_Up messages individually on both the ports.

Figure 3: PRP Redbox as DABC with E2E



On Redbox S, the regular BMCA operation determines port A to be a 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 as follows:

- 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.

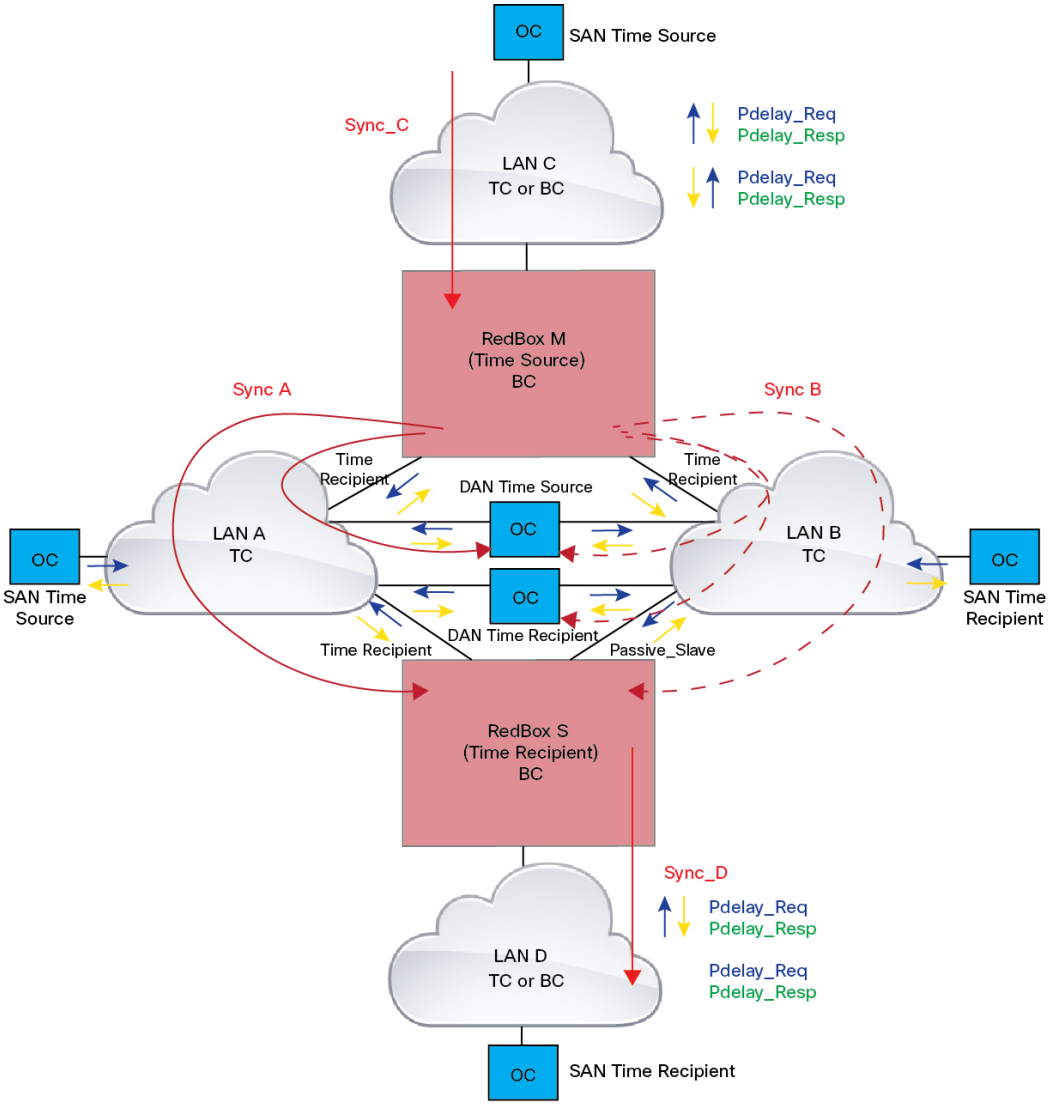
It is passive in the sense that it maintains the calculated delay and offset, but does not perform any operation on the local clock. Having the delay and offset information readily available equips it to seamlessly change its role to time recipient if there is loss of connectivity to the time source on port A.

PRP RedBox as Doubly Attached BC (DABC) with P2P

The following figure shows an example where Redbox M and Redbox S are configured to run in Power Profile as Boundary Clocks that use Peer-to-Peer (P2P) delay measurement mechanism. In this example, the GMC is the ordinary clock attached through LAN C. 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 M determines ports A and B to be connected to the time source. The PTP protocol running on Redbox M treats both ports A and B individually as time source ports and sends out Sync and Follow_Up messages individually on both the ports.

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 as follows:

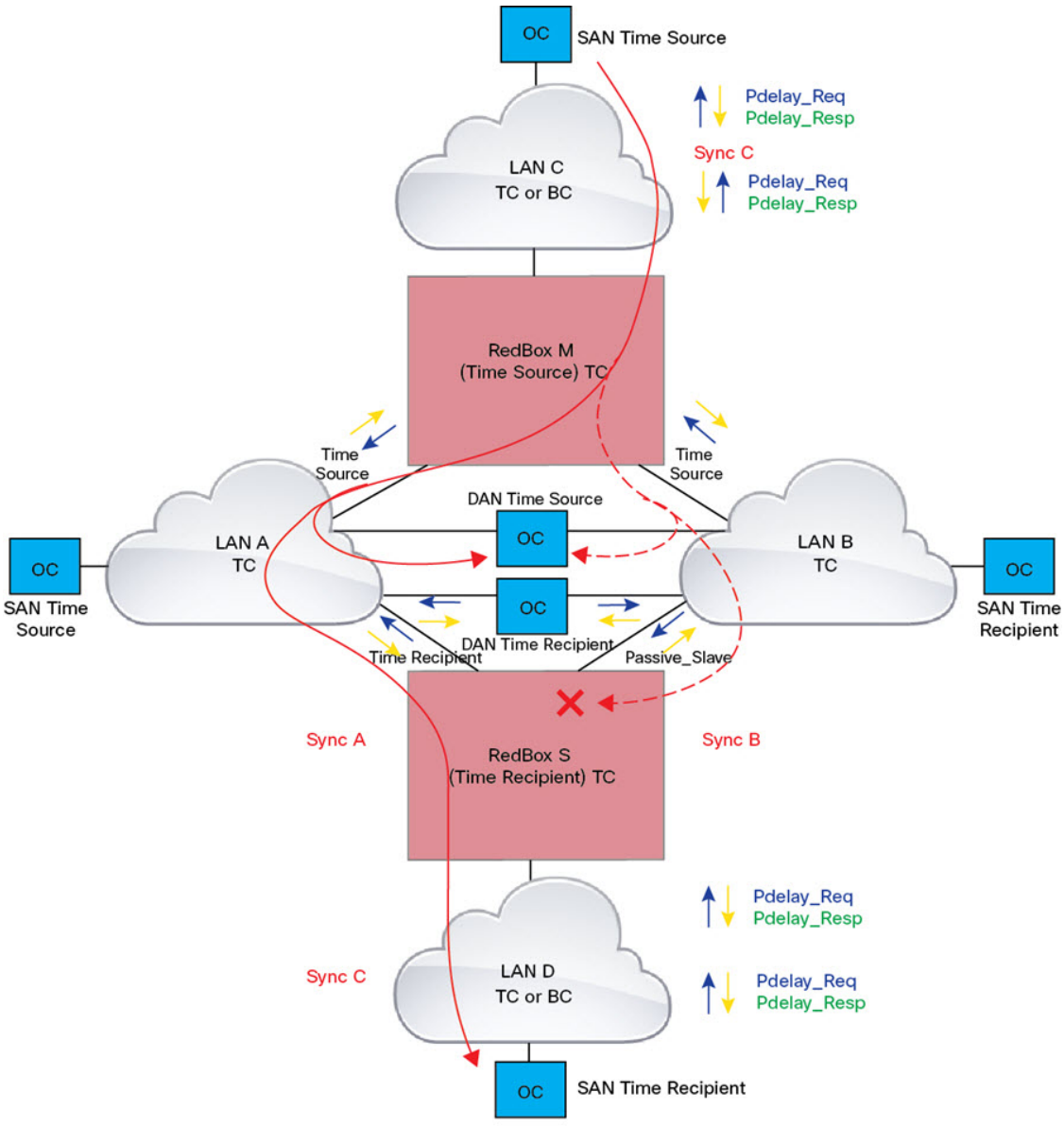
- Port A works as a regular time recipient port. It uses the Sync and Follow_Up messages along with their correction field to calculate the delay and offset from time source and synchronize the local clock. (Unlike an E2E BC, it does not need to generate Delay_Req messages because all the link delays 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 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 port A loses communication with the GM.

PRP RedBox as Doubly Attached TC (DATC) with P2P

The following 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 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.

Redbox M and Redbox S run BMCA even though it is not mandatory for a P2P TC 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 5: PRP Redbox as DATC with P2P



On Redbox S, port A is determined to be time recipient and port B to be 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 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 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.

Using the example that is shown in PRP RedBox as DATC with P2P with the GMC as a SAN in LAN C, a failure in LAN-A or LAN-B pertaining to PTP can occur due to the following reasons:

- A device within the LAN goes down.
- A link within the LAN goes down resulting in loss of connectivity.
- 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.

The BMCA, once invoked, changes the state of the PASSIVE_SLAVE port to time recipient and time recipient to PASSIVE_SLAVE or PASSIVE or FAULTY. The state changes are done atomically to avoid transient cases where there are 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

If you have enabled PTP over PRP on a switch, you can use certain CLI **show** commands to see data for the PTP clock specific for PRP.

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

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
```

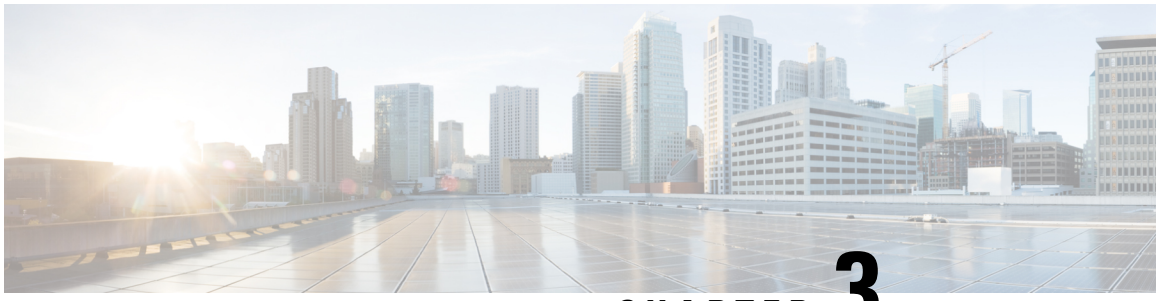
The following example sets a PTP clock boundary domain for a power profile:

```
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 3

Resilient Ethernet Protocol

Resilient Ethernet Protocol

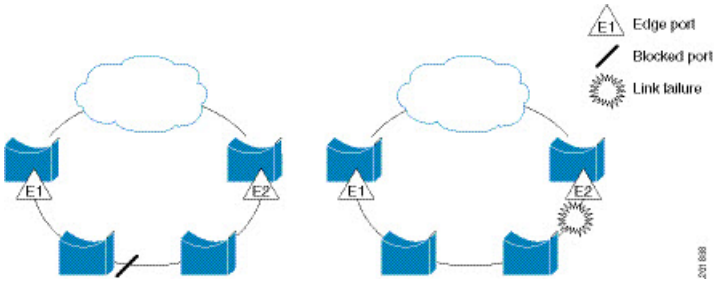
Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time. REP controls a group of ports that are connected in a segment, ensures that the segment does not 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.

Note REP is supported in Cisco IOS XE Cupertino 17.9.x and later releases for Cisco Catalyst IE9300 Rugged Series Switches with the Network Essentials license.

REP segment is a chain of ports that are connected to each other and 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, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link, only two ports can belong to the same segment. REP is supported only on Trunk ports.

The following figure shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), a single port is blocked, shown by the diagonal line. This blocked port is also known as the Alternate port (ALT port). When there is a failure in the network, the blocked port returns to the forwarding state to minimize network disruption.

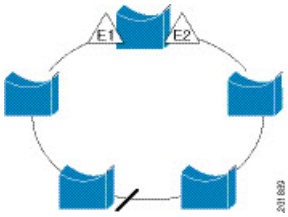
Figure 6: REP Open Segment



The segment shown in the preceding figure is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop, and you can safely connect the segment edges to any network. All hosts connected to switches inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a failure occurs on any segment or on any port on a REP segment, REP unblocks the ALT port to ensure that connectivity is available through the other gateway.

The segment in the following figure is a closed segment, also known as Ring Segment, with both edge ports located on the same router. With this configuration, you can create a redundant connection between any two routers in the segment.

Figure 7: REP Ring Segment



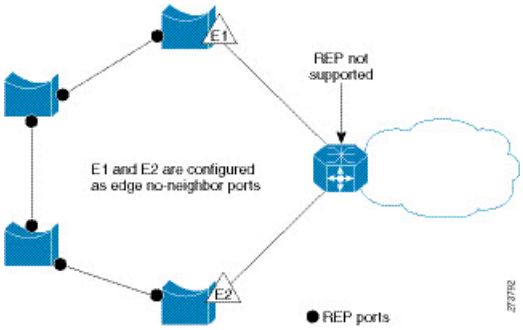
REP segments have the following characteristics:

- If all ports in a segment are operational, one port (referred to as the ALT port) is in the blocked state for each VLAN. If VLAN load balancing is configured, two ALT ports in the segment control the blocked state of VLANs.
- 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.

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

Figure 8: 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.
- You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

Link Integrity

REP does not use an end-to-end polling function between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All the VLANs are blocked on an interface until the neighbor is detected. After the neighbor is identified, REP determines which neighbor port should become the alternate port and which ports should forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to that used by the spanning tree algorithm: a port number (unique on the bridge) associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared as operational after it performs a three-way handshake with a neighbor in the same segment.

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.

Each port creates an adjacency with its immediate neighbor. After the neighbor adjacencies are created, the ports negotiate with each other to determine the blocked port for the segment, which will function as the alternate port. All the other ports become unblocked. By default, REP packets are sent to a bridge protocol data unit-class MAC address. The packets can also be sent to a Cisco multicast address, which is used only to send blocked port advertisement (BPA) messages when there is a failure in the segment. The packets are dropped by the devices not running REP.

Fast Convergence

REP runs on a physical link basis and not on a per-VLAN basis. Only one hello message is required for all the VLANs, and this reduces the load on the protocol. We recommend that you create VLANs consistently on all the switches in a given segment and configure the same allowed VLANs on the REP trunk ports. To avoid the delay introduced by relaying messages in software, REP also allows some packets to be flooded to a regular multicast address. These messages operate at the hardware flood layer (HFL) and are flooded to the entire network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. You can control flooding of these messages by configuring an administrative VLAN for the entire domain or for a particular segment.

VLAN Load Balancing

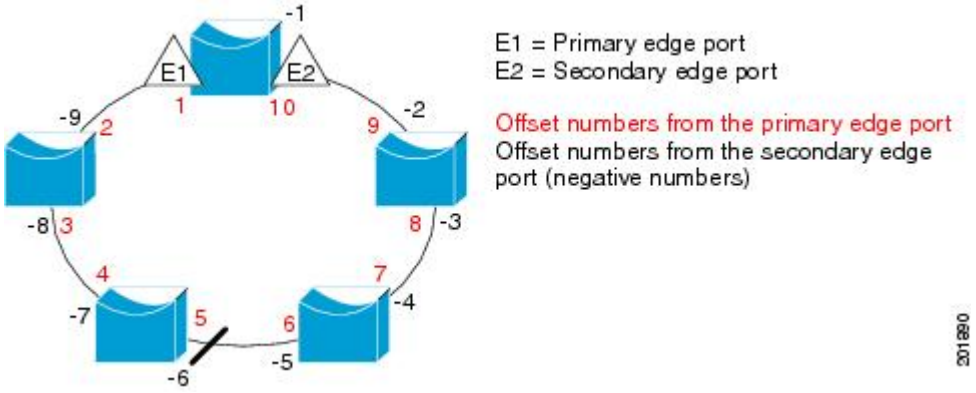
One edge port in the REP segment acts as the primary edge port; and another as the secondary edge port. It is the primary edge port that always participates in VLAN load balancing in the segment. REP VLAN balancing is achieved by blocking some VLANs at a configured alternate port and all the other VLANs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

Note 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.

The following 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. Note that you can identify all the ports (except the primary edge port) by either a positive offset number (downstream position from the primary edge port) or a negative offset number (downstream position 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 9: Neighbor Offset Numbers in a Segment



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 two ways:

- 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.
- 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.

Note 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.

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.

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, begin by configuring a single port in the ring as part of the segment and continue by configuring 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. When the segment has been configured in both directions up to the location of the edge ports, you then configure the edge ports.

Resilient Ethernet Protocol (REP) Negotiated

Note REP Negotiated works only on uplink ports.

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.

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, and when the segment settles, one blocked port remains in the alternate role and all the 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.

A regular segment port converted to an edge port, or an edge port converted 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.

REP was originally designed for Fast Ethernet (FE 10/100) ports. On Fiber GE ports, link down detection time is also 10 ms, but on GE copper interfaces, the link drop detection and recovery times are between 750 ms and 350 ms. As a result, link loss and recovery can be detected a lot more quickly on GE fiber interfaces than on corresponding copper interfaces. This in turn means that the convergence time for REP is a lot higher when using GE copper interfaces.

To improve link down detection time, a beacon mechanism is implemented to trigger faster link failure detection (within 5-10 ms) when a REP interface is configured for 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 successful transmission and reception of the frame, both the timers are reset. If the packet is not received after the transmission, then the second timer is triggered to check the reception within 10 ms. If the packet is not received, upon the timer expiry, a link down message is sent to the switch.

REP Fast works on an individual link basis. It does not impact the REP Protocol. REP Fast requires both ends of the link to support REP Fast to work. REP Fast can be used on any interface link pair that is configured for REP, but it was created to solve an issue on Gigabit copper links. REP Fast speeds up detection of the link failure on Gigabit copper interfaces.

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. REP Fast enablement does not impact REP ring size since it operates only on the pair of interfaces that are 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.

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 Enter global configuration mode:

configure terminal

Step 2 Specify the interface and enter interface configuration mode:

interface *interface-id*

Step 3 Enable REP Fast:

REP fastmode

Step 4 Return to privileged exec mode:

end

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

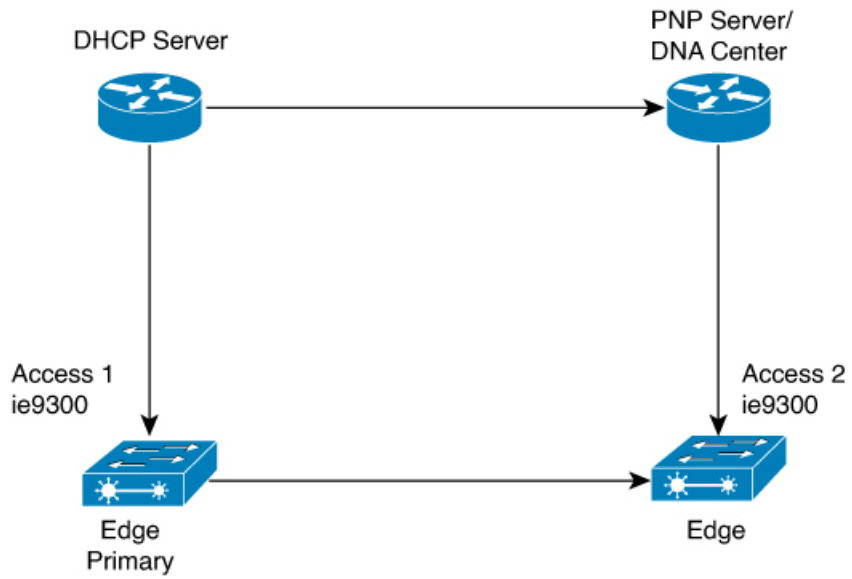
Before a network device such as a router or a switch is deployed online and fully functional, a fair amount of manual configuration is required. Zero Touch Provisioning (ZTP) technologies automate these processes, bringing up network devices into a functional state with minimal to no manual configuration. The Cisco Network Plug and Play (PnP) and Autoinstall Day Zero solutions provide a simple, secure, unified, and integrated offering for enterprise and industrial network customers to ease device rollouts for provisioning updates to an existing network. However, PnP does not support Resilient Ethernet Protocol (REP) due to the way REP is designed. Prior to the REP ZTP feature, REP ring provisioning for Day Zero required manual intervention. The REP ZTP feature introduces a new type-length-value (TLV) extension into the REP LSL packets to support configuring REP rings with zero-touch technologies.

REP and Day Zero

In a typical switch deployment using ZTP, the switch, with no startup configuration in the NVRAM, triggers the Cisco Open Plug-n-Play (PnP) agent to initiate a DHCP discovery process. This process acquires the IP configuration required for the switch from the DHCP server. The DHCP server can be configured to insert additional information in a DHCP message using vendor specific option 43. After the DHCP server receives a DHCP DISCOVER message with option 60 and the string "cisco pnp" from the switch, the DHCP server sends the IP address or hostname of the PnP server to the requesting switch. When the switch receives the DHCP response, the PnP agent extracts the option 43 from the response to get the IP address or the hostname of the PnP server. The PnP agent on the switch then uses this IP address or hostname to communicate with the PnP server. Finally, the PnP server downloads the required Day Zero configuration to the switch to complete the provisioning.

The example shown in the following diagrams illustrates REP ring provisioning on Day Zero, prior to the introduction of REP ZTP.

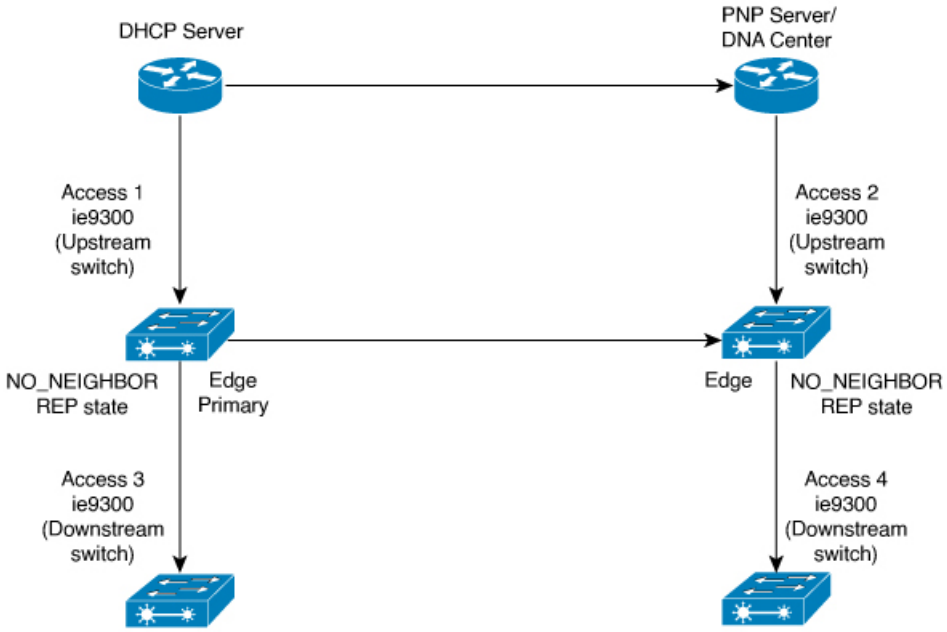
Figure 10: Adding Edge Nodes to the REP Ring



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

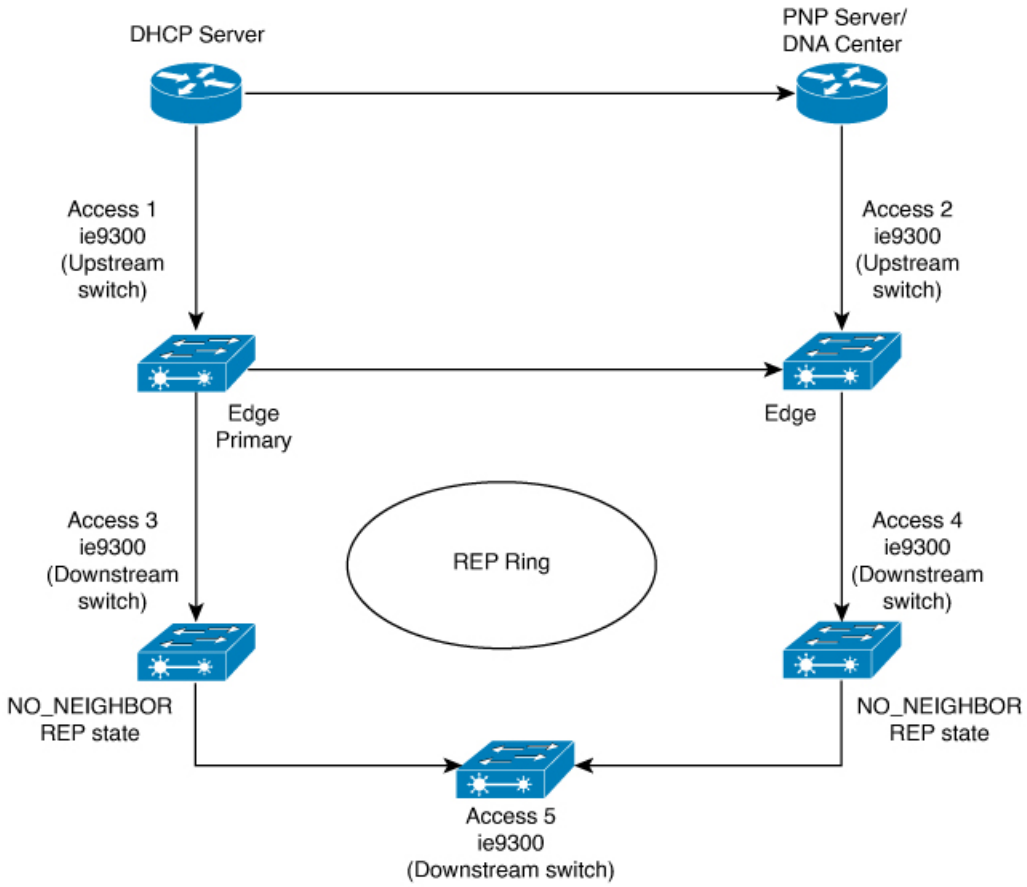
The first set of nodes to be provisioned are Access 1 and Access 2 in the diagram. These are the 2 edge nodes of the REP ring. Note that PnP has configured the downlink port as primary edge on Access 1 and secondary edge on Access 2.

Figure 11: Adding Downstream Nodes



When either Access 3 or Access 4 are powered on, the REP edge primary port starts the REP protocol negotiation and discovers that the neighbor port is not a REP enabled port. (Recall that the switch will be added to the REP ring only after PnP provisioning, for which it needs to first contact the DHCP server as explained earlier.) When an upstream switch port has REP configured and a downstream switch is getting on-boarded with PnP, the REP port goes into the NO_NEIGHBOR state because it is not able to discover its REP peer. In the NO_NEIGHBOR state, REP blocks all the VLANs on that port. This means that the DHCP discovery message from the new switch on the PnP startup VLAN is dropped by the upstream switch because its REP state is NO_NEIGHBOR. The same sequence of blocked ports continues for all new switches added to the REP ring (see Access 5 in figure below).

Figure 12: NO_NEIGHBOR REP State



REP ZTP Overview

The REP ZTP enhancements require that both the upstream and the downstream switches support the feature. When the 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).

Even though the interface on the upstream switch is blocked, it will transmit REP LSL packets to the downstream switch. This is normal. With the enhancement of the REP ZTP feature, the downstream switch will start transmitting REP LSL packets with a new TLV to inform the upstream switch that its neighbor is attempting PNP provisioning.

When the upstream switch reads this REP LSL with the new TLV, it will unblock the interface for the PNP startup VLAN only. All other VLANs for which the upstream interface is a member continue to be blocked. Because the upstream switch is forwarding packets on the PNP startup VLAN for this interface, the downstream switch can complete the PNP process.

The intent of this feature is to allow new switches to join a REP ring with no manual intervention. The interface on the upstream switch keeps the startup VLAN unblocked until the downstream switch has received its configuration and has configured its own interface for REP. If there's a failure in the PNP proccess, the interface on the upstream switch reverts to blocking on the PNP startup VLAN. If the configuration received by the downstream switch does configure the interface for REP, the upstream switch reverts to blocking the PNP startup VLAN.

The downstream behavior to transmit the REP LSL with new TLV to request the PnP startup VLAN be unblocked is the default behavior for switches with no startup configuration. For security purposes, the upstream switch must have the interface to the downstream switch explicitly enabled to put the PnP startup VLAN into unblocked state. The interface level command is **rep ztp-enable**. See Configuring REP ZTP , on page 71.

Note The upstream switch can be part of multiple REP rings and thereby connected to multiple downstream neighbours. The PnP startup VLAN is unblocked only on the interfaces to which the downstream switch is connected.

Configuring Resilient Ethernet Protocol

A segment is a collection of ports that are connected to one another in a chain and configured with a segment ID. To configure REP segments, configure the REP administrative VLAN (or use the default VLAN 1) and then add the ports to the segment, using interface configuration mode. You should configure two edge ports in a segment, with one of them being the primary edge port and the other the secondary edge port by default. A segment should have only one primary edge port. If you configure two ports in a segment as primary edge ports, for example, ports on different switches, the REP selects one of them to serve as the segment's primary edge port. If necessary, you can configure the location to which segment topology change notices (STCNs) and VLAN load balancing are to be sent.

Default REP Configuration

- REP is disabled on all the interfaces. When enabled, the interface is a regular segment port unless it is configured as an edge port.
- When REP is enabled, the task of sending segment topology change notices (STCNs) is disabled, all the VLANs are blocked, and the administrative VLAN is VLAN 1.
- When VLAN load balancing is enabled, the default is manual preemption with the delay timer disabled. If VLAN load balancing is not configured, the default after manual preemption is to block all the VLANs in the primary edge port.
- REP Fast is disabled by default.
- REP Zero Touch Provisioning is enabled by default at the global level and disabled at the interface level.

REP Configuration Guidelines and Limitations

Follow these guidelines when configuring REP:

- We recommend that you begin by configuring one port and then configure contiguous ports to minimize the number of segments and the number of blocked ports.
- If more than two ports in a segment fail when no external neighbors are configured, one port goes into a forwarding state for the data path to help maintain connectivity during configuration.

  In the **show interfaces rep** command output, the Port Role for this port shows as “Fail Logical Open”; the Port Role for the other failed port shows as “Fail No Ext Neighbor”. When the external neighbors for the failed ports are configured, the ports go through the alternate port state transitions and eventually go to an open state or remain as the alternate port, based on 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.
- Be careful when configuring REP through a SSH or Telnet connection. Because REP blocks all VLANs until another REP interface sends a message to unblock it. You might lose connectivity to the router if you enable REP in a SSH or Telnet session that accesses the router through the same interface.
- You cannot run REP and STP on the same segment or interface.
- If you connect an STP network to a REP segment, be sure that the connection is at the segment edge. An STP connection that is not at the edge could cause a bridging loop because STP does not run on REP segments. All STP BPDUs are dropped at REP interfaces.
- If REP is enabled on two ports on a switch, both ports must be either regular segment ports or edge ports. REP ports follow these rules:
  - Only two ports on a switch can belong to 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 be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch 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 one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.
- REP interfaces come up in a blocked state and remain in a blocked state until they are safe to be unblocked. You must be aware of this status to avoid sudden 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 how long a REP interface remains up without receiving a hello from a neighbor. You can use the **rep lsl-age-timer** value interface configuration command to set the time from 120 ms to 10000 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 try to configure a value less than 1000 ms on a port channel, you receive an error message and the command is rejected.
- **lsl-age-timer** is intended to be used when normal link down detection will be too slow for convergence time.

  FastEthernet and fiber connections do not need **lsl-age-timer**. Gigabit copper can use REP Fast instead of **lsl-age-timer**.

- REP ports cannot be configured as one of the following port types:
  - Switched Port Analyzer (SPAN) destination port
  - Tunnel port
  - Access port
- REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.
- Switch supports maximum of 4 REP segments and 3 REP Fast segments.
- There is no limit to the size of a REP ring. REP ring sizes greater than 20 nodes may not achieve desired convergence.

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 mixed into a REP segment where not all interfaces have REP Fast.
- Be aware of the following limitations:
  - A maximum of three REP segments can have REP Fast enabled..
  - MAC Sec is not supported.
  - Overstacking is not supported.
  - REP Fast over EtherChannel is not supported.

REP ZTP Configuration Guidelines

- REP ZTP requires the PnP feature to be present on Cisco Catalyst IE9300 Rugged series switches.
- REP behavior during the NO_NEIGHBOR state is modified beginning in in Cisco IOS XE 17.14.1 and later. This transient state change in port forwarding behavior in NO_NEIGHBOR state allows a DHCP request message to reach a DHCP server and unblock PnP provisioning of a new switch. There should not be any impact to the REP state machine after PnP completion.
- The changes in REP behavior during the NO_NEIGHBOR state apply only to REP Zero Touch Provisioning (ZTP) in Cisco IOS XE 17.14.1 and later. If the PnP feature is not present, normal REP functionality should work as expected.
- The REP ZTP feature coexists with REP bpduleak/negotiated feature on fiber uplink ports.

- The REP ZTP feature is not supported on EtherChannel interfaces for day 0 on an upstream switch because EtherChannel is not present on the downstream interface by default. REP ZTP works only on physical interfaces.
- REP ZTP is supported on both copper (downlink) and fiber (uplink) interfaces.
- REP ZTP is interoperable only with other IE switching products running IOS XE that claim REP ZTP support.

Configure REP Administrative VLAN

To avoid the delay created by link-failure messages, and VLAN-blocking notifications during load balancing, REP floods packets to a regular multicast address at the hardware flood layer (HFL). These messages are flooded to the whole network, and not just the REP segment. You can control the flooding of these messages by configuring an administrative VLAN.

Follow 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, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **rep admin vlan** *vlan-id*
4. **end**
5. **show interface** [*interface-id*] **rep detail**
6. **copy running-config startup config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**rep admin vlan** *vlan-id* **Example:** `Device(config)# rep admin vlan 2`	Specifies the administrative VLAN. The range is from 2 to 4094. To set the admin VLAN to 1, which is the default, enter the **no rep admin vlan** global configuration command.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show interface** [*interface-id*] **rep detail** **Example:** `Device# show interface gigabitethernet1/0/1 rep detail`	(Optional) Verifies the configuration on a REP interface.
Step 6	**copy running-config startup config** **Example:** `Device# copy running-config startup config`	(Optional) Saves 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. This task is mandatory, and must be done before other REP configurations. You must also configure a primary and secondary edge port on each segment. All the other steps are optional.

Follow these steps to enable and configure REP on an interface:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode trunk**
5. **rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]
6. **rep stcn** {**interface** *interface id* | **segment** *id-list* | **stp**}
7. **rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
8. **rep preempt delay** *seconds*
9. **rep lsl-age-timer** *value*
10. **end**
11. **show interface** [*interface-id*] **rep** [**detail**]
12. **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Device(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 4	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Configures the interface as a Layer 2 trunk port.
Step 5	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**] **Example:** `Device(config-if)# rep segment 1 edge no-neighbor primary`	Enables REP on the interface and identifies a segment number. The segment ID range is from 1 to 1024. **Note** You must configure two edge ports, including one primary edge port, for 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. • (Optional) **primary**: Configures the port as the primary edge port, the port on which you can configure VLAN load balancing. • (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.

	Command or Action	Purpose
		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. **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 6	**rep stcn** {**interface** *interface id* | **segment** *id-list* | **stp**} **Example:** `Device(config-if)# rep stcn segment 25-50`	(Optional) Configures the edge port to send segment topology change notices (STCNs). • **interface** *interface-id*: Designates a physical interface or port channel to receive STCNs. • **segment** *id-list*: Identifies one or more segments to receive STCNs. The range is from 1 to 1024. • **stp**: Sends STCNs to STP networks. **Note** 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 7	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**} **Example:** `Device(config-if)# rep block port id 0009001818D68700 vlan 1-100`	(Optional) Configures VLAN load balancing on the primary edge port, 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. • **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**

	Command or Action	Purpose
		to identify the secondary edge port as the alternate port. **Note** Because 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 8	**rep preempt delay** *seconds* **Example:** `Device(config-if)# rep preempt delay 100`	(Optional) Configures a pre-empt time delay. • 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 9	**rep lsl-age-timer** *value* **Example:** `Device(config-if)# rep lsl-age-timer 2000`	(Optional) 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 10	**end** **Example:** `Device(config-if)# end`	Exits global configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 11	**show interface** [*interface-id*] **rep** [**detail**] **Example:** `Device# show interface gigabitethernet1/0/1 rep detail`	(Optional) Displays the REP interface configuration.
Step 12	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the router startup configuration file.

Setting Manual Preemption for VLAN Load Balancing

If you do not enter the **rep preempt delay** *seconds* interface configuration command on the primary edge port to configure a preemption time delay, the default is to manually trigger VLAN load balancing on the segment. Be sure that all the other segment configurations have been completed before manually preempting VLAN load balancing. When you enter the **rep preempt delay segment** *segment-id* command, a confirmation message is displayed before the command is executed because preemption might cause network disruption.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**rep preempt segment** *segment-id*
	Example:
	`Device# rep preempt segment 100`
	`The command will cause a momentary traffic disruption.`
	`Do you still want to continue? [confirm]`
		Manually triggers VLAN load balancing on the segment.
		You need to confirm the command before it is executed.

Step 3	**show rep topology segment** *segment-id* **Example:** `Device# show rep topology segment 100`	(Optional) Displays REP topology information.
Step 4	**end** **Example:** `Device# end`	Exits privileged EXEC mode.

Configuring SNMP Traps for REP

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp mib rep trap-rate** *value* **Example:** `Device(config)# snmp mib rep trap-rate 500`	Enables the switch to send REP traps, and sets the number of traps sent per second. • Enter the number of traps sent per second. The range is from 0 to 1000. The default is 0 (no limit is imposed; a trap is sent at every occurrence).
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Device# show running-config`	(Optional) Displays the running configuration, which can be used to verify the REP trap configuration.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the switch startup configuration file.

Configuring 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 PNP server user must explicitly add this CLI configuration in the configuration template for the feature to be enabled.

Procedure

Step 1 Enter global configuration mode:

```
Switch# configure terminal
```

Step 2 Globally enable REP ZTP:

```
Switch(config)# rep ztp
```

Use the no form of the command to disable REP ZTP: `Switch(config)# no rep ztp`

Step 3 Enter interface configuration mode on the upstream device interface that is connected to the downstream device:

```
Switch(config)# interface <interface-name>
```

Step 4 Enable REP ZTP on the interface:

```
Switch(config-if)#rep ztp-enable
```

Use the no form of the command to disable REP ZTP on the interface: `Switch(config-if)#no rep ztp-enable`

Example

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
```

Monitoring Resilient Ethernet Protocol Configurations

This is an example of the output for the **show interface** [*interface-id*] **rep** [**detail**] command. This display shows the REP configuration and status on an 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
```

This is an example of the output for the **show interface** [*interface-id*] **rep** [**detail**] command. This display shows 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 is an example for the **show rep topology** [**segment** *segment-id*] [**archive**] [**detail**] command. This display shows the REP topology information for all the 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
```

Displaying REP ZTP Status

Use the **show** command to identify the state of REP ZTP on an interface. In the following example, the feature is disabled on interface GigabitEthernet 1/0/1 and it is enabled on interface GigabitEthernet 1/0/2. The status of **pnp_startup_vlan** is "Blocked".

Procedure

Step 1 In priviledged exec mode, enter:

show interfaces rep detail

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 command again to display the status of **pnp_startup_vlan**.

When the downstream device is booted up, it sends notification to the connected upstream switch interface to unblock the **pnp_startup_vlan** for it to get the DHCP IP address and further establish communication with the PNP server or DNAC. The show command indicates the status as "Unblocked".

The following 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 the following debug commands to troubleshoot REP ZTP:

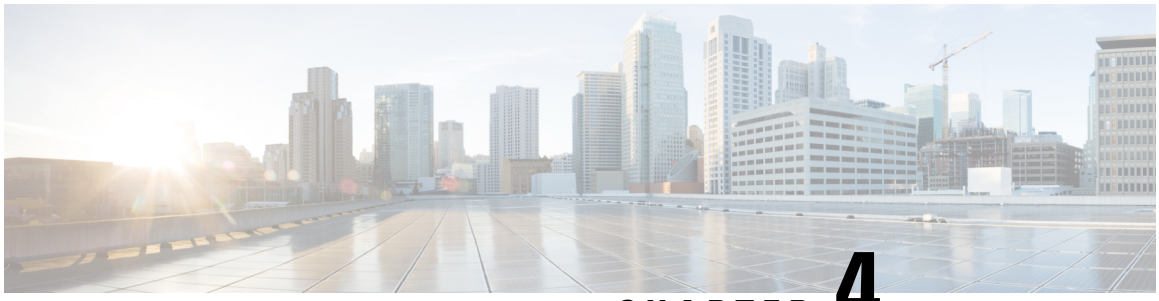
- **debug rep lslsm**: This command helps you understand LSL state machine events in the NO_NEIGHBOR state.
- **debug rep packet**: Use this command to dump LSL packets with the REP ZTP LSL TLV to check the PnP status on the peer client node.

What to do next

Feature History for Resilient Ethernet Protocol

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 Cupertino 17.9.x	Resilient Ethernet Protocol Fast	This feature became available for Cisco Catalyst IE9300 Rugged Series Switches in this release.
Cisco IOS XE Cupertino 17.14.x	Resilient Ethernet Protocol Zero Touch Provisioning	This feature became available for Cisco Catalyst IE9300 Rugged Series Switches in this release.



CHAPTER 4

Media Redundancy Protocol

Media Redundancy Protocol

Media Redundancy Protocol (MRP), defined in International Electrotechnical Commission (IEC) standard 62439-2, provides fast convergence in a ring network topology for Industrial Automation networks. MRP Media Redundancy Manager (MRM) defines its maximum recovery times for a ring in the following range: 10 ms, 30 ms, 200 ms and 500 ms.

Note The default maximum recovery time on the Cisco IE switch is 200 ms for a ring composed of up to 50 nodes. You can configure the switch to use the 500 ms recovery time profile as described in Configure MRP Manager, on page 85. The 10 ms and 30 ms recovery time profiles are not supported.

MRP is supported on all Cisco Catalyst IE9300 Rugged Series Switches:

- 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

MRP operates at the MAC layer and is commonly used in conjunction with the PROFINET standard for industrial networking in manufacturing.

MRP Mode

MRP is supported on Cisco Catalyst IE9300 Rugged Series Switches, MRP Command-line interface (CLI) mode.

MRP CLI mode is managed by the Cisco IOS XE CLI and WebUI, a web-based user interface (UI).

Note When managing the switch in MRP CLI mode, you cannot download the MRP configuration from Siemens STEP7/TIA.

Protocol Operation

In an MRP ring, the MRM serves as the ring manager, while the Media Redundancy Clients (MRCs) act as member nodes of the ring. Each node (MRM or MRC) has a pair of ports to participate in the ring. The MRM initiates and controls the ring topology to react to network faults by sending control frames on one ring port over the ring and receiving them from the ring over its other ring port, and conversely in the other direction. An MRC reacts to received reconfiguration frames from the MRM and can detect and signal link changes on its ring ports.

On Cisco Catalyst IE9300 Rugged Series Switches, certain nodes or all nodes in the ring can also be configured to start as a Media Redundancy Automanager (MRA). MRAs select one MRM among each other by using a voting protocol and a configured priority value. The remaining MRAs transition to the MRC role.

All MRM and MRC ring ports support the following states:

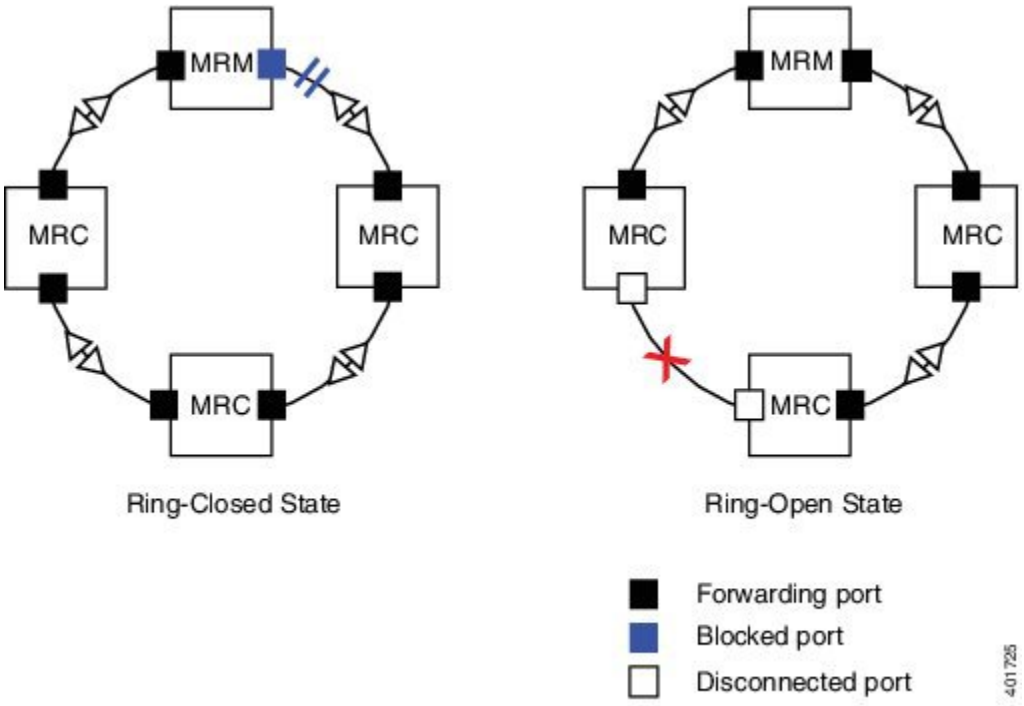
- Disabled: Ring ports drop all received frames.
- Blocked: Ring ports drop all received frames except MRP control frames and some standard frames, for example, LLDP.
- Forwarding: Ring ports forward all received frames.
- Not Connected: The link is physically down or disconnected. (This state differs from the Disabled state, in which the MRP Port is manually disabled through software.)

During normal operation, the network operates in the Ring-Closed state (see figure below). To prevent a loop, one of the MRM ring ports is blocked, while the other port is forwarding. Most of the time, both ring ports of all MRCs are in the forwarding state. With this loop avoidance, the physical ring topology becomes a logical stub topology.

In the figure, note the following details about the two rings, left and right:

- Left Ring: The connection (small blue square, top) on the MRM is in a blocked state (as shown by the two parallel lines) because no ports are disconnected.
- Right Ring: Two MRC connections (left and center small white squares) are in the disabled state because the link between them is broken, as marked by a red "x".

Figure 13: MRP Ring States



If a network failure occurs:

- The network shifts into the Ring-Open state.
- In the case of failure of a link connecting two MRCs, both ring ports of the MRM change to the forwarding state, the MRCs adjacent to the failure have a disabled and a forwarding ring port, and the other MRCs have both ring ports forwarding.

In the Ring-Open state, the network logical topology becomes a stub.

Layer 2 Ethernet frames will be lost during the time required for the transition between these two ring states. The MRP protocol defines the procedures to automatically manage the switchover to minimize the switchover time. A recovery time profile, composed of various parameters, drives the MRP topology convergence performance. The 200 ms profile supports a maximum recovery time of 200 ms.

MRP uses three types of control frames:

- To monitor the ring status, MRM regularly sends test frames on both ring ports.
- When MRM detects failure or recovery, it sends TopoChange frames on both ring ports.

- When MRC detects failure or recovery on a local port, it sends LinkChange subtype frames, Linkdown and Linkup, to the MRM.

Media Redundancy Automanager

If configured to start as a Media Redundancy Automanager (MRA), the node or nodes select an MRM using a voting protocol and configured priority value. The remaining MRAs transition to the MRC role. All nodes must be configured as MRA. A manually configured MRM and MRA in the same ring is not supported.

Note

- You can activate MRA through the CLI. See the section Configuring MRP CLI Mode, on page 85 in this guide.
- Although MRAs transition to the MRC role after an MRM is selected, you cannot explicitly configure an MRC.

The MRA role is not an operational MRP role like MRM or MRC. It is only an administrative, temporary role at device startup, and a node must transition to the MRM role or the MRC role after startup and the MRM is selected though the manager voting process.

MRA functions as follows:

1. At power on, all MRAs begin the manager voting process. Each MRA begins to send MRP_Test frames on both ring ports. The MRP_Test frame contains the MRA's priority value. The remote manager's priority value contained in the received MRP_Test frames are compared with the MRA's own priority. If its own priority is higher than the received priority, the MRA sends a negative test manager acknowledgment (MRP_TestMgrNAck) frame, along with the remote manager's MAC address.
2. If the receiving MRA receives an MRP_TestMgrNAck with its own MAC address, the receiving MRA initiates the transition into the client (MRC) role.
3. The MRP_TestPropagate frame informs other MRA devices in the client role about the role change and the new higher priority manager. The clients receiving this frame update their higher priority manager information accordingly. This ensures that clients remain in the client role if the monitored higher priority manager role changes.

Licensing

You do not need a feature license to use MRP with Cisco Catalyst IE9300 Rugged Series Switchesl MRP works with either base license—Network Essentials or Network Advantage.

To find information about platform support and to know which license levels a feature is available with, use Cisco Feature Navigator. To access Cisco Feature Navigator, go to https://www.cisco.com/go/cfn. An account on cisco.com is not required.

Multiple MRP Rings

In an Industrial Ethernet network, an MRP ring in a cell/area is a sub-ring of the access layer. You can connect multiple MRP rings, which you can then aggregate into the distribution layer.

You can configure up to 12 rings for Cisco Catalyst IE9300 Rugged Series Switches. The switch can be either an automanager or a client.

MRP-STP Interoperability

MRP works with Spanning Tree Protocol (STP) to prevent unwanted broadcast loops in the event that a user accidentally connects a device that does not participate in the MRP ring. In a network operating with MRP and STP, spanning tree bridge protocol data units (BPDUs) are not sent on MRP-enabled ports. If ports are unconfigured from an MRP ring, then the ports are added to the spanning tree.

MRP-STP interoperability is supported in MRP CLI mode, and functions without additional CLI configuration.

Prerequisites

- Because MRP is deployed in a physical Ring topology, before configuring or unconfiguring the MRP feature, it is advised to leave one physical connection between two nodes in each ring open by either issuing a **shut** command on the connecting interfaces or physically removing the cable to avoid any network storms. After you have properly configured all MRMs, issue a **no shut** command on the port or re-connect the cable between the nodes.

Guidelines and Limitations

General Guidelines and Limitations

- MRP is supported on Cisco Catalyst IE9300 Rugged Series Switches beginning with the IOS XE 17.13.1 release.
- MRP is not supported in a stacked environment of IE-9300 switches.
- To avoid Smart License registration failure, ensure that the NTP configuration and the device clock are in sync.
- Support for multiple MRP rings is available only through the CLI or WebUI.
- The switch supports up to 50 MRCs per ring.
- MRP cannot run on the same interface (port) as Resilient Ethernet Protocol (REP), Spanning Tree Protocol (STP), Flex Links, macsec, or Dot1x.
- For access ports, you must specifically configure **switchport mode access** and **switchport access vlan** *x* commands in the MRP interface.

- MRP interfaces come up in a forwarding state and remain in a forwarding state until notified that it is safe to block. The MRP ring state changes to Ring-Closed.
- MRP ports cannot be configured as any of these port types: SPAN destination port, Private VLAN port, or Tunnel port.
- MRP is not supported on EtherChannels or on an individual port that belongs to an EtherChannel.
- Each MRP ring can have one MRP VLAN. The VLAN must be different for each ring in a device to avoid traffic flooding.

MRP CLI Mode Guidelines and Limitations

- After using the CLI to configure the MRP ring, you must attach the MRP ring to a pair of ports that support MRP.
- Both MRP ports must have the same interface mode (access or trunk).
- To change an existing MRP ring's configuration (mode), or to change the interface mode of the ring ports between access and trunk, you must first delete the ring and then recreate it with the new configuration.
- When both MRP ports are in access mode, the access VLANs should match. If the configured MRP VLAN does not match the ports' access VLAN, the MRP VLAN is automatically changed to the MRP ports' access VLAN.
- In an MRP ring with two access ports, if the ports do not belong to the same access VLAN when you create the MRP ring or you change the access VLAN for only one of the ports after the MRP ring is created, the MRP ring operation is suspended and a message similar to the following 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
  ```

  Resolve the issue by configuring the access VLAN to be the same for the two ring ports.
- The 200 ms standard profile and 500 ms profile are supported. The 10 ms profile and 30 ms profile are not supported.
- You can activate MRA through the CLI.
- Although MRAs transition to the MRC role after an MRM is selected, you cannot explicitly configure an MRC.

Default Settings

- MRP is disabled by default; MRP CLI is the default mode when MRP is enabled.
- The default VLAN is 1.

Note Create the non-default VLAN before you assign it to MRP ring 1.

Configuring MRP CLI Mode

To configure MRP, configure the node as MRA and specify the two MRP ports. You can configure up to 12 rings on the device (the device can be manager or client) with a manager instance for each ring and one manager per device.

The following MRP configuration parameters are optional:

- domain-id: A unique ID that represents the MRP ring.
- domain-name: Logical name of the configured MRP domain-ID.
- profile: 200 ms (the default)
- vlan-id: VLAN for sending MRP frames.

Configure MRP Manager

Follow this procedure to configure the switch as MRA in MRP CLI mode, which is the default.

Note If the device is connected to a PLC module, please make sure “no device in the ring” is selected for MRP.

SUMMARY STEPS

1. Enable MRP:
2. Configure MRP manager mode on the switch:
3. (Optional for single MRP ring) Configure the domain ID:
4. (Optional for single MRP ring) Configure the domain name:
5. (Optional) Configure the VLAN ID:
6. (Optional) Configure the recovery profile:
7. Configure the MRA priority:
8. Configure the interval:
9. Specify the ID of the port that serves as the first ring port:
10. Configure the interface mode:
11. Associate the interface to the MRP ring:
12. Return to global configuration mode:
13. Specify the ID of the port that serves as second ring port:
14. Configure the interface mode:
15. Associate the interface to the MRP ring:
16. Return to privileged EXEC mode:
17. (For multiple rings) Repeat step 1 through 14 for each additional ring:

DETAILED STEPS

Procedure

Step 1 Enable MRP:

mrp ring *mrp_id*

MRP supports up to 12 rings.

Step 2 Configure MRP manager mode on the switch:

mode auto-manager

Step 3 (Optional for single MRP ring) Configure the domain ID:

domain-id *value*

value: UUID string of 32 hexadecimal digits in five groups separated by hyphens

Example: 550e8400-e29b-41d4-a716-446655440000

The default domain ID for ring 1 is FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFE.

Note Only change the domain-ID from the default when required.

Step 4 (Optional for single MRP ring) Configure the domain name:

domain-name *name*

name: String of up to 32 characters

Step 5 (Optional) Configure the VLAN ID:

vlan-id *vlan*

Step 6 (Optional) Configure the recovery profile:

profile { |**200** | **500**}

- 200: Maximum recovery time 200 milliseconds
- 500; Maximum recovery time 500 milliseconds

Step 7 Configure the MRA priority:

priority *value*

value: Range <36864 – 61440>, lowest: 65535.

The default priority is 40960.

Step 8 Configure the interval:

interval *interval*

Note The Interval field is not displayed in WebUI for MRP.

- 3: 3 milliseconds MRP_Test default interval for 30 ms profile

- 20: 20 milliseconds MRP_Test default interval for 200 ms profile
- 50: 50 milliseconds MRP_Test default interval for 500 ms profile
- <3-10>: Optional faster MRP_Test interval in milliseconds

Note The optional faster MRP_Test interval can be configured only when the ring is formed with IE3x00 devices.

Step 9 Specify the ID of the port that serves as the first ring port:

interface *port*

Step 10 Configure the interface mode:

switchport mode { **access** | **trunk** }

Note You must specify **switchport mode access** when configuring MRP in access mode.

Step 11 Associate the interface to the MRP ring:

mrp ring 1

Step 12 Return to global configuration mode:

exit

Step 13 Specify the ID of the port that serves as second ring port:

interface *port*

Step 14 Configure the interface mode:

switchport mode { **access** | **trunk** }

Note You must specify **switchport mode access** at this step when configuring MRP in access mode.

Step 15 Associate the interface to the MRP ring:

mrp ring 1

Step 16 Return to privileged EXEC mode:

end

Step 17 (For multiple rings) Repeat step 1 through 14 for each additional ring:

- Assign ring number 2 for the second ring.
- Assign a unique domain ID for Ring 2. The default domain ID for ring 2 is FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFD.
- Assign ring number 3 for the third ring.
- Assign a unique domain ID for Ring 3. The default domain ID for ring 3 is FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFC.

Note Each ring should have its own domain ID. No two rings share the same domain ID.

Example

The following example shows configuring MRP automanager:

```
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 manager
Switch(config-mrp-manager)#domain-id FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
Switch(config-mrp-manager)#priority 40960
Switch(config-mrp-manager)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#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)#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
Switch(config-if)#end

Switch# show mrp ring 1
MRP ring 1

Profile : 200 ms
Mode : Auto-Manager
Priority : 40960
Operational Mode: Client
From : CLI
License : Active
Best Manager :
MAC Address : 00:78:88:5E:03:81
Priority : 36864

Network Topology: Ring
Network Status : OPEN
Port1: Port2:
MAC Address :84:B8:02:ED:E8:02 MAC Address :84:B8:02:ED:E8:01
Interface :GigabitEthernet1/0/22 Interface :GigabitEthernet1/0/21
Status :Forwarding Status :Forwarding

VLAN ID : 1
Domain Name : Cisco MRP Ring 1
Domain ID : FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF

Topology Change Request Interval : 10ms
Topology Change Repeat Count : 3
Short Test Frame Interval : 10ms
Default Test Frame Interval : 20ms
Test Monitoring Interval Count : 3
Test Monitoring Extended Interval Count : N/A
Switch#show mrp ports

Ring ID : 1
```

```
PortName                Status
--------------------------------------
GigabitEthernet1/0/22         Forwarding
GigabitEthernet1/0/21         Forwarding
```

Note The **show mrp ring** output shows "License: Not Applicable" in CLI and Profinet mode in Cisco IOS XE release 17.7.1 and later.

Configuration Example

The following example shows the MRP switch configured as manager:

```
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 manager
Switch(config-mrp-manager)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gi1/0/21-28
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 gi1/0/27
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)#end

Switch#show mrp ring
MRP ring 1

Profile     : 200 ms
Mode        : Master
From        : CLI

Network Topology: Ring
Port1:                                    Port2:
MAC Address    :2C:54:2D:2C:3E:0A         MAC Address    :2C:54:2D:2C:3E:09
Interface      :gigabitEthernet1/0/28           Interface      :gigabitEthernet1/0/27
Status         :Forwarding                Status         :Forwarding

VLAN ID     : 1
Domain Name : Cisco MRP
Domain ID   : FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF

Topology Change Request Interval        : 10ms
Topology Change Repeat Count            : 3
Short Test Frame Interval               : 10ms
Default Test Frame Interval             : 20ms
Test Monitoring Interval Count          : 3
Test Monitoring Extended Interval Count : N/A
```

```
Switch#show mrp ports

Ring ID : 1
PortName                Status
-------------------------------------
gigabitEthernet1/0/27         Forwarding
gigabitEthernet1/0/28         Forwarding
```

The following example shows the MRP switch configured as automanager:

```
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)#priority 36864
Switch(config-mrp-auto-manager)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gi1/0/22
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 gi1/0/21
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)#end

Switch#show mrp ring
MRP ring 1

Profile     : 200 ms
Mode        : Auto-Manager
Priority    : 36864
Operational Mode: Manager
From        : CLI
License     : Active
Best Manager MAC Address    :84:B8:02:ED:E8:01     priority 36864

Network Topology: Ring
Network Status  : OPEN
Port1:                                      Port2:
 MAC Address    :84:B8:02:ED:E8:02          MAC Address    :84:B8:02:ED:E8:01
 Interface      :GigabitEthernet1/0/22      Interface      :GigabitEthernet1/0/21
 Status         :Forwarding                 Status         :Forwarding

VLAN ID     : 1
Domain Name : Cisco MRP Ring 1
Domain ID   : FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF

Topology Change Request Interval        : 10ms
Topology Change Repeat Count            : 3
Short Test Frame Interval               : 10ms
Default Test Frame Interval             : 20ms
Test Monitoring Interval Count          : 3
Test Monitoring Extended Interval Count : N/A
```

```
Topology Change Request Interval        : 10ms
Topology Change Repeat Count            : 3
Short Test Frame Interval               : 10ms
Default Test Frame Interval             : 20ms
Test Monitoring Interval Count          : 3
Test Monitoring Extended Interval Count : N/A
```

The following example shows the configured MRP switch:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mrp ring 1
Switch(config-mrp)#mode client
Switch(config-mrp-client)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gi1/0/23
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
Switch(config-if)#exit
Switch(config)#interface gi1/0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
Switch(config-if)#end
```

Verifying the Configuration

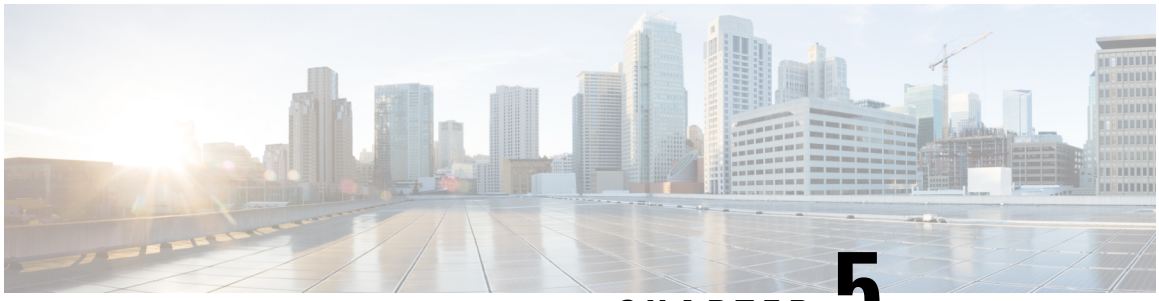
You can use the following commands to verify the MRP configuration.

Command	Description
show mrp ring? {**1 - 22**}	Display details about the MRP ring configuration.
show mrp ports	Display details about the MRP port states. If MRP is not configured on any ports, display shows N/A.
show mrp ring {**1 - 22**} **statistics** [**all** | **event** | **hardware** | **packet** | **platform**]	Display details about the MRP ring operation.
debug mrp-ring [**alarm**|**cli** | **client** | **license** | **manager** | **packet** | **platform**]	Trace MRP events. **Note** **manager** is available only when the switch is configured as manager or automanager. **license** is available only in Cisco IOS XE 17.6.x and earlier.
show tech-supportmrp	Display all MRP details.

Feature History

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 17.13.1	Media Redundancy Protocol (MRP)	MRP provides fast convergence in a ring network topology for Industrial Automation networks. The feature became available for Cisco Catalyst IE9300 Rugged Series Switches in this release.



CHAPTER 5

High-availability Seamless Redundancy

High-availability Seamless Redundancy

High-availability Seamless Redundancy (HSR) is defined in International Standard IEC 62439-3-2016 clause 5. HSR is similar to Parallel Redundancy Protocol (PRP) but is designed to work in a ring topology. Instead of two parallel independent networks of any topology (LAN-A and LAN-B), HSR defines a ring with traffic in opposite directions. Port-A sends traffic counter clockwise in the ring, and Port-B sends traffic clockwise in the ring.

The HSR packet format is also different from PRP. To allow the switch to determine and discard duplicate packets, additional protocol specific information is sent with the data frame. For PRP, this is sent as part of a trailer called the redundancy control trailer (RCT), whereas for HSR this is sent as part of the header called the HSR header. Both the RCT and HSR header contain a sequence number, which is the primary data used to determine if the received frame is the first instance or a duplicate instance.

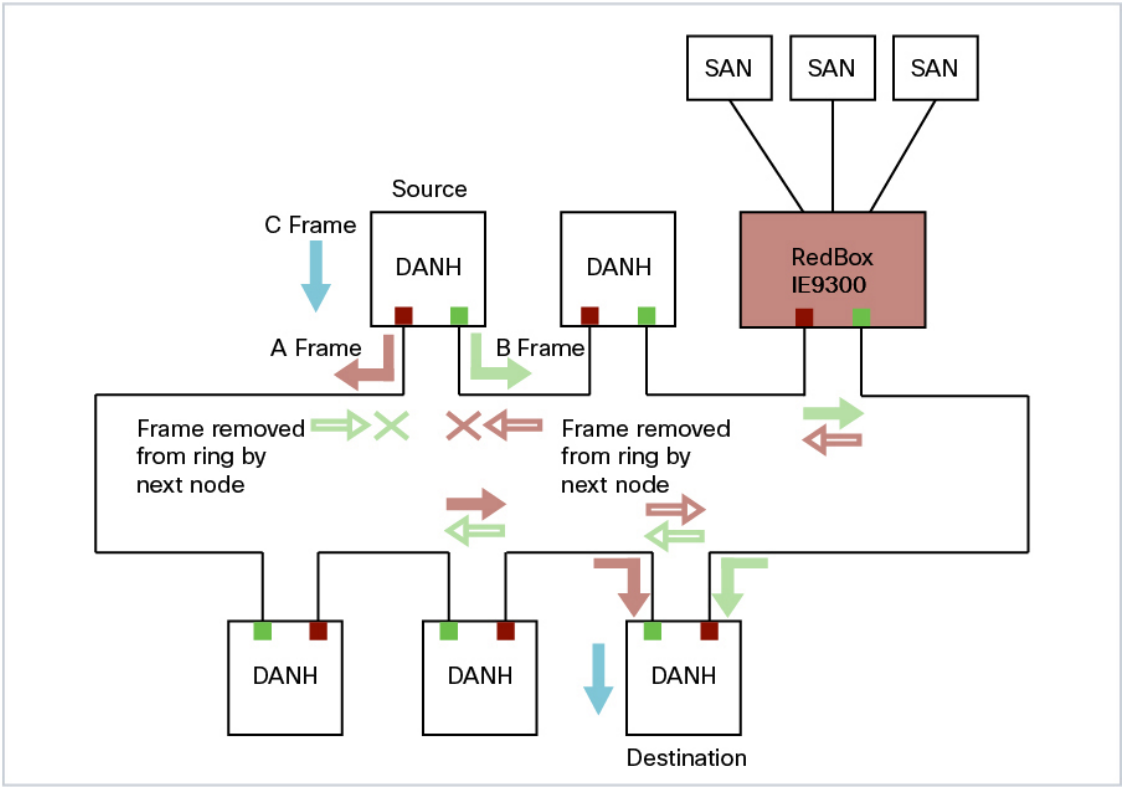
Note HSR is supported on certain SKUs of the Cisco Catalyst IE9300 Rugged Series Switches (see the Guidelines and Limitations section in this guide for supported SKUs). The term *switch* in this document refers to a Cisco Catalyst IE9300 Rugged Series Switch unless otherwise noted.

In this release, the switch supports only HSR-singly attached node (SAN) and only one HSR instance. In addition, you can create only one HSR or one PRP instance. If you have created a PRP instance, no HSR instance can be created.

The non-switching nodes with two interfaces attached to the HSR ring are referred to as Doubly Attached Nodes implementing HSR (DANHs). Similar to PRP, Singly Attached Nodes (SANs) are attached to the HSR ring through a device called a RedBox (Redundancy Box). The RedBox acts as a DANH for all traffic for which it is the source or the destination. The switch implements RedBox functionality using Gigabit Ethernet port connections to the HSR ring.

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 14: Example of HSR Ring Carrying Unicast Traffic



Devices that do not support HSR out of the box (for example, laptops and printers) cannot be attached to the HSR ring directly because all HSR capable devices must be able to process the HSR header on packets received from the ring and add the HSR header to all packets sent into the ring. These nodes are attached to the HSR ring through a RedBox. As shown in the figure above, the RedBox has two ports on the DANH side. Non-HSR SAN devices are attached to the upstream switch ports. The RedBox generates the supervision frames on behalf of these devices so that they are seen as DANH devices on the ring. Because the RedBox emulates these as DANH, they are called Virtual Doubly Attached Nodes (VDAN).

Loop Avoidance

Each node in the HSR ring forwards frames received from one port to the other port of the HSR pair. To avoid loops and use network bandwidth effectively, the RedBox does not transmit frames that are already transmitted in same direction. When a node injects a packet into the ring, the packet is handled as follows to avoid loops:

- 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: Because this packet does not have a destination node in the ring, it is forwarded by every node in the ring until it reaches the originating node. Because every node has a record of the packet it sent, along with the direction in which it was sent, the originating node detects that packet has completed the loop and drops the packet.
- Multicast packet: A multicast packet is forwarded by each node because there can be more than one consumer of this packet. For this reason a multicast packet always reaches the originating node. However, every node will check whether it has already forwarded the received packet through its outgoing interface. Once the packet reaches the originating node, the originating node determines that it already forwarded this packet and drops the packet instead of forwarding it again.

HSR RedBox Modes of Operation

The most basic mode of operation is HSR-SAN mode (single RedBox mode). In this mode, the RedBox is used to connect SAN devices to the HSR ring. The Redbox's responsibility in this mode is to represent SAN devices as VDANs on the ring.

Note In this release, the switch supports HSR-SAN mode only.

HSR SAN Mode

In HSR-SAN mode, the RedBox inserts the HSR tag on behalf of the host and forwards the ring traffic, except for frames sent by the node itself, duplicate frames, and frames for which the node is the unique destination. In this mode, packets are handled as follows:

- A source DANH sends a frame passed from its upper layers (C frame), prefixes it 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. A node will not forward frames received on one port to the other under the following conditions:
  - 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 such as the local and remote interface 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 then use the neighbor information from each node to determine the complete HSR network topology and debug and locate ring faults.

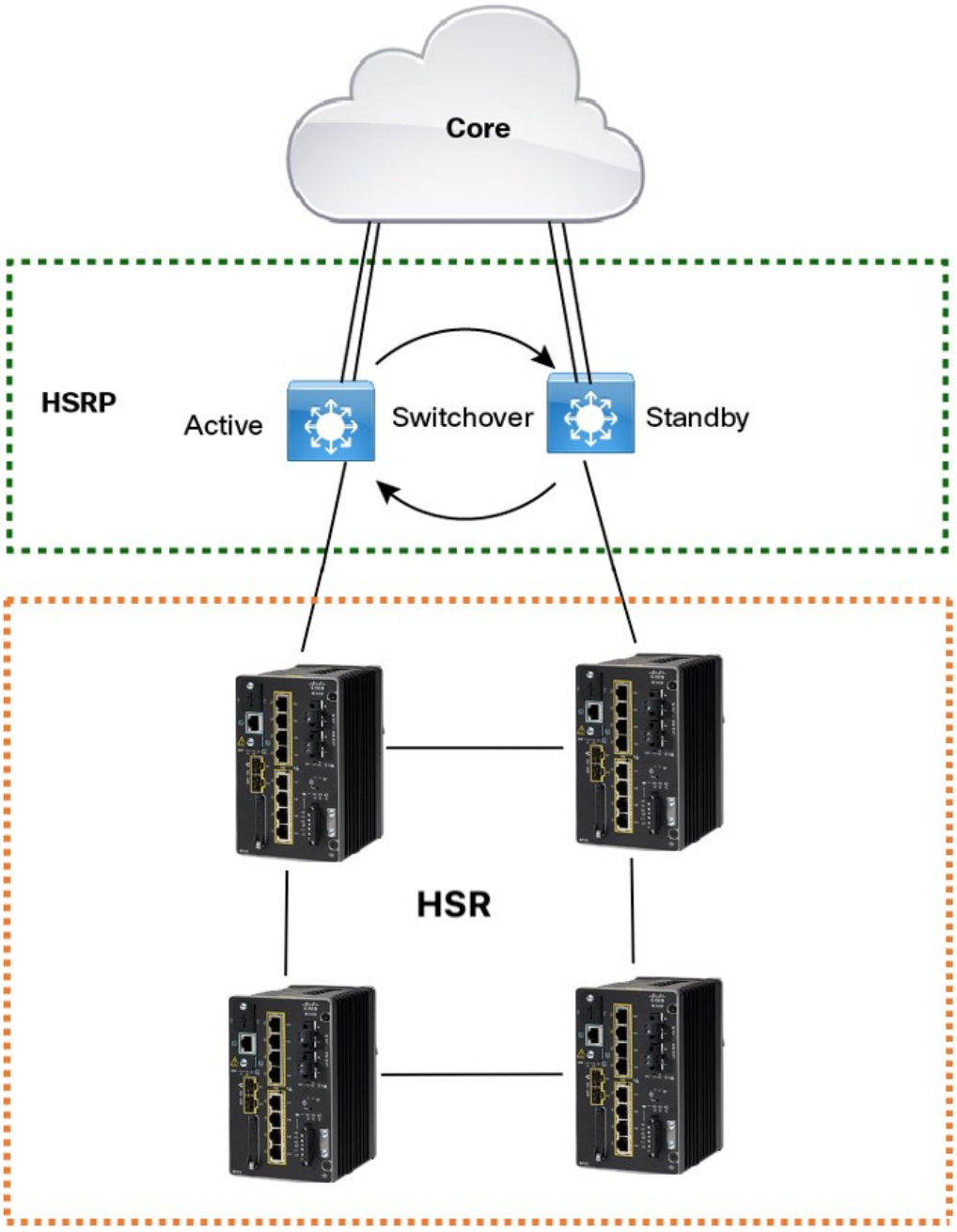
CDP and LLDP are configured on physical interfaces only.

For more information, see Configuring an HSR Ring and Verifying Configuration.

HSR Uplink Redundancy Enhancement

The HSR Uplink Redundancy Enhancement feature allows for flexible designs that enable two separate interfaces to connect upstream from the HSR ring through two separate HSR RedBoxes. This ensures there is no single point of failure exiting the HSR ring. Examples of protocols that can leverage this feature to improve high availability include HSRP, VRRP and REP. Prior to this enhancement, if these protocols were utilized on redundant uplinks, undesirable results could occur, such as next-hop split-brain conditions or slow REP failover times.

The following diagram shows an example network with HSR and HSRP that allows uplink next-hop gateway redundancy out of the HSR ring.



To implement HSR Uplink Redundancy, ensure that the **fpgamode-DualUplinkEnhancement** feature is not disabled. This feature is required to support the connectivity to a dual router (HSRP in this case) on the distribution layer:

```
Switch#show hsr ring 1 detail | include fpgamode
 fpgamode-DualUplinkEnhancement: Enabled
```

If the output shows *fpgamode-DualUplinkEnhancement,:Disabled* issue the following command:

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hsr-ring 1 fpgamode-DualUplinkEnhancement
Switch(config)# end
```

HSRP Configuration

The following example HSRP configuration applies to the two distribution switches Active & Standby in the above figure. In the following 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
```

Guidelines and Limitations

- HSR-SAN is supported only on the following Cisco Catalyst IE9300 Rugged Series Switches:
  - IE-9320-26S2C-E and IE-9320-26S2C-A
  - IE-9320-22S2C4X-E and IE-9320-22S2C4X-A
- HSR-SAN (Single RedBox mode) is the only HSR mode supported in this release.
- HSR is supported only in a standalone deployment; there is no support for HSR for stacked switches.
- Only one HSR instance is supported. Note that the switch supports only one HSR or one PRP instance, so if a PRP instance has been created, no HSR instance can be created.
- HSR ring 1 can only be configured as a pair of ports: Gi1/0/21 and Gi1/0/22 or Gi1/0/23 and Gi1/0/24. Using these port pairs, you can configure 1 HSR ring.
- The HSR feature requires the Network Essentials license.
- The HSR feature is not enabled by default and you must explicitly configure the HSR rings.
- HSR is disabled automatically if the required firmware image is not available on the system.
- Once a port is part of a ring, the media-type, speed, and duplex settings of the port cannot be changed. We recommend that you apply those settings before configuring ring membership.
- If mode of HSR interfaces is changed from access to trunk mode or vice-versa after configuring the ring,we recommended that you flap the HSR ring.
- The recommended maximum number of nodes in the node table is 512. Nodes are all the DANH and VDAN devices that can be connected to the ring at same time. This number is not an absolute limit, but higher numbers of entries may increase the number of duplicate packets received by the 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.
- Both ports of one ring must be of same speed and type (that is, both can be SFPs or both can be copper)
- 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)
  - Resilient Ethernet Protocol (REP)

- MACsec, HSR, and PRP are not allowed together.
- PTP over HSR is not supported.
- HSR supports an MTU size of up to 1998 bytes of Ethernet payload.
- 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. That is, 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.
- It is important for all interfaces in an HSR ring to have the same speed and duplex settings. It is recommended to apply those settings before configuring ring membership.
- 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)# interface range gi1/0/23-24
Switch(config-if-range)#shutdown
 %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:

```
Switch# conf t
Switch(config)#int hs1
Switch(config-if-range)#shut
```

- 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)# interface range gi1/0/23-24
Switch(config-if-range)# switchport mode  access
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)
```

- 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.
- As soon as you configure an HSR ring on two ports of a switch, MAC flaps will be observed on other switches where the HSR configuration is yet to be applied. We recommend that you shut down the newly created HSR ring on the switch before configuring the ring on all switches, and then re-enable them one by one as shown below. For example, if there are four switches in the ring, disable the HSR ring interfaces on each switch:

```
Switch1(config)# interface range gi1/0/21-22
Switch1(config-if-range)# shutdown
```

```
Switch1(config-if-range)# hsr-ring 1
Creating a HSR-ring interface hs1
Switch1(config-if-range)# int hs1
Switch1(config-if-range)# shutdown
Switch1(config-if-range)# end
```

After all four switches are configured with the ring, re-enable the HSR ports on each switch:

```
Switch1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)# interface range gi1/0/21-22
Switch1(config-if-range)# int hs1
Switch1(config-if-range)# no shutdown
Switch1(config-if-range)# end
Switch1#
```

This prevents interim MAC flapping during HSR ring configuration in member switches.

HSR or PRP on a IE9300 Stack

The Parallel Redundancy Protocol (PRP) offers significant advantages in facilitating redundancy with zero downtime. High-availability Seamless Redundancy (HSR) is similar to PRP but is designed to work in a ring topology. While the initial implementation was limited to standalone switches, recent advancements have enabled PRP or HSR to be utilized in stacked configurations.

Benefits of PRP or HSR on a IE9300 Stack

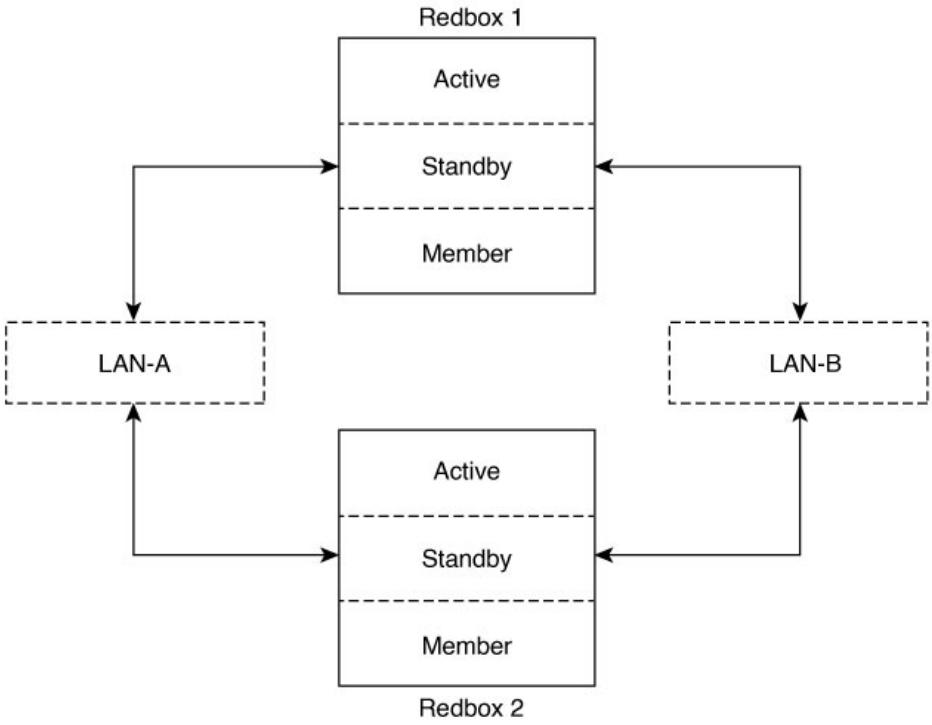
Deploying PRP or HSR in a stacked setup introduces a node level redundancy within the network.

- This enhancement mitigates the risk of single points of failure.
- Ensures the system remains operational even if a stack member or the active switch fails.
- The functionality and behavior of PRP and HSR remain consistent in both standalone and stacked configurations.
- Provides seamless integration and reliability across the network.

For more information on Switch Stacks, see Managing Switch Stacks.

Note There are no changes to the functionality or behavior of PRP and HSR when implemented in a IE9300 stack compared to their standalone configurations.

The following illustration displays a IE9300 stack as a RedBox.



Note A maximum of four-member stack can be configured with PRP or HSR as RedBox.

Guidelines and Limitations

The following guidelines and limitations apply:

- You can create any one of the following configurations:
  - HSR: Maximum of two rings

    or
  - PRP: Maximum of two channels

    or
  - One HSR ring and one PRP channel
- PRP and HSR are supported on IE-9320-26S2C and IE-9320-22S2C4X only.
- PRP and HSR on IE9300 stack is supported only if both the active and standby switches are FPGA-based SKUs.
- Both ports of a channel and a ring must be on the same slot, that is, the primary and secondary interfaces must be on the same switch member.
- When PRP or HSR is configured on the active unit and the switch goes down, it remains unavailable until the switch is restored.

Active-Standby Synchronization Mechanism Post-Switchover

Synchronization of the PRP or HSR to a redundant standby, supportis both incremental and bulk synchronization updates.

The behavior of PRP channel or HSR ring when a switch goes down, is as follows:

- If the channel or ring is configured on the standby switch, it will synchronize with the previous states of the channel or ring from the last active configuration.
- If the channel or ring is configured on the active switch, it will transition to a down state due to the slot being inactive. Once the slot is reactivated, the volatile FPGA will be reprogrammed with the previously configured values.

Default Settings

Table 1: 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	Set FPGA register for source mac filtering.	enable or disable	enable
nodeForgetTime	Time to clear an inactive entry from the node table.	0-65535	6000 ms
nodeRebootInterval	Time after which the RedBox must start sending supervision frames after bootup.	0-65535	500 ms
pauseFrameTime	Time interval between HSR pause frames.	0-65535	25 ms
proxyNodeTableForgetTime	Time to clear an inactive entry from the proxy node table or vdan table.	0-65535	6000 ms
supervisionFrameLifeCheckInterval	Life check interval value for supervision frames.	0-65535	2000 ms
supervisionFrameOption			
mac-da	The last bytes of the destination MAC address of supervision frames (01:15:4E:00:01:00). The last 00 is replaced by the value of this parameter.	1-255 MAC DA last eight bits option value	No default

Parameter	Description	Range	Default Value
vlan-cfi	Enable Canonical Format Indicator (CFI) for the VLAN tagged frame.	enable or disable	disable
vlan-cos	Class of Service (COS) value to be set in the VLAN tag of the Supervision frame.	0-7	0
vlan-id	The VLAN tag of the supervision frame.	0-4095	0
vlan-tagged	Set VLAN tagging option.	enable or disable	disable
supervisionFrameRedboxMacaddress	The RedBox MAC address in the supervision frames.	48-bit RedBox MAC address	The interface HSR ring MAC address
supervisionFrameTime	Time 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 and Limitations, on page 99 section of this chapter.
- Ensure that the member interfaces of a HSR ring are not participating in any redundancy protocols such as FlexLinks, EtherChannel, REP, and so on before configuring a HSR ring.

Procedure

Step 1 Enter global configuration mode:

```
Switch# configure terminal
```

Step 2 (Optional) Globally enable CDP to provide information about HSR ring nodes:

```
Switch(config)# cdp run
```

Step 3 (Optional) Globally enable LLDP to provide information about HSR ring nodes:

```
Switch(config)# lldp run
```

Step 4 Enter interface configuration mode and disable PTP on the ports to be assigned to the HSR ring:

```
Switch(config)# interface range gi1/0/21-22
Switch(config-if-range)# no ptp enable
```

Step 5 (Optional) Enable CDP on the ports to be assigned to the HSR ring:

```
Switch(config-if-range)#cdp enable
```

Step 6 (Optional) Enable LLDP on the ports to be assigned to the HSR ring:

```
Switch(config-if-range)#lldp transmit
Switch(config-if-range)#lldp receive
```

Step 7 Shut down the ports before configuring the HSR ring:

```
Switch(config-if-range)# shutdown
```

Step 8 Create the HSR ring interface and assign the ports to the HSR ring:

```
Switch(config)# interface range gigabitEthernet 1/0/21-22
Switch(config-if-range)# hsr-ring 1
```

Step 9 (Optional) If required, configure HSR ring optional parameters. See the Default Settings section for the parameter descriptions, ranges and default values.

```
Switch(config-range)# hsr 1 supervisionFrameLifeCheckInterval 10000
```

Step 10 Turn on the HSR interface:

```
Switch(config-if-range)# no shutdown
Switch(config-if-range)# end
```

Example

```
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
```

Clear All Node Table and VDAN Table Dynamic Entries

Procedure

Step 1 To clear all dynamic entries in the node table, enter the following command: **clear hsr node-table**

Step 2 To clear all dynamic entries in the VDAN table, enter the following command; **clear hsr vdan-table**

Verifying the Configuration

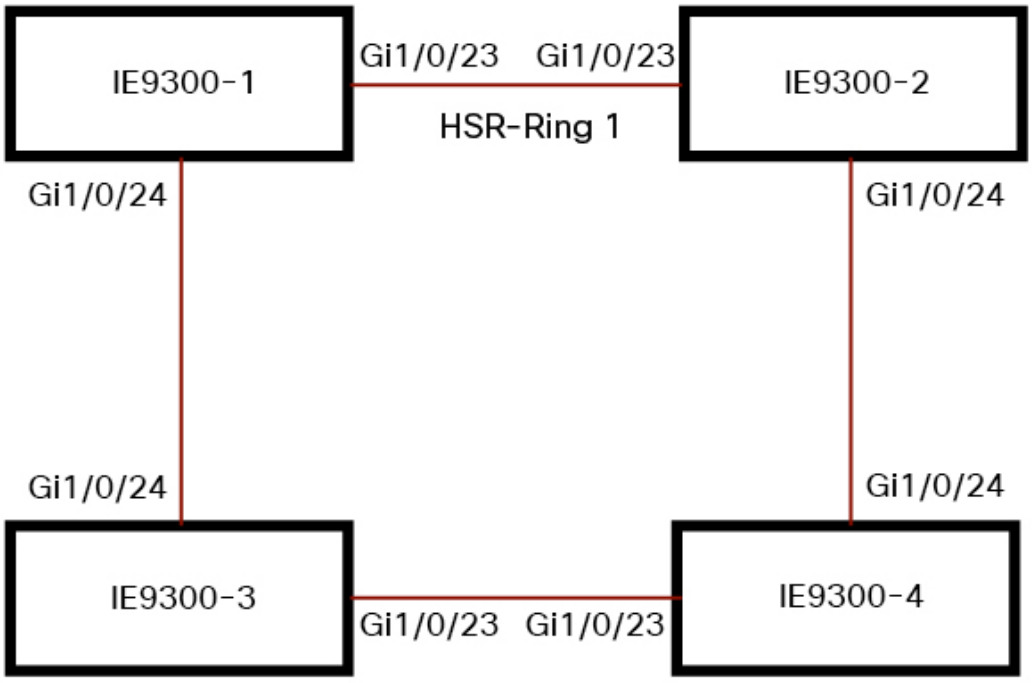
Command	Purpose
show hsr ring 1 [**detail**]	Displays configuration details for the specified HSR ring.
show hsr statistics {**egressPacketStatistics** | **ingressPacketStatistics** | **nodeTableStatistics** | **pauseFrameStatistics**}	Displays statistics for HSR components. **Note** To clear HSR statistics information, enter the command **clear hsr statistics**.
show hsr node-table	Displays HSR node table.
show hsr vdan-table	Displays HSR Virtual Doubly Attached Node (VDAN) table. **Note** The VDAN table and Proxy node table are the same.
show cdp neighbors	Displays CDP neighbor information for an HSR ring.
show lldp neighbors	Displays LLDP neighbor information for an HSR ring.

Configuration Examples

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 15: 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

- Cisco Catalyst IE9300 Rugged Series Switch documentation.
- IEC 62439-3, Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)

Feature History

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