

Parallel Redundancy Protocol

- Information about PRP, on page 1
- Prerequisites, on page 5
- Guidelines and limitations, on page 6
- TrustSec on a PRP interface, on page 7
- Default Settings, on page 12
- Create a PRP channel and group, on page 12
- Configure PRP channel with supervision frame VLAN tagging, on page 15
- Add static entries to the node and VDAN tables, on page 20
- Clear all node table and VDAN table dynamic entries, on page 22
- Disable the PRP channel and group, on page 22
- Errors and warnings as syslog messages , on page 23
- Example for creating VLANs and PRP Channels, on page 24

Information about PRP

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

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

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

Traditional redundancy vs. PRP

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

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

How PRP works with dually attached nodes (DANs)

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

Singly attached nodes (SANs)

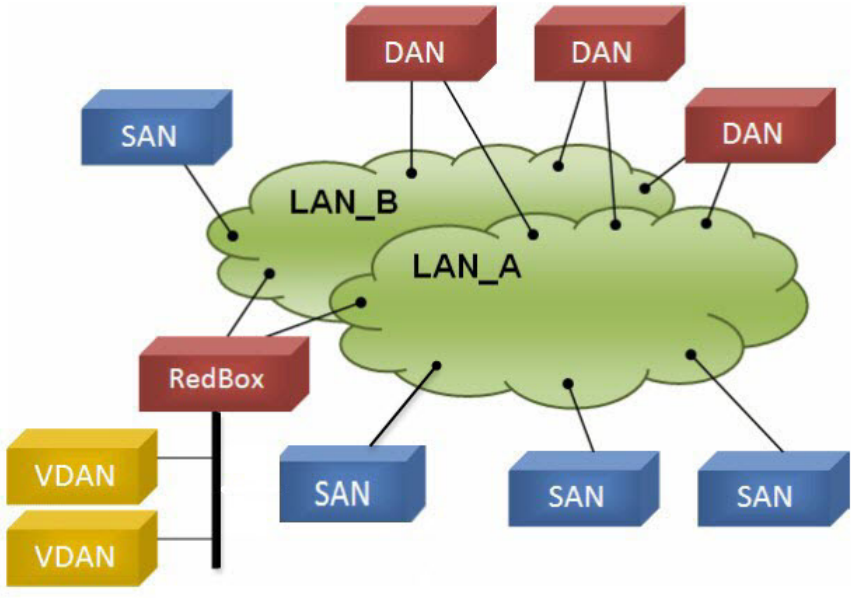
Non-redundant endpoints in the network that attach only to either LAN-A or LAN-B are known as Singly Attached Nodes (SANs).

Redundancy box (RedBox) and virtual DAN (VDAN)

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

The image here shows a PRP redundant network.

Figure 1: PRP Redundant Network



Supervision frames

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

Role of switches

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

PRP Channels

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

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

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

Table 1: Supported interfaces for PRP channel

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

Mixed traffic and supervision frames

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

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

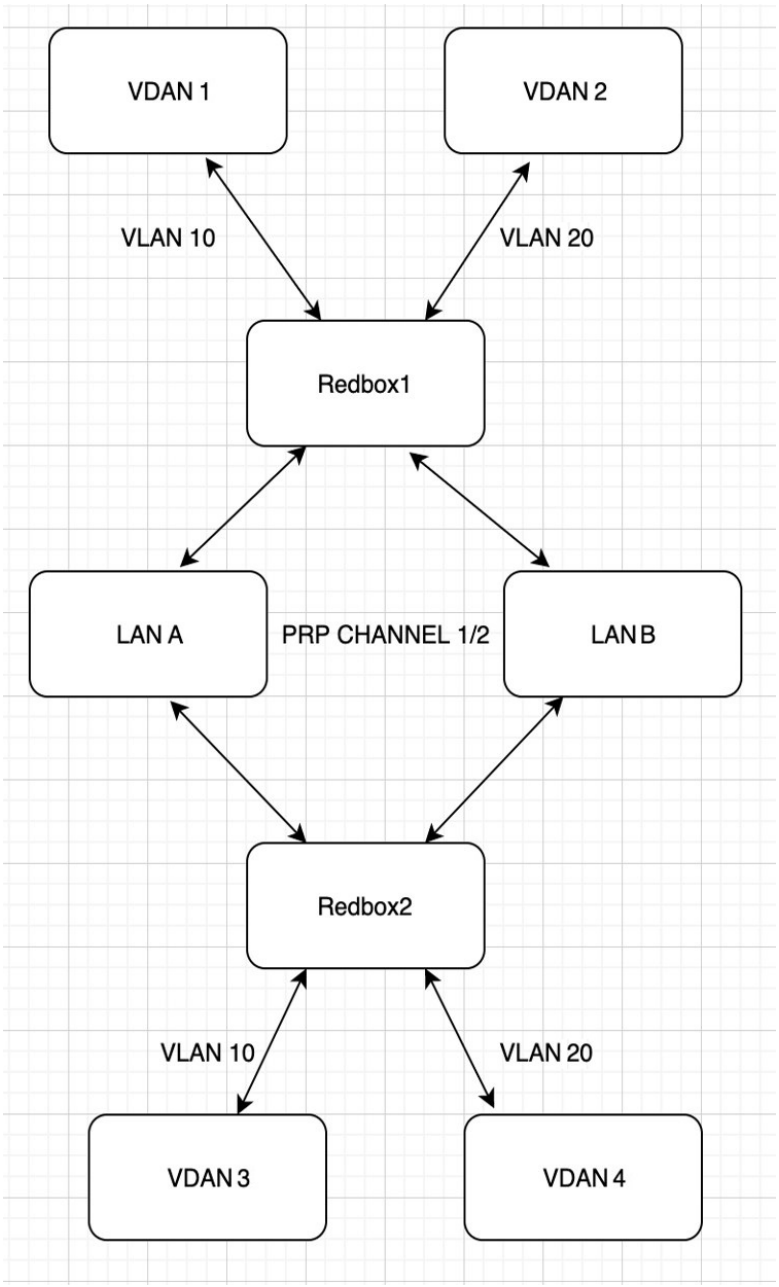
VLAN tags in supervision frame

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

Example: Configuring PRP channel with supervision frame VLAN tagging

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

Figure 2: Configuring PRP Channel with Supervision Frame VLAN Tagging



See Configure PRP channel with supervision frame VLAN tagging, on page 15 for configuration information.

Prerequisites

These prerequisites are applicable for setting up PRP.

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

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

Guidelines and limitations

Review these guidelines and limitations before you configure PRP.

Feature availability and support limitations

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

Commands and operational monitoring guidelines

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

Interface configuration guidelines

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

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

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

Hardware and physical interface limitations

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

  ```
  system mtu 1506
  ```

Spanning tree protocol (STP) guidelines

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

Node and VDAN table limitations

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

TrustSec on a PRP interface

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

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

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

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

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

Examples for configuring TrustSec on a PRP interface

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

Configuring TrustSec on each interface

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

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

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

Configuring TrustSec on a range of interfaces

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

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

Configuring TrustSec when interface is a member of a PRP channel

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

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

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

CTS and PRP show commands

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

show cts interface summary

```
switch#show cts interface summary
CTS Interfaces
----------------------
Interface                      Mode    IFC-state dot1x-role peer-id    IFC-cache
Critical-Authentication
-------------------------------------------------------------------------------
Gi1/0/21                       MANUAL  OPEN      unknown    unknown    invalid  Invalid
Gi1/0/22                       MANUAL  OPEN      unknown    unknown    invalid  Invalid
R1#show cts pacs
AID: 51F577DCE176855650F2F5609418AC6
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: 51F577DC7E176855650F2F5609418AC6
  I-ID: petra3400ipv4
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 09:06:08 UTC Wed Nov 01 2023
PAC-Opaque:
000200B80003000100040001051F577DC7E176855650F2F5609418AC60006009C000301002BBB79441FEE97B0E0B339B9036F9C710000001364C8D
1A000093A8054BC5FA1780A24E23B60A4BFF46AF47A317EB20391BFCA6F0CAABA7F66393F05799A3B0EAB602B54749DCF7225A45FDDB1349A81977D857B9C3
1959A2B54CFC4505CD903D84394E69E5795D31543BB575FB8D51A6FA021FB5E6A0C296F8CA21318377688073516714125D38973D9BF2A66792E3AD1C0A05C3
E739CA1
Refresh timer is set for 12w4d
R1#show cts interface GigabitEthernet1/0/21
Global Dot1x feature is Disabled
Interface GigabitEthernet1/0/21:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Interface Active for 00:03:25.772
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    SUCCEEDED
        Peer SGT:            30
        Peer SGT assignment: Trusted
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Enabled
    Cache Info:
        Expiration            : N/A
```

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

show cts role-based counters

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

show prp channel detail

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

show prp statistics ingressPacketStatistics

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

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

show prp statistics egressPacketStatistics

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

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

Default Settings

By default, no PRP channel exists on the switch until you create it. Interfaces that can be configured for PRP are fixed, as described in PRP Channels, on page 3 .

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 3.
- Review the Prerequisites, on page 5 and Guidelines and limitations, on page 6.
- Ensure that the member interfaces of a PRP channel are not participating in any redundancy protocols such as FlexLinks, EtherChannel, or REP, before creating a PRP channel.

Procedure

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

- For channel 1, enter:

  interface range GigabitEthernet1 *interface range/channel group*

- For channel 2, enter:

  interface range GigabitEthernet2*interface range/channel group*

Example:

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

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

Note

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

Step 2 Perform these optional steps, as required.

Option	Description

Configure a switch port	Use the **switchport** command for Layer 2 traffic.
	`switch(config)#switchport`
	Use the **no switchport** command for Layer 3 traffic.
	`switch(config)#no switchport`

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

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

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

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

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

Example:

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

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

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

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

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

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

Example:

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

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

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

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

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

Examples of creating a PRP channel and group

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

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

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

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

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

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

Verify PRP channel

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

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

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

Configure PRP channel with supervision frame VLAN tagging

Before you begin

- Review the specific interfaces supported for each switch type, as described in PRP Channels, on page 3.
- Review the Prerequisites, on page 5 and Guidelines and limitations, on page 6.
- Ensure that the member interfaces of a PRP channel are not participating in any redundancy protocols such as FlexLinks, EtherChannel, REP, and so on before creating a PRP channel.

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

Procedure

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

- For channel 1, enter:

  interface range GigabitEthernet1 *interface range/channel group*

- For channel 2, enter:

  interface range GigabitEthernet2*interface range/channel group*

Example:

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

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

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

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

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

Example:

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

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

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

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

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

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

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

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

Example:

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

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

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

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

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

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

Example:

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

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

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

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

prp-channel-number: 1 or 2

value:VLAN number from 0 to 4095

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

prp-channel-number: 1 or 2

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

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

prp-channel-number: 1 or 2

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

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

Configuration example for VLAN tagging

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

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

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

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

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

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

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

PRP_IE9300#
```

Verify VLAN tagging

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

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

Add static entries to the node and VDAN tables

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

Procedure

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

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

Example:

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

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

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

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

Example:

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

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

Display PRP node table and VDAN table

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

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

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

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

Clear all node table and VDAN table dynamic entries

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

Procedure

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

Example:

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

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

Example:

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

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

Note
The **clear prp node-table** and **clear prp vdan-table** commands clear only dynamic entries. To clear static entries, use the **no** form of the **nodeTableMacaddress** or **vdanTableMacaddress** commands as shown in Add static entries to the node and VDAN tables, on page 20.

Disable the PRP channel and group

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

Procedure

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

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

prp-channel-number: 1 or 2

Example:

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

Errors and warnings as syslog messages

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

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

- Wrong LAN ID A

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

- Wrong LAN ID B

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

- Warning LAN A

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

- Warning LAN B

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

- Oversize packet A
- Oversize packet B

You can configure the interval at which the syslog messages are generated. See the section Configure the PRP Logging Interval, on page 23 for more information.

Configure the PRP Logging Interval

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

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

Procedure

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

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

Example:

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

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

The switch generates syslogs from the PRP errors and warnings listed in the section Errors and warnings as syslog messages , on page 23 .

This text shows sample output after configuring the logging interval.

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

Verify PRP logging interval

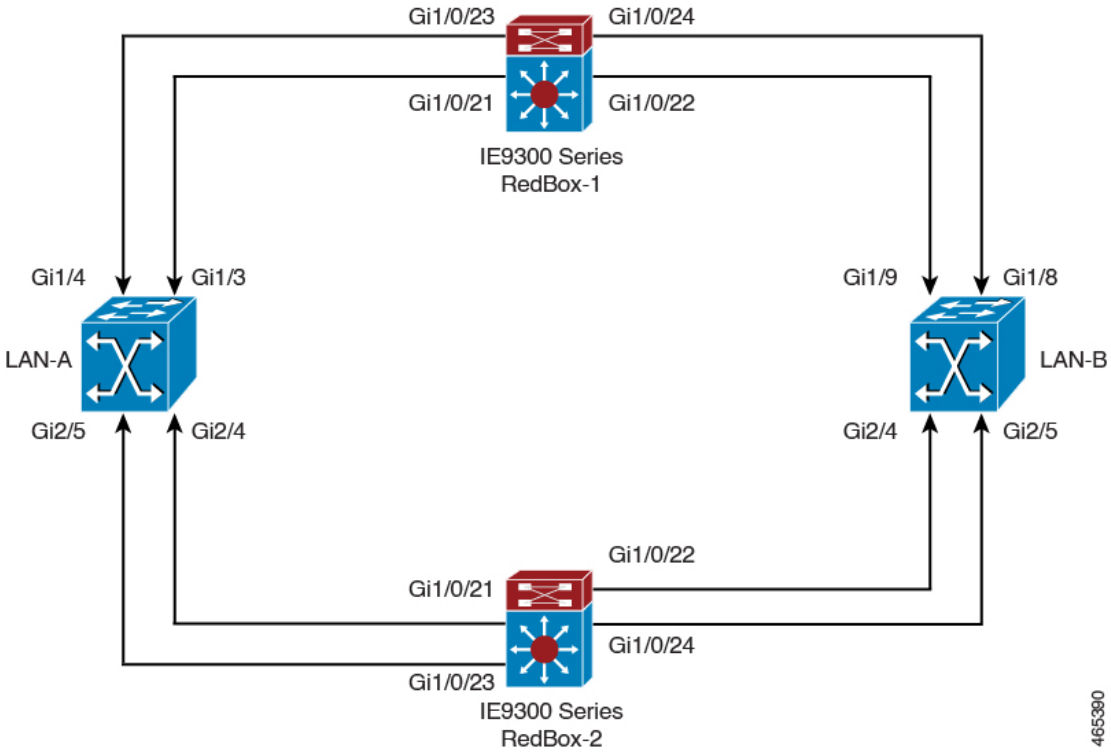
Use the **prp logging-interval** command to verify that the PRP logging interval is successfully configured.

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

Example for creating VLANs and PRP Channels

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

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



Following is the configuration for LAN-A:

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

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

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

The configuration for LAN-B is shown below:

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

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

Following is the configuration for RedBox-1:

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

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

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

Following is the configuration for RedBox-2:

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

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

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

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

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