



Parallel Redundancy Protocol

- [Information About PRP, on page 1](#)
- [TrustSec on a PRP Interface, on page 6](#)
- [Prerequisites, on page 11](#)
- [Guidelines and Limitations, on page 12](#)
- [Default Settings, on page 14](#)
- [Create a PRP Channel and Group, on page 14](#)
- [Configuring PRP Channel with Supervision Frame VLAN Tagging, on page 17](#)
- [Add Static Entries to the Node and VDAN Tables, on page 20](#)
- [Clearing All Node Table and VDAN Table Dynamic Entries, on page 21](#)
- [Disabling the PRP Channel and Group, on page 21](#)
- [Errors and Warnings as Syslog Messages , on page 22](#)
- [Configuration Examples, on page 23](#)
- [Verify Configuration, on page 35](#)
- [Related Documents, on page 37](#)
- [Feature History, on page 37](#)

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-E and 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.

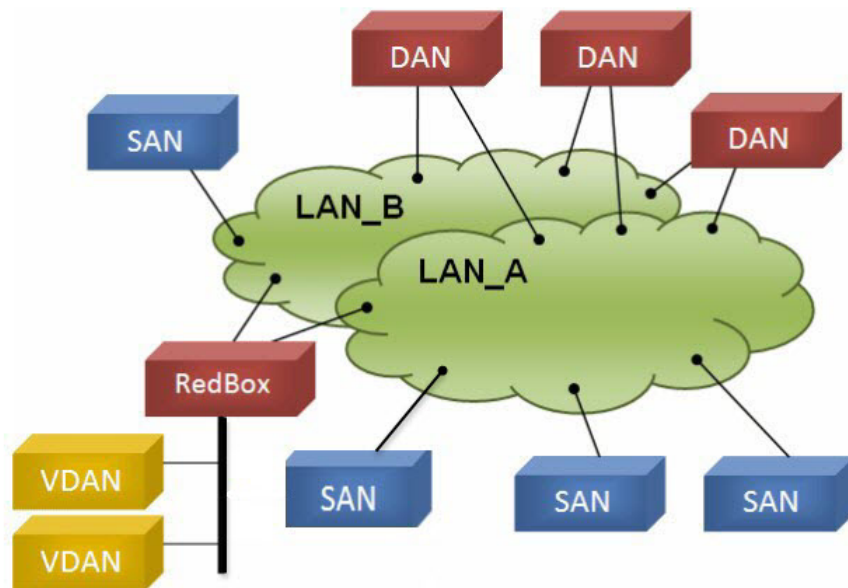
PRP uses a different scheme, where the end nodes implement redundancy (instead of network elements) by connecting two network interfaces to two independent, disjointed, parallel networks (LAN-A and LAN-B). Each of these Dually Attached Nodes (DANs) then have redundant paths to all other DANs in the network.

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.

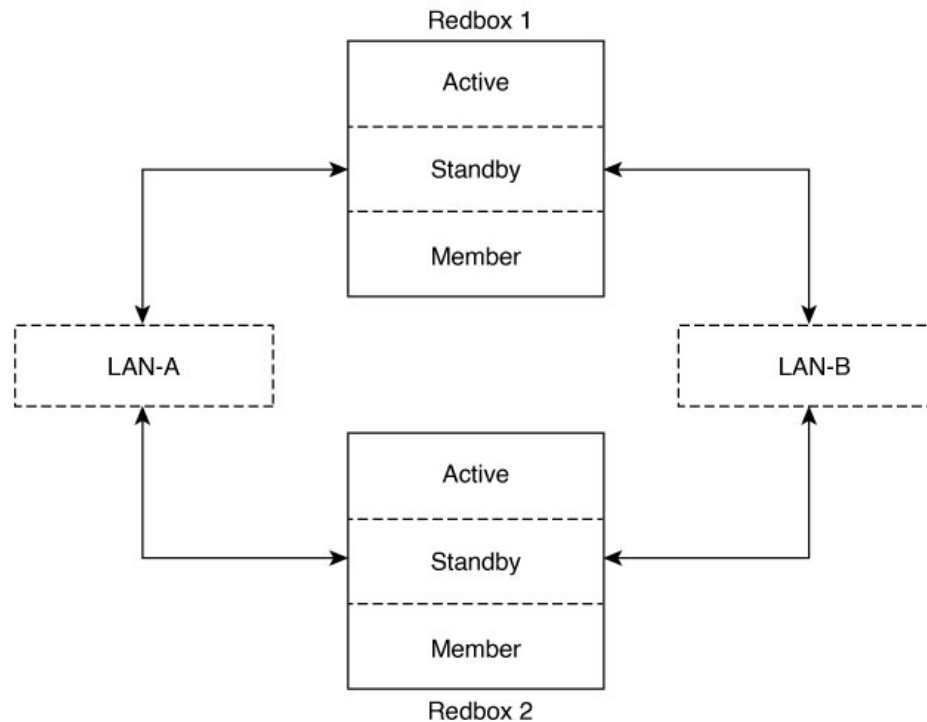
- This enhancement mitigates the risk of single points of failure.
- Ensures the system remains operational even if a stack member or the active switch fails.
- The functionality and behavior of PRP and HSR remain consistent in both standalone and stacked configurations.
- Provides seamless integration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

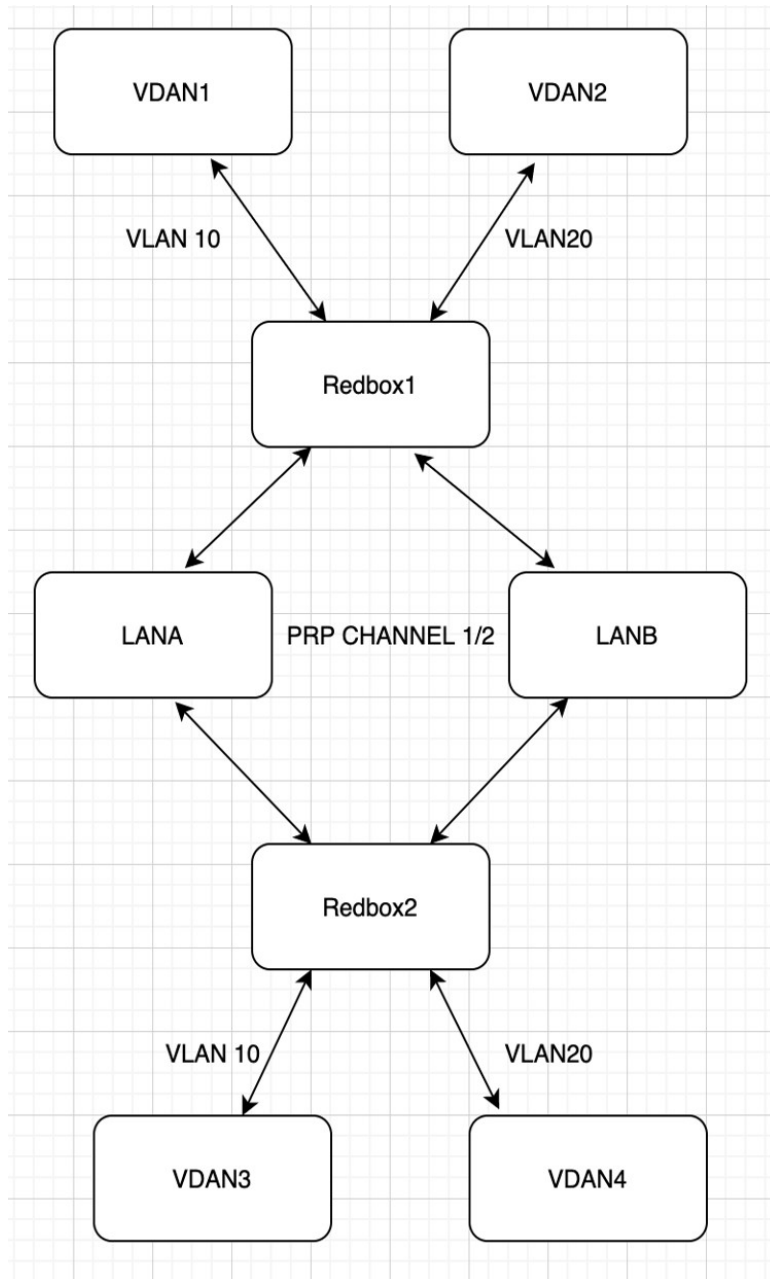
A RedBox with VDANs needs to send supervision frames on behalf of those VDANs. For traffic coming in on all other ports and going out PRP channel ports, the switch learns source MAC addresses, adds them to the VDAN table, and starts sending supervision frames for these addresses. Learned VDAN entries 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:
000200B8000300010004001051F577DC7E176855650F2F5609418AC60006009C000301002BBB79441FEE97B0E0B339B9036F9C710000001364C8D
1A000093A8054BC5FA1780A24E23B60A4BFF46AF47A317EE20391BFC6F0CAABA7F66393F05799A3B0EAB602B54749DCF7225A45FDD81349A81977D857B9C3
```



```

1959A2B54CFC4505CD903D84394E69E5795D31543EB575FB8D51A6FA021FB5E6A0C296F8CA21318377688073516714125D38973D9BF2A66792E3AD1C0A05C3
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:     SUCCEDED
    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 bpdupfilter 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 bpdupfilter 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 bpdudfilter on the prp-channel interface:
spanning-tree bpdudfilter 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 bpdudfilter 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 bpdupfilter 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 bpdudfilter on the prp-channel interface:

spanning-tree bpdudfilter 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 interval 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.

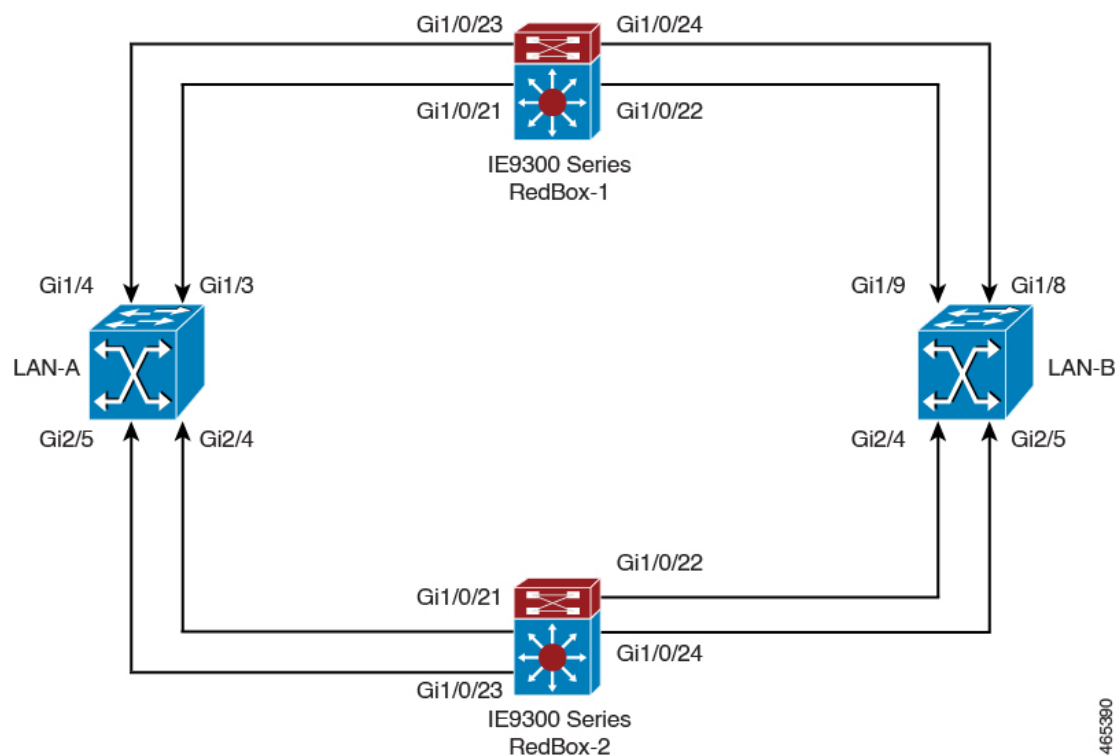
Example

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
!
!
!
!
!
!
!
!
!
!
!
!

```

485380


```
!  
!  
!  
!  
!  
!  
!  
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
  udd 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
  udd 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  
  uddld 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  
  uddld 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
 uddl port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdudfilter enable
!
interface GigabitEthernet1/0/24
 switchport mode trunk
 switchport trunk allowed vlan 30,40
 no ptp enable
 uddl port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdudfilter 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 |
|--|--|
| <code>show prp channel {1 2 [detail status summary] detail status summary}</code> | Displays configuration details for a specified PRP channel. |
| <code>show prp control {VdanTableInfo ptpLanOption ptpProfile supervisionFrameLifeCheckInterval supervisionFrameOption supervisionFrameRedboxMacaddress supervisionFrameTime}</code> | Displays PRP control information, VDAN table, and supervision frame information. |
| <code>show prp node-table [channel-group <group> detail]</code> | Displays PRP node table. |
| <code>show prp statistics {egressPacketStatistics ingressPacketStatistics nodeTableStatistics pauseFrameStatistics ptpPacketStatistics}</code> | Displays statistics for PRP components. |
| <code>show prp vdan-table [channel-group <group> detail]</code> | Displays PRP VDAN table. |
| <code>show interface prp-channel {1 2}</code> | 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. |

